LATIN LAWYER

THE GUIDE TO CORPORATE COMPLIANCE

FOURTH EDITION

Editor
Andrew M Levine

The Guide to Corporate Compliance

The Guide to Corporate Compliance

Fourth Edition

Editor

Andrew M Levine

Published in the United Kingdom by Law Business Research Ltd
by Law Business Research Ltd, London
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.latinlawyer.com

Enquiries concerning reproduction should be sent to Law Business Research, at the address above. Enquiries concerning editorial content should be directed to the Publisher – clare.bolton@lbresearch.com

ISBN 978-1-80449-252-9

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

Andrew B Jánszky

Anheuser-Busch InBev

Beccar Varela

Carey

Chevez, Ruiz, Zamarripa y Cía

Davis Polk & Wardwell LLP

Debevoise & Plimpton LLP

Deloitte

FTI Consulting

Hogan Lovells

Hughes Hubbard & Reed LLP

Incode Technologies Inc.

McGuireWoods LLP

Mijares Angoitia Cortés y Fuentes SC

Morrison & Foerster LLP

Ropes & Gray

Skadden, Arps, Slate, Meagher & Flom LLP

Sullivan & Cromwell LLP

Vinson & Elkins LLP

Von Wobeser y Sierra, SC

Publisher's Note

Latin Lawyer and LACCA are delighted to publish the fourth edition of *The Guide to Corporate Compliance*.

Edited by Andrew M Levine, litigation partner at Debevoise & Plimpton LLP, this brings together the knowledge and experience of leading practitioners from a variety of disciplines and provides guidance that will benefit all those who must navigate the region's complex, fast-changing framework of rules and regulations. In particular, this latest edition offers a fresh focus on forensic accountancy, how a volatile political situation can push ESG to the top of the agenda and the compliance challenges involved with fintech – among other areas.

We are delighted to have worked with so many leading individuals to produce *The Guide to Corporate Compliance*. If you find it useful, you may also like the other books in the Latin Lawyer series, including *The Guide to Infrastructure and Energy Investment* and *The Guide to Corporate Crisis Management*, as well as our jurisdictional references and our tool providing overviews of regulators in Latin America.

My thanks to the editor for his vision and energy in pursuing this project and to my colleagues in production for achieving such a polished work.

Contents

Introduction

Andrew M Levine[1]

Compliance in context

I recall vividly the first time I led a compliance seminar in Latin America. Although I received a warm welcome that day in São Paulo, many in the room seemed uncertain about the relevance locally of the US Foreign Corrupt Practices Act and, more generally, anti-corruption best practices. From a compliance perspective, that was a lifetime ago. So much has changed.

Back then, it seemed improbable that Brazil would soon adopt a sweeping anti-corruption law. Only a short time later, following riots in the streets, Brazil did precisely that, and the law dramatically took effect in January 2014. Those sceptical that Brazil ever would adopt such a law quickly transitioned their scepticism, next doubting that Brazil ever would enforce this law. That assumption again proved faulty. A tsunami of enforcement followed soon after, making headlines around the globe. Companies have paid big penalties, and high-profile politicians and business executives have been charged, convicted and imprisoned. Even so, questions persist regarding some of these proceedings, and backlash continues in various forms. It also remains unclear exactly how the recent change in administration will impact Brazil's anti-corruption path.

In addition to spawning countless enforcement operations within Brazil, these developments have reverberated throughout Latin America, with further shockwaves felt around the world. Although Brazil has played an outsized role in Latin America's anti-corruption narrative, other jurisdictions also have augmented their efforts to combat corruption. Numerous countries in the region (such as Argentina, Colombia, Mexico and Peru) have adopted new and expansive anti-corruption laws. More surprising to many, local authorities increasingly have enforced these laws, albeit to varying degrees and while grappling with an

1 Andrew M Levine is a partner at Debevoise & Plimpton LLP.

array of political, economic and other challenges. Anti-corruption contours vary throughout the region, but some of the basic ingredients persist, including highly relevant laws, locals fed up with corruption and scandals that abound.

Within this context, actual enforcement can serve as a powerful motivator of intensified corporate compliance efforts. For obvious reasons, the spectre of aggressive enforcement offers a highly persuasive justification for finding religion in this area and making the necessary adjustments and investments. Along these lines, the US Deputy Attorney General has warned that '[c]ompanies need to actively review their compliance programs to ensure they adequately monitor for and remediate misconduct – or else it's going to cost them down the line'.[2]

More broadly, enforcement risk remains acute in the United States and certain other jurisdictions. This is especially the case in the United States after the Biden administration in 2021 elevated fighting corruption to a national security priority and since has launched related initiatives. Unsurprisingly, a significant element of the resulting US anti-corruption strategy involves active engagement and close coordination with foreign partners, possibly foretelling greater collaboration between US authorities and Latin American counterparts.

An effective compliance programme

Companies and individuals often want to do the right thing, but an effective compliance programme entails more than just a pristine ethical mindset. Among other essential features discussed in this book, a compliance programme requires the commitment of management at all levels and sufficient resourcing to do the job well.

Indeed, much ink has been spilled over what constitutes an effective compliance programme, including in Latin America. Yet the main elements are relatively uncontroversial, with certain compliance truths remaining generally applicable. For example, as outlined in guidance issued by the US Department of Justice and updated most recently in March 2023, proper evaluation of a corporate compliance programme necessarily involves assessing its design, implementation and effective functioning:

2 US Department of Justice, 'Deputy Attorney General Lisa O. Monaco Gives Keynote Address at ABA's 36th National Institute on White Collar Crime' (28 October 2021), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute.

- Design: proper design begins with a thoughtful risk assessment. This includes evaluating a company's compliance risk factors, such as its jurisdictions of operation, industry, government touchpoints and reliance on third parties. Just as no two companies are the same, a compliance programme cannot be one-size-fits-all but must be tailored to a company's risk profile and integrated into its internal controls.
- Implementation: even the most brilliantly crafted programme can provide only limited comfort if it is not implemented effectively. This requires the commitment of management, autonomy, resourcing and empowerment of the compliance function, and both incentives for compliance and disincentives for non-compliance.
- Functioning: a compliance programme is only as good as it functions in practice. Adequate monitoring, testing and review are necessary to ensure that a programme is working as intended and is refined as needed. Proper functioning also requires the investigation of potential misconduct and remediation of any underlying issues.[3]

It bears underscoring that risks posed by third parties, in particular, remain many companies' most significant anti-corruption exposure. Countless examples of recent enforcement in Latin America illustrate this reality: third parties rather than company employees often pay the bribes later subjected to government investigations. Third-party management is therefore a core element of an effective compliance programme and should include risk-based due diligence, written contracts that enshrine compliance obligations and careful oversight of the third parties' services.

In the end, no compliance programme is perfect or can prevent all wrongdoing, even with the best of intentions and good-faith efforts. For most companies, the question is not whether a compliance violation one day will occur but how severe and extensive it will be, how early and by what means it will be detected, and how the company ultimately will respond.

Companies and their stakeholders must accept this reality while making judicious use of sometimes limited compliance resources. This balancing act becomes particularly challenging amid a crisis, such as the covid-19 pandemic. However, it is predictably during a crisis when the cost of neglecting a compliance programme

3 US Department of Justice, Criminal Division, 'Evaluation of Corporate Compliance Programs' (updated March 2023), https://www.justice.gov/criminal-fraud/page/file/937501/download.

may be most acute. And, since 2020, economic challenges and political upheaval have both exacerbated the pandemic's devastating impacts and disrupted some of region's anti-corruption momentum.

Prosecutors play a valuable role in helping to incentivise companies to implement and maintain effective compliance programmes. Authorities in the region can do even more to support the growing compliance culture, including by imposing lower penalties on companies that implement effective programmes or, better yet, by declining altogether under appropriate circumstances from penalising these companies when certain things go wrong. This is especially so when companies are plagued by isolated misconduct of a rogue employee or a small number of employees. While active enforcement undoubtedly breeds greater efforts to comply, enforcement decisions that respect such genuine compliance efforts arguably can do so even more.

Overview of the book

This project has been a true labour of love for many. It also has been an absolute delight to collaborate with such knowledgeable and thoughtful contributors. I thank them deeply for their regional insights, nuanced analysis, spirited advice and deep commitment to spreading the gospel of compliance.

The book proceeds in four parts and includes significant updates since the prior edition and several new chapters (12, 20 and 21). Part 1 sets the scene by surveying the broader Latin American compliance landscape:

- Chapter 1: Peter Spivack and Isabel Costa Carvalho of Hogan Lovells LLP examine the dramatic rise and evolution of compliance in Latin America over several decades, becoming the necessity that it is today. They illustrate the increasing importance of compliance in the region, bolstered in part by guidelines issued by authorities in Argentina, Brazil, Colombia, Mexico and Peru. While acknowledging challenges in promoting cultural change and ensuring appropriate enforcement, the authors also observe how compliance now is transcending strict legal compliance to consider broader societal impacts.
- Chapter 2: Julie Bédard, Lauren A Eisenberg and Mayra Suárez of Skadden, Arps, Slate, Meagher & Flom LLP assess the current compliance climate and significant legislative changes in Latin America. The authors also explore regional enforcement trends, including the impact of increasing cooperation and coordination among regulators, the prioritisation of prosecuting individuals and enforcement involving particular industries. In light of these developments, the authors illuminate why companies operating in Latin America should maintain appropriate anti-corruption policies and other safeguards.

Part 2 then addresses key considerations in building an effective compliance programme:

- Chapter 3: Reynaldo Manzanarez Radilla, head of legal affairs and compliance at Incode Technologies Inc., profiles a successful compliance department. Although recognising that there is not a single formula for success, he analyses some of the fundamentals, including a strong tone at the top, core compliance policies, a true team of professionals and adequate resourcing. He explains how the compliance function must act as a trusted adviser to the business, operating cost-effectively and demonstrating its value, including when dealing with the unexpected.
- Chapter 4: Brendan P Cullen and Anthony J Lewis of Sullivan & Cromwell LLP elaborate on building a robust compliance programme in Latin America. They describe the elements of an effective programme, including based on guidance issued by US regulators, and associated challenges. Additionally, the authors recount compliance best practices such as documenting programme changes and successes, broadcasting a culture of compliance, obtaining local input and buy-in, relying on local counsel and leveraging data analytics.
- Chapter 5: Andrew Jánszky, a corporate governance and compliance consultant, turns to the pivotal role a company's board of directors should play, suggesting that expectations of boards have risen and should continue to do so. Specifically, he calls on board members to engage substantively on risk assessment and other compliance matters, actively complementing (but not supplanting) the essential role of management. While recognising the improbability that any company could achieve best practices in all respects, he extracts from various case studies cautionary lessons for boards and underscores the importance for a compliance function of independence, autonomy, and structural and cultural compatibility.
- Chapter 6: Daniel S Kahn, Tatiana R Martins and Jordan Leigh Smith of Davis Polk & Wardwell LLP next tackle conducting compliance risk assessments, the starting point for designing an effective compliance programme. As part of this process, they review the elemental tasks of mapping compliance risks based on factors such as a company's geographical and operational footprint and then ensuring that compliance resources and controls adequately address the identified risks. The authors also identify significant considerations regarding who conducts a compliance risk assessment, as well as the importance of refreshing an assessment, especially in the face of triggers that may alter a company's intrinsic risk profile.

- Chapter 7: Palmina M Fava, Zachary Terwilliger and Martin Pereya of Vinson & Elkins LLP tackle the significant compliance risks and related challenges posed by third parties. The authors provide compelling enforcement examples and then recount best practices for mitigating potential exposures, including by conducting risk-based due diligence, documenting compliance expectations and appropriately training third parties and monitoring their activities.
- Chapter 8: María González Calvet, Krystal Vazquez and Baldemar Conzalez of Ropes & Gray LLP next discuss best practices for building effective internal communications channels and the vital role of compliance training. They address the centrality of communications from the top and elsewhere regarding a deep commitment to compliance, the foundational role of compliance policies and procedures, and the imperative of an anonymous reporting mechanism. The authors explore challenges involving third-party messaging applications and mobile devices, as well as the prospect of measuring compliance through data analytics. They elaborate on the importance of tailoring a compliance programme to relevant laws and cultures, including adapting a global policy to a given location and delivering training that is customised for local workforces and replete with real-world examples.
- Chapter 9: Adrián Magallanes Pérez and Diego Sierra Laris of Von Wobeser y Sierra, SC review best practices for conducting internal investigations of alleged wrongdoing. After elaborating on why these investigations are vital, they detail the investigative life cycle, including conducting a preliminary assessment, determining whether to engage external counsel, developing an investigative plan, preserving evidence, taking steps to avoid any retaliation, reviewing documents, conducting interviews, preparing a final report and proposing any remedial steps. The authors highlight the value of conducting internal investigations and, in certain circumstances, self-reporting improper conduct to authorities.
- Chapter 10: my Debevoise & Plimpton LLP colleague Erich O Grosz and I delve into assessing and mitigating compliance risks in the transactional context, including before, during and after a transaction. While unknowingly buying a compliance problem can be disastrous, even assets tainted by corruption can sometimes be attractive targets. This chapter examines why and how compliance due diligence is essential for evaluating a potential transaction's true value and appropriateness, offering practical steps for conducting due diligence and addressing related risks. In addition, the chapter explains why identifying any problematic conduct pre-investment can be critical, both to avoid overpaying for an asset and to terminate and remediate any misconduct promptly after closing.

- Chapter 11: Gabriela Paredes, Dheeraj Thimmaiah, Jaime Munoz and John Sardar, all compliance professionals at Anheuser-Busch InBev, articulate a provocative technological manifesto, illustrating in practical terms how a data-driven approach can and must revolutionise corporate compliance programmes. The authors espouse benefits for programmes that leverage data science and analytics, including across risk assessments, internal investigations, and compliance monitoring. While recognising that companies will proceed in varying ways, the authors note opportunities encompassing automation and process optimisation, identification and harmonisation of data sets, and application of both supervised and unsupervised machine learning.
- Chapter 12: Nelson Luis, Raúl Saccani and Fernando Peyretti of Deloitte explore how attorneys and forensic accountants work collaboratively to help clients mitigate financial and compliance risks, including by detecting and preventing fraud and other malfeasance. For both proactive and reactive matters, such as due diligence and investigations, respectively, the authors describe attorneys' and accountants' complementary skills that help clients make better informed decisions. Among other timely topics, the authors examine best practices involving third-party risk management, challenges of preserving and collecting evidence, and approaches to transaction testing and monitoring.

Part 3 turns to specific legislative and regulatory pressure points:

- Chapter 13: Lorena Pavic, José Pardo, Benjamín Torres and Raimundo Gálvez of Carey explore challenges in navigating competition rules, drawing in part on reforms in Argentina, Brazil, Chile, Ecuador, Mexico and Peru. The authors address relevant legal landscapes, illustrating the increased anticompetition standards throughout the region. The chapter then examines related exposures, including cartel investigations, and proposes safeguards to mitigate competition risks, including avoiding, deterring and detecting collusive behaviour. As the authors note, close attention to competition law is imperative for effective corporate compliance in Latin America.
- Chapter 14: a team from Vinson & Elkins LLP – Palmina M Fava, Gabriel Silva, Christopher James anc Martin Pereyra – discusses how data protection laws have proliferated throughout Latin America, more recently following the European Union's model. The authors explore differences in the various legal regimes, including around breach notification requirements. Additionally, the authors explain the value of an effective data compliance programme, subject to testing and updating, both to prevent violations and, if necessary, to defend a company against any related lawsuits or investigations.

- Chapter 15: relatedly, Antonio Gesteira, Jordan Rae Kelly and Adriana Prado of FTI Consulting explore strategies for reducing cybersecurity and data risk, focusing in particular on ensuring incident readiness and building a culture of compliance. The authors detail the perfect storm of growing risks involving data breaches and cyber incidents, compounded by increasing enforcement in Latin America regarding data protection. In particular, the authors underscore the importance of prevention, including careful attention to incident response planning, and best practices for confronting an incident and dealing with the aftermath.
- Chapter 16: Ryan Fayhee, Diego Durán de la Vega, Tyler Grove and Anna Hamati of Hughes Hubbard & Reed LLP explore risks in Latin America involving compliance with US sanctions, a topic of particular prominence given recent global events. After providing an overview of US economic sanctions, the authors focus on recent developments regarding Nicaragua, Paraguay, Venezuela and Russia, and they assess related enforcement, including civil penalty and secondary sanctions actions. The authors conclude with recommendations for designing and implementing an effective sanctions compliance programme, emphasising the importance of such steps given the far reach of US enforcement.
- Chapter 17: Maximiliano D'Auro and Gustavo Papeschi of Beccar Varela provide an Argentine perspective on risk management in the financial services industry. Although financial services providers usually recognise their inherent exposure to anti-money laundering risk, the authors argue that these providers often insufficiently appreciate their anti-corruption exposure, notwithstanding the breadth of government touchpoints. Accordingly, the authors expound the elements of an integrity programme for financial services providers, especially in light of changes to Argentine law and associated compliance guidelines.

Last, Part 4 looks to the future, highlighting some compliance trends to watch:

- Chapter 18: Ben O'Neil and Elissa N Bauer of McGuire Woods LLP foretell the creep of legislation targeting private corruption. They review the corrosive effects of commercial bribery, which are increasingly borne by the public, and the differing regulatory regimes used to combat these types of corrupt practices. The authors also discuss strategies for identifying the telltale signs of kickback schemes and for preventing private corruption through appropriate compliance policies and internal controls.

- Chapter 19: a team from Morrison & Foerster LLP – Ruti Smithline, Hayley Ichilcik, James M Koukios, Lauren Navarro and Stephanie Pong – delves deeply into the social pillar (the 'S') of environmental, social and governance (ESG), broadly encompassing companies' relationships with stakeholders including employees, suppliers, customers and others. The authors detail several frameworks for measuring associated progress, such as the UN Sustainable Development Goals, and then explore relevant legal developments in Brazil, Chile, Colombia, Mexico and Peru. In addition, the authors highlight practical considerations for companies in addressing the social pillar, concluding that those doing so effectively may enjoy a competitive advantage, especially as new ESG-related legal regimes emerge.
- Chapter 20: relatedly, Martín Sánchez, Gabriel Calvillo, Adriana Morales and Paula Pérez Benítez of Mijares Angoitia Cortés y Fuentes SC recount relevant ESG risks and developments in the region, with particular focus on Mexico. In a post-pandemic world, the authors observe that ESG challenges are more visible. Especially given the lack of an internationally harmonised approach to ESG, the authors note how stakeholders in Latin America and elsewhere leverage tools to help identify ESG risks, while hopefully mitigating the dangers of green and social washing. The authors conclude by identifying best practices for effective ESG management, including ethical commitment and appropriate oversight, and how traditional compliance infrastructure can serve as a valuable foundation for ESG matters.
- Chapter 21: a team from Chevez, Ruiz, Zamarripa y Cía – Ana Sofía Ríos, Valentín Ibarra and Alejandra Pacheco – delves deeply into the constantly evolving fintech industry, highlighting recent changes in Mexico and associated opportunities and challenges. As relevant regulations proliferate, including with respect to data privacy and anti-money laundering, the authors suggest embracing technology to help strengthen compliance efforts. More broadly, given the strict regulations that govern fintech firms, the authors emphasise that strict compliance is essential to maintain customer, investor and regulator trust and to foster an environment in which the industry can thrive.

Looking ahead

Companies throughout the region (and world) naturally find themselves in different places in their compliance journeys. There is understandably a learning curve when it comes to compliance programmes, and companies often are learning in real time, as are prosecutors.

As this book illustrates, compliance is a continuing process of assessing risks in a dynamic environment amid ever-increasing regulatory expectations, and then crafting, implementing and refining strategies to mitigate these risks. Building effective compliance programmes and respecting the relevant laws help us to reach the desired destination, but these programmes and laws are the means and not the end.

On behalf of all the contributors, we sincerely hope that this book can serve as a valuable resource to the many compliance professionals, lawyers, business executives, board members, advisers, investors and others making this essential journey.

Andrew M Levine
Debevoise & Plimpton LLP
June 2023

Part I

Setting the Scene

CHAPTER 1

The Evolution of Compliance and Where it is Headed Next

Peter Spivack and Isabel Costa Carvalho[1]

Introduction

Corporate compliance is the focus of many corporations around the world these days, but compliance has not always been a priority. In the United States, compliance programmes have transformed during the past five decades from a passive, reactive approach to a proactive approach that seeks to harness big data to monitor and ensure compliance. This new decade favours an approach that considers not only traditional aspects of effective compliance programmes, but also incorporates new elements such as behavioural science, social responsibility and societal benefits.

The United Nations, the Organisation for Economic Co-operation and Development (OECD), the World Bank and other multilateral organisations have sought to promote compliance programmes as part of economic development. The United States and other nations have similarly incorporated law enforcement cooperation and compliance enhancement as part of their diplomatic strategies. These efforts have slowly taken hold. Prior to 2014, there was minimal awareness pertaining to corporate governance in Latin America. *Operation Car Wash*, the largest anti-corruption investigation in Latin America, which spread across the region, was a catalyst for countries in the region to focus their attention on compliance and its effects.

---

1 Peter Spivack and Isabel Costa Carvalho are partners at Hogan Lovells. The authors gratefully acknowledge the considerable assistance of Rafael Szmid and Jessica Bigby, senior associates at Hogan Lovells.

Despite these advancements, there have also been some setbacks, with some relevant gains made since *Operation Car Wash* being reversed or overlooked due to political pressures. For instance, in Brazil, we have seen attempts to roll back many of the anti-corruption measures implemented in recent years by the Congress and Court decisions. This has led to a decline in public trust and a general sense of uncertainty regarding the ability of Latin America governments to fight corruption in the long term.

This chapter reviews the evolution of compliance from the 1970s until today in the United States and Latin America. It traces how compliance programmes have evolved from being considered a luxury to becoming a necessity, especially for leniency in corporate prosecutions.[2] It also shows that constant vigilance is a necessity to keep corruption in check, especially in Latin America.

1970s and 1980s: accounting compliance and accountability

In the United States, the 1970s was a decade riddled by scandal. An investigation by the US Securities and Exchange Commission (SEC) revealed that hundreds of US companies – including some of the most widely known and respected – bribed foreign officials to further their business interests. Corporations across a wide range of industries chose to remediate mistakes internally instead of correcting and reporting the errors. In response, the Foreign Corrupt Practices Act (FCPA) was signed into law in December 1977.

In the 1980s, there was an emphasis on ethics, specifically in the defence and healthcare industries, that required government contractors to adhere to stringent rules. It was not until a decade later, as corporations began to be held liable and be prosecuted for the criminal acts of their employees and agents, that corporations paid greater attention to proactive compliance programmes. Before this, corporate compliance was largely addressed passively through codes of conduct and value statements that were provided to employees or hung on walls but carried little weight.

1990s: expansion of corporate liability

In the United States, corporate criminal liability can be traced back to respondeat superior, a legal doctrine commonly used in tort law. Respondeat superior requires that corporations take responsibility for the acts of their employees and agents if the acts occur within the scope of employment or agency, even if

2 See Chapter 4, 'Developing a Robust Compliance Programme in Latin America' by Brendan P Cullen and Anthony J Lewis.

contrary to organisational policy and training. Under early case law, a corporation was considered to be a legally fictitious entity, incapable of forming the mens rea necessary to commit a criminal act. The Supreme Court ultimately rejected this notion in 1909 in *New York Central & Hudson River Railroad v. United States*.[3] (Notably, this concept of a legal person not being subject to criminal liability was also recognised in most civil code countries. As discussed below, that legal doctrine is also changing in countries such as Brazil, Argentina and Colombia.)

The modern notion of corporate criminal liability was established in *United States v. Hilton Hotels Corp*.[4] This case established that corporations can be liable for the criminal activity of its employees and agents even if the employee or agent acted contrary to the corporation's policies or an officer's direction, as long as the employee or agent acted within the scope of his or her apparent authority and with the intent – even if only in part – to benefit the corporation.

Despite a corporation's best efforts to prevent criminal conduct within the organisation, corporate prosecution could bring forth financial and reputational ruin, as well as negatively affecting the morale of the corporation's employees.

To address this institutional vulnerability and incentivise corporations to exemplify good corporate citizenship, as well as to provide a means to rehabilitate corporations that have engaged in criminal conduct, the United States Sentencing Commission developed the Federal Sentencing Guidelines for Organizations (the Organizational Guidelines). These Guidelines signalled to corporations that the corporate code of conduct and value statements established decades ago were no longer sufficient by themselves to reduce penalties. The Guidelines recognise that an effective compliance programme is necessary to prevent and deter corporate criminal activity.

Federal Sentencing Guidelines for Organizations

The Federal Sentencing Guidelines for Organizations apply to corporations, partnerships, non-profit entities, workforce unions, government units, pension funds and trusts. They address two key elements of sentencing: just punishment and deterrence.[5] Just punishment intends to justly reflect the offender's degree

3 212 US 481 (1909).

4 467 F.2d 1000 (9th Cir. 1973).

5 US Sentencing Commission, Guidelines Manual, § 8 (November 2018), https://www.ussc.gov/guidelines/2018-guidelines-manual.

of blameworthiness; deterrence offers incentives for organisations to detect and prevent criminal acts. These Guidelines lay out the minimum criteria for an effective corporate compliance programme, under which an organisation must:

- establish standards and procedures to prevent and detect crime;
- provide oversight by high-level management, typically the board of directors;
- exercise due care in delegating substantial discretionary authority;
- establish effective communication and training for all employees;
- monitor, audit and report suspected wrongdoing, and periodically evaluate the effectiveness of the ethics and compliance programme;
- promote and consistently enforce the corporate compliance programme by incentivising use of the established mechanisms, and disciplining employees who commit crimes or fail to take reasonable steps to prevent or detect criminal conduct; and
- take reasonable steps to respond to criminal conduct once it has been detected and to prevent further criminal conduct.

Corporate compliance programmes

The most effective compliance programmes are those tailored for particular companies. However, a typical programme includes the key elements required by the Organizational Guidelines. In practical terms, the following are necessary: the endorsement and commitment of senior management, the appointment of a responsible officer to run the programme, risk assessment, relevant policies and procedures, training, certification of compliance with the rules and procedures of the programme, internal financial controls, due diligence of business partners, reporting mechanisms, investigation protocol, a progressive discipline policy, periodic auditing, monitoring, assessments of effectiveness and trend analysis. The Guidelines deliberately do not address the implementation of compliance programmes to provide organisations with the flexibility to design a programme that is best suited to their needs and particular industry.[6]

---

6 The following is an example of an industry-specific compliance programme. The Office of Inspector General (OIG) for the US Department of Health and Human Services issued a series of voluntary compliance programme guidance documents specifically tailored to the healthcare industry. The initial guidance, issued in 1997, applied to clinical laboratories, seeking to safeguard them from fraud and abuse. A year later, the OIG issued guidance aimed at hospitals, nursing homes, durable medical equipment suppliers and third-party billers. The 1998 guidance supports the development and use of internal controls to promote compliance with applicable US federal and state law, federal and state programme requirements, and private health plans. The model compliance programme should, as a minimum, include: written policies and procedures that emphasise a commitment to

Corporate compliance programmes are likewise important because of the liability a corporation and its officers can face. *In re Caremark*[7] established a duty at the board of directors level to ensure companies had reporting systems in place to detect, prevent and mitigate violations of law. Courts view the Organizational Guidelines as powerful incentives for corporations 'to have in place compliance programs to detect violations of law, promptly to report violations to appropriate public officials when discovered, and to make prompt, voluntary remedial efforts'.[8] Officers can breach their fiduciary duty if they intentionally disregard red flags that should alert them to fraudulent activity within their corporation.[9] Note, however, that officers can be civilly liable for unintentional actions as well.[10]

2000s: reaction to financial scandals and economic crisis

The start of the millennium brought fraudulent accounting scandals that resulted in bankruptcy for corporate giants Enron and Worldcom, and Enron's auditor, accountancy firm Arthur Andersen. Enron and Worldcom were prosecuted for falsifying balance sheets to inflate earnings. These acts eroded investors' confidence and the Sarbanes-Oxley Act of 2002 (SOX) was enacted to provide investors with a slate of protections from future wrongdoings.

Securities and Exchange Commission

In October 2001, the SEC issued a Report of Investigation and Statement (known as the Seaboard Report) explaining its decision not to take enforcement action against a public company it had investigated for financial statement irregularities. In this Report, the SEC articulated an analytical framework for evaluating cooperation by companies. In respect of compliance programmes, the Report

---

compliance; designation of an officer charged with the development and monitoring of compliance programme training for all employees; a hotline to receive complaints; policies and procedures to ensure the anonymity of complainants and to protect whistleblowers from retaliation; audits or a similar mechanism to monitor compliance and to detect and prevent crime; and disciplinary policies to address potentially criminal misconduct. See Federal Register, Vol 63, No. 35, February 23, 1998, https://oig.hhs.gov/authorities/docs/cpghosp.pdf.

7 698 A.2d 959 (Del. Ch. 1996).

8 *id.*, at 982.

9 *McCall v. Scott*, 239 F.3d 808, 819 (6th Cir. 2001).

10 *id.*, at 817 ('unconsidered inaction can be the basis for [officer] liability because . . . ordinary business decisions . . . can significantly injure the corporation and make it subject to criminal sanctions'); but see *Dellastatious v. Williams*, 242 F.3d. 191, 196 (4th Cir. 2001) (holding that officers can avoid liability by making a good-faith effort to have a reporting system).

stressed the importance of '[s]elf-policing prior to the discovery of the misconduct, including establishing effective compliance procedures and an appropriate tone at the top' and '[r]emediation, including dismissing or appropriately disciplining wrongdoers, modifying and improving internal controls and procedures to prevent recurrence of the misconduct, and appropriately compensating those adversely affected'.[11]

Sarbanes-Oxley Act of 2002

The United States Congress soon saw an opportunity to include compliance measures in legislation borne out of a series of financial crises. SOX is a federal law that addresses corporate fraud. Named after its sponsors, Senator Paul Sarbanes, D-Md and Congressman Michael Oxley, R-Ohio, SOX is primarily enforced by the SEC, and its main goal is to increase corporate responsibility and protect investors. Many companies in Latin America have sought access to the US capital markets and, as a result, have become familiar with SOX compliance.

SOX holds corporate officers responsible for transparent and accurate financial accounting and timely reporting of violations. The Act mandates that chief executive officers and chief financial officers acknowledge responsibility for the accuracy, documentation and submission of all financial reports to the SEC. Management is responsible for internal control of financial records and flaws within this reporting. SOX requires corporations to develop, communicate and enforce formal data security policies for all financial data that is stored and used. Corporations must document, continuously update and remain compliant with SOX requirements. SOX also mandates annual audits and requires external auditors to attest that a corporation's internal controls regarding financial records are appropriate. Both results of annual audits and certification by management and attestation by external auditors must be made available to stakeholders.

SOX also includes a provision that protects whistleblowers at publicly traded companies. The provision encourages internal reporting by prohibiting retaliation against a whistleblower who provides information, causes information to be provided, or assists in an investigation of any conduct that the whistleblower reasonably believes should be reported to the SEC.

---

11 SEC Issues Report of Investigation and Statement Setting Forth Framework for Evaluating Cooperation in Exercising Prosecutorial Discretion' (2001), https://www.sec.gov/news/press/2001-117.txt.

Before the first decade was out, the United States suffered another financial crisis. In response, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank) was enacted. A major goal of Dodd-Frank was to protect the US economy from the collapse of financial institutions, such as was experienced in 2007 and 2008.

Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010

Dodd-Frank significantly reformed regulatory schemes by improving accountability and transparency in corporate accounting in an effort to promote financial stability. The Act forced improvements in corporate governance, such as executive compensation review, clawback and other provisions.

This law also expanded on the whistleblower protections created under SOX. Section 1057 of Dodd-Frank expanded the SOX protections to create a private cause of action for whistleblowers in the financial industry, lowered the burden of proof to prevail on a claim, extended the statute of limitations and rewarded prospective whistleblowers.

The most significant change in Dodd-Frank is that it amends the Securities Exchange Act of 1934 to provide a 'bounty' system for prospective whistleblowers.[12] The amended provisions financially reward whistleblowers who voluntarily report to the SEC 'original information' that leads to a successful recovery by the SEC as it relates to a violation of securities law. A whistleblower is eligible for an award of between 10 per cent and 30 per cent of the collected monetary sanctions in excess of US$1 million. The amended provision incentivises whistleblowers to report directly to the SEC at the same time as they report to the company through internal channels.[13]

The Dodd-Frank protections apply to publicly traded companies, subsidiaries and affiliates. Whistleblowers are protected when providing information about, or refusing to participate in, activity reasonably believed to be a violation of law under the SEC's jurisdiction. The burden of proof necessary to prevail is also reduced under Dodd-Frank. To prevail, the whistleblower must show by a preponderance of the evidence that protected conduct contributed to retaliation

12 This system is similar to that used in the Federal False Claims Act since its modernisation in 1986, with the express intent of increasing the incentives to report violative conduct to the US government.

13 In fiscal year 2019, approximately 480 whistleblower tips came from outside the United States, including Latin America, US SEC, 2019 Annual Report to Congress on the Dodd-Frank Whistleblower Program, Appendix C, https://www.sec.gov/files/sec-2019-annual%20report-whistleblower%20program.pdf.

against the whistleblower. To defeat the action, the employer must demonstrate by clear and convincing evidence that the employer's action against the whistleblower would be the same even if the employee had not reported the activity. The provision also prohibits pre-dispute arbitration, except when it is set forth in collective bargaining agreements.

Whistleblower provisions, as well as the prosecution of Arthur Andersen in the midst of the Enron scandal, moved the focus to the internal workings of an organisation. In part as a result of the collapse of Arthur Andersen following its prosecution, the corporate prosecutorial strategy of the US Department of Justice (US DOJ) shifted from the punishment of corporate conduct to the reform of corrupt corporate cultures. One way to assess a corporation from the inside out is through an external corporate monitor.

Corporate monitors

Now relatively common, the US DOJ required a corporate monitor for the first time in 2008.[14] Corporate monitors are required in a particular case as part of a plea or deferred prosecution agreement, usually when the US DOJ or the SEC (or both) believe that the corporate's compliance system is not adequately developed or mature. A corporate monitor is responsible for developing, maintaining and monitoring a corporation's compliance programme. As part of its Principles of Federal Prosecution of Business Organizations, the US DOJ considers corporate compliance programmes when making charging decisions.

2010s: voluntary disclosure and government enforcement of compliance

The 2010s highlighted a concerted effort to export compliance through public and private enforcement. In the United States, regulatory agencies created policies to incentivise corporations to develop effective compliance programmes, and corporations have increasingly understood the benefit of compliance. In fact, corporations without effective compliance programmes may suffer significant penalties. Organisational and regulatory agency guidance assists companies in developing and monitoring the effectiveness of compliance programmes, which, in turn, assesses risks and increases the likelihood of voluntary disclosure of violations. A summary of some of the more significant guidance is below.

14 See *United States v. Siemens Aktiengesellschaft*, Case No. 08-CR-367-RJL (D.D.C. 2008).

OECD Good Practice Guidance on Internal Controls, Ethics, and Compliance

In 2010, the OECD adopted good practice guidance to establish and ensure the effectiveness of compliance programmes and internal controls to detect and prevent foreign bribery in international business transactions. The guidance is similar to the components of effective compliance programmes in the United States and 'recognises that to be effective, such programmes or measures should be interconnected with a company's overall compliance framework'.[15]

Guidance on compliance

In 2020, the US DOJ and SEC updated its jointly issued 2012 guidance that made clear that in exercising judgement, prosecutors will look to determine whether the company had a compliance programme in place and whether there was a commitment by the company to make effective use of such a programme.[16] The US DOJ further elaborated on this guidance in its FCPA Corporate Enforcement Policy.[17] A strong demonstration of a company's compliance programme can help to change the structure of a resolution, moving it from a criminal charge

15 'Good Practice Guidance on Internal Controls, Ethics, and Compliance', https://oecd.org/daf/anti-bribery/44884389.pdf.

16 A Resource Guide to the US Foreign Corrupt Practices Act', https://www.justice.gov/criminal-fraud/file/1292051/download. (Key updates in 2020 guidance include a new definition of 'instrumentality of a foreign government' and a non-exhaustive list of factors to determine (1) whether an entity is controlled by the government, and (2) whether the entity performs a function that the government treats as its own, that the court articulated in *United States v. Esquenazi*, which involved a state-owned enterprise when designing its compliance programmes; further limits to FCPA's 'local laws defence'; and a clarification that the statute of limitations is five years for violations of anti-bribery provisions, but six years for violations of the accounting provisions. There are also revisions that are not changes but rather indications that DOJ and SEC continue to emphasise the importance of companies conducting pre-acquisition due diligence. DOJ and SEC also are still taking an expansive view of their jurisdiction over foreign companies and individuals for conspiracy and aiding and abetting offences, and companies' compliance efforts must reflect this.

17 The updated Guide also incorporates new principles and resources that inform DOJ's corporate enforcement decisions. DOJ continues to follow the department long-standing Principles of Federal Prosecution of Business Organizations, which provide factors to be 'considered in conducting an investigation, determining whether to charge a corporation, and negotiating plea or other agreements'. New to those factors is 'the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging or resolution decision'. In addition, the updated Guide includes the Anti-Piling On Policy, which influences how DOJ and SEC 'strive to avoid imposing duplicative penalties, forfeiture, and disgorgement for the same conduct', https://www.justice.gov/criminal-fraud/page/file/937501/download.

to a deferred prosecution agreement, and can reduce the compliance obligations, such as for an external monitor. [18] Moreover, even if a company is charged with a criminal violation of the FCPA, the Organizational Guidelines, which have considerable influence on the ultimate penalty imposed, provide for a mitigation of penalties if a company can demonstrate that the violation occurred in spite of an effective compliance programme.[19] These Guidelines apply to all corporate criminal conduct and not just FCPA violations.[20]

---

18 The costs of compliance failures have continued to ratchet up. In 2020, DOJ and SEC announced record-breaking penalties for FCPA violations. In January 2020, a major aerospace defence contractor agreed to pay US$3.9 billion in global penalties for foreign bribery and International Traffic In Arms Regulations (ITAR) violations. Nine months later, in November 2020, a major investment bank was charged with a US$2.9 billion joint DOJ and SEC enforcement action for FCPA violations including conspiracy to violate the FCPA anti-bribery provisions, internal accounting controls, and books and records provisions of federal securities laws. The investment bank allegedly engaged in a conspiracy to pay more than US$1.5 billion to multiple high-level officials. Notably, although the investment bank had a comprehensive anti-corruption and compliance programme, the DOJ and SEC found its internal controls to be deficient because both high- and low-level employees were able to circumvent the controls and engage in corrupt activities.

19 US Sentencing Commission, Guidelines Manual, § 8 (November 2018), https://www.ussc.gov/guidelines/2018-guidelines-manual.

20 For Latin American countries and other countries that wish to do business with the US government, the Federal Acquisition Regulation (FAR) establishes other requirements. The FAR prioritises ethics and compliance throughout the federal procurement process, from solicitation to execution of the awarded contract, and embodies the US government's policy of dealing with only 'presently responsible' contractors. Government contractors must develop and maintain a compliance programme within 30 days of award. The programme must be in writing, available to all employees on the contract, and contain mechanisms to report violations; further, violations must be reported in writing to the contracting officer or the Office of Inspector General for the US Department of Health and Human Services in a timely manner. Solicitations and contracts expected to exceed US$5.5 million in value and 120 days in performance are required to include the Contractor Code of Business Ethics and Conduct clause in the documentation. To be compliant with the FAR, it is not enough to conduct only due diligence. The FAR views compliance programmes as a good judge of a government contractor's character and an effective compliance programme may lead to contract awards. There is also no excuse for omitting a required clause in contracting documents. The Christian Doctrine states that if the FAR requires a clause to be in a contract, it is considered a requirement regardless of whether it is actually in the contract. In 2015, seven years after mandating compliance programmes, the FAR added a human trafficking requirement relevant to government contracting overseas. Supplies acquired and services performed overseas in excess of US$500,000 require that contractors certify compliance and monitoring of human trafficking issues. Importantly, government contractors may be liable for the actions of all contractors, subcontractors and agents

In January 2023, US DOJ revised its Corporate Enforcement Policy (CEP) seeking to increase the incentives to corporations to voluntarily self-disclose misconduct and cooperate with government investigations. Under the revised policy, even companies with aggravating circumstances may be eligible for a declination under the CEP and reduced penalties if they satisfy three factors:

- the voluntary self-disclosure was made immediately upon the company becoming aware of the allegation of misconduct;
- at the time of the misconduct and the disclosure, the company had an effective compliance programme and system of internal accounting controls that enabled the identification of the misconduct and led to the company's voluntary self-disclosure; and
- the company provided extraordinary cooperation with the Department's investigation and likewise undertook extraordinary remediation.[21]

Under specified circumstances, the revised CEP allows companies to avoid the most serious consequences – a corporate guilty plea and an external compliance monitor – even if aggravating factors such as a prior criminal enforcement action or pervasive misconduct are present.[22]

US DOJ compliance guidance

Corporations have been rewarded for effective compliance programmes for decades, and the US DOJ expects that corporations ensure their compliance programmes are strong. As announced in 2020, there is a focus on individual responsibility and accountability. The US DOJ takes a wider view of companies' past wrongdoing, requires more detailed information on individuals related to

21 United States Department of Justice, Assistant Attorney General Kenneth A Polite Jr Delivers Remarks on Revisions to the Criminal Division's Corporate Enforcement Policy (17 January 2023), https://www.justice.gov/opa/speech/assistant-attorney-general-kenneth-polite-jr-delivers-remarks-georgetown-university-law; United States Department of Justice, Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy (January 2023), https://www.justice.gov/opa/speech/file/1562851/download.

22 *id.*, in cases where a criminal resolution is still warranted, a corporation that voluntarily self-discloses can receive up to a 75 per cent reduction in penalties (up from a maximum of 50 per cent). Absent particularly egregious circumstances and an ineffective compliance programme, a corporate guilty plea and corporate monitorship is not required. For corporations that do not voluntarily self-disclose but still cooperate and remediate, prosecutors can recommend up to a 50 per cent reduction in penalties (up from a maximum of 25 per cent).

actions in question and allows for the broader use of corporate compliance monitorships. Companies will need to be able to demonstrate their internal efforts to detect, prevent and mitigate fraud should an issue come to light.

The US DOJ's updated compliance programme guidance announced in March 2023[23] focuses on the company's policies and procedures governing the use of personal devices, communications platforms and messaging applications (including ephemeral messaging applications), and whether such policies are tailored to the company's risk profile, specific business needs, and ensures that to the greatest extent possible, business-related data and communications are accessible and amenable to preservation by the company. US DOJ also looks to how these policies are communicated to employees, as well as whether they are enforced on a consistent and regular basis. [24]

US DOJ's recent changes also include the creation of a three-year pilot programme (the Programme), beginning in March 2023, meant to reward corporations with compliance-promoting bonus and compensation programmes.[25] The Programme notes three non-exclusive criteria that may be required to receive credit, including: (1) a prohibition on bonuses for employees who fail to satisfy compliance requirements; (2) disciplinary measures for employees who violate applicable law, as well as for knowing or willfully blind supervisors of these employees; and (3) incentives for employees fully committed to the compliance process. In requiring such criteria as part of a corporate resolution, federal prosecutors have discretion to consider applicable foreign and domestic laws. The Programme offers potential fine reductions to corporations that attempt to claw-back money from employees who committed the wrongdoing.[26] US DOJ also has discretion to provide a 25 per cent reduction in the fine if the corporation made a good faith but unsuccessful attempt to recoup the compensation. Time will tell how this Programme plays out, but corporations must now account for this new framework in their compliance programmes.

---

23 https://www.justice.gov/criminal-fraud/page/file/937501/download.

24 *id.*

25 Deputy Attorney General Lisa Monaco Delivers Remarks at American Bar Association National Institute on White Collar Crime, https: //www.justice.gov/opa/speech/deputy-attorney-general-lisa-monaco-delivers-remarks-american-bar-association-national (March 2023)

26 *id.*

Harnessing big data: the rise of data analytics in compliance programmes

Compliance is a top priority for corporations today, and they are now harnessing internal data to monitor employees and increase the effectiveness of compliance programmes.[27] Data analytics help compliance personnel within corporations to identify patterns that human beings cannot recognise, improve the way risk is managed and respond quickly to developing compliance issues. Of course, data analytics are only as effective as the data inputs and analytical outputs. Although this technique is a useful tool, it is not a replacement for a well-integrated compliance programme.

Soft skills and integrity

This new decade ushers in an approach that considers not only traditional aspects of effective compliance programmes but must also incorporate social responsibility and societal benefits. The new approach requires corporations to move beyond the letter of the law or actions within corporate policy, and view compliance as a benefit for society.

Environmental, social and corporate governance factors

A corporation's financial performance drives its business decisions. Corporate officers focus on hard numbers to determine success. The new approach asks these officers to look beyond the data and to environmental, social and corporate governance (ESG) factors to strengthen financial performance and compliance. ESG factors, such as how a corporation responds to climate change, how effective health and safety policies are at preventing accidents, and how good the corporation is at building trust and fostering innovation, are not traditionally calculated in a financial analysis, but adherents are advocating that they have relevance and financial impact.

ESG is different from the movement to motivate corporations to be more socially responsible. Unlike social responsibility, which examines what corporations will not do (such as sell firearms), investors evaluate a corporation's ESG to understand its purpose and value. Using this information, investors make decisions about where to invest. For this reason, the financial effects of ESG factors can be significant.

---

27 See Chapter 11, 'Why Fresh Perspectives on Tech Solutions Are Key to Evolving Data-Driven Compliance Monitoring' by Martín Sánchez, Gabriel Calvillo, Adriana Morales and Paula Pérez Benítez.

Renewed focus on anti-corruption and coordination among national enforcement authorities

In 2021, the Biden administration conveyed its focus on anti-corruption efforts, established that anti-corruption is a national security interest, and issued the first ever US Strategy on Countering Corruption (the Strategy). The Strategy is a five-pillar framework:

- modernising, coordinating and resourcing US government efforts to fight corruption;
- curbing illicit finance;
- holding corrupt actors accountable;
- preserving and strengthening multilateral anti-corruption architecture; and
- improving diplomatic engagement and leveraging foreign assistance resources to advance policy objectives.

This framework reflects the government's broader-lens approach to understand and stop corrupt activity and signals increased scrutiny for corporations.[28]

Shortly after the Strategy was issued, the OECD adopted a comprehensive series of recommendations for Member States and for OECD Anti-Bribery Convention signatories to integrate into their legal frameworks to combat foreign bribery of public officials. The recommendations include strengthening enforcement of foreign bribery laws, addressing the demand side of foreign bribery, enhancing international cooperation, introducing principles on the use of non-trial resolutions in foreign bribery cases, incentivising anti-corruption compliance by companies, and providing comprehensive and effective protection for reporting persons.[29]

One trend that the pandemic has reinforced is the cooperation among national enforcement authorities and across borders.[30] Multinational corporations must be prepared for investigation by jurisdictional authorities as well as coordination among other enforcement officials as parallel inquiries proceed.

---

28 The Biden administration also committed to rooting out anti-corruption in Latin America by forming the Northern Triangle Anticorruption Task Force. This task force investigates and prosecutes asset recovery related to corruption through FCPA enforcement, counter-narcotics prosecutions, and the Kleptocracy Asset Recovery Initiative, which focuses on recovering assets gained from foreign corruption and prosecuting money laundering.

29 https://www.oecd.org/daf/anti-bribery/2021-oecd-anti-bribery-recommendation.htm.

30 'Since the covid-19 outbreak, different jurisdictions have constructively enacted and promulgated laws, regulations, acts and orders to ensure that they are sufficient to strengthen supervision over the implementation of compliance on enterprises and individuals within each jurisdiction . . . the promulgation of these laws and regulations

Compliance in Latin America

As has been noted, until the beginning of 2010s, compliance was merely a secondary concern for companies in Latin America, seen as a superfluous investment with uncertain incomes. Without effective enforcement at the local level combined with a high level of legal uncertainty – and even a degree of impunity – companies were less likely to invest in compliance as they did not view it as a priority or were concerned about the potential consequences of non-compliance. Even for companies subject to international anti-corruption laws, such as the FCPA and UK Bribery Act, compliance was often in place just as a paper programme without sufficient human and financial resources.

However, this situation began to change at the end of 2014 with the launch of *Operation Car Wash*. Although Brazil passed its anti-corruption law (the Clean Company Act) in late 2013, *Operation Car Wash* was the decisive turning point that transformed the fight against corruption in Brazil and across Latin America. This massive anti-corruption investigation was responsible for 295 arrests, 1,450 dawn raids, and 4.3 billion reais in ill-gotten gains being returned to the Brazilian state.[31] As a result, the perception of the need for compliance policies also changed.

Operation Car Wash is the most extensive anti-corruption investigation in Latin America, focused on bribery schemes surrounding infrastructure projects and involving a series of construction companies, public officials and politicians. It is a cross-border investigation that exposed the corruption of public officials from several Latin American countries in addition to Brazil, including Argentina, Chile, Colombia, Dominican Republic, Ecuador, Mexico, Panama, Peru and Venezuela.

The compliance notions in Latin America were modified by two main elements of *Operation Car Wash*. The first was the fact that media attention put a red flag on investments in the region, which required a change of approach, especially by Latin American companies, to recover market confidence. The second was the international cooperation in investigations, resulting in multilateral agreements with rigid clauses, promoting the 'regulation by enforcement' in compliance rules.

---

also provides guidance to companies while encountering cross-border investigations and responding to the law enforcement movement from other jurisdictions from different perspectives.' https://globalinvestigationsreview.com/review/the-asia-pacific-investigations-review/2022/article/china-related-cross-border-government-investigation-after-the-covid-19-pandemic.

31 https://www.mpf.mp.br/grandes-casos/lava-jato/resultados.

With *Operation Car Wash*, several cross-border violations became public and resulted in close cooperation between Brazilian and foreign authorities. As the investigation by US authorities into Latin American companies continued, the companies were forced to seek agreements with their own local authorities as well. Three leading cases that led to cooperation between the US DOJ, the SEC and Brazilian authorities were Petróleo Brasileiro SA (Petrobras), Eletrobras – Centrais Elétricas Brasileiras SA (Eletrobras) and Construtora Norberto Odebrecht SA (Odebrecht). In all three cases, companies were subject to FCPA regulations as well as Brazil's Clean Company Act since they are public entities listed on the New York Stock Exchange or had conducted business in the United States.

In addition to strengthening dialogue and cooperation between countries to build a global anti-corruption environment, these cases introduced new preventive, mitigation and disciplinary measures, creating a cross-regulation by enforcement. The imposition of corporate monitors is a clear example of innovation gained from this cooperation. A dual monitorship (i.e., the appointment of monitors from the United States and Brazil) was included in the settlement agreed between the US authorities and Odebrecht. Although it was not provided as a sanction in most Latin American compliance legislation, this alternative is currently on the radar of the local authorities[32]. Since then, corporate monitors have been increasingly utilised by Latin American authorities in both transnational and local investigations. The main challenge of using such monitors in this region arises from the prevalence of family-owned businesses, legal uncertainty and spread out corruption, which create unique complexities. As a result, government authorities must consider the local particularities to incentivise companies to embrace corporate monitors.[33]

On 1 February 2021, after 79 action plans (or their so-called phases with their hand-picked names), *Operation Car Wash* was formally dissolved as a task force in Brazil. However, the remaining and related, and upcoming corruption cases continued to be closely investigated under the leadership of the permanent team called Special Group for the Fight Against the Organized Crime of the Federal Public Prosecutor's Office. Some members of the former group, including its head, have transitioned to the special group.

---

32 See 'SZMID. Rafael. Monitores Corporativos Anticorrupção no Brasil: Um Guia para sua Utilização no Processo Administrativo e Judicial,' Quartier Latin, 2021.'

33 *id.*

Ultimately, *Operation Car Wash* put a spotlight on the weakness of compliance regulation and enforcement in Latin America, which resulted in a call for change. The response was the disruption of the current schemes and a movement to establish control measures. In Brazil, for example, participation in public tenders requires having a robust compliance programme addressing non-interference of the competitive nature of public tenders. Anti-corruption laws enacted in Mexico in 2016 (General Law of Administrative Responsibility) and Argentina (Corporate Criminal Liability Law) in 2018 followed the Brazilian Clean Company Act in including similar requirements regarding undue non-interference in public bids. In fact, bid rigging has become a hot topic in Latin America. Many countries in the region have large public sectors and rely heavily on government contracts for procuring goods and services, making them particularly vulnerable to bid rigging.

Compliance guidelines in Brazil

Although inspired by the FCPA, Brazil's Clean Company Act is broader in certain respects than the US requirements, extending to local officials and conduct against public administration, such as fraud in the public tender process and bid rigging.

The Clean Company Act forbids direct and indirect, active and passive bribery of local and foreign public officials, including the concealment and the use of intermediaries to engage in bribery. It also forbids fraud in public bids and obstruction of government investigations. It imposes civil and administrative strict liability for violations by an entity's directors, officers, employees and agents when acting on behalf of the entity.

While the Clean Company Act outlines specific corruption violations, it was its supplementary law (Decree No. 8,420), issued in 2015, that initially provided details about corporate liability, penalties and mitigating measures – including fines, public disclosure of violation and debarment from contracting with government entities for violations. Besides setting benefits relating to collaboration in investigations through leniency agreements, Decree No. 8420 provided for the existence of an effective compliance programme as the primary defence and mitigating measure.

Decree No. 8,420 defined a compliance programme as a set of internal integrity and audit mechanisms, policies and guidelines to detect and remedy deviations, fraud, irregularities and unlawful acts committed against national or foreign public administration, and procedures for reporting irregularities and effectively enforcing codes of ethics and conduct. According to Decree No. 8420,

a compliance programme must be tailored, implemented and updated following the peculiarities and risks of the entity, and to ensure its continuous improvement and effectiveness.

To be considered as a defence, a compliance programme would be evaluated according to several parameters, as outlined by Decree No. 8,420:

- Tone at the top: the commitment of senior management, including board members, who must show unequivocal and public support for the compliance programme.
- Implementation of internal policies: standards of conduct, codes of ethics, integrity policies and procedures shall apply to all employees and managers regardless of their position or function.
- Third-party policies: policies for hiring, selecting and monitoring of third parties, due diligence procedures and risk matrix. In addition, third parties must be provided with the code of ethics and other applicable standards of conduct in force at the company.
- Training: periodic training that is tailored to the target audience.
- Periodic risk assessment: regular risk analysis to identify risks and to implement improvements.
- Internal control: accurate and precise accounting records and information, and maintaining effective internal controls for financial reports and statements.
- Specific policies concerning interaction with public officials: specific policies and procedures to prevent fraud and illicit conduct relating to bidding processes, execution of contracts with public entities, obtaining licences, and other interaction with public officials, including interactions intermediated by third parties.
- Responsible officer: independence, sufficient powers and adequate human and financial resources available to the internal body responsible for the implementation and enforcement of the compliance programme.
- Reporting channels: effective channels for reporting violations, based on non-retaliation and confidentiality, which shall be clearly and widely disclosed to employees and third parties.
- Disciplinary measures: policies on internal investigations and enforcement of disciplinary measures for violations.
- Remediation and mitigation: procedures that ensure the prompt interruption of violations when they are detected and the timely remediation of the damage generated.

On 12 July 2022, the Brazilian federal government enacted Decree No. 11,129/2022, which revoked Decree No. 8,420/2015. Decree No. 11,129/2022 outlines relevant changes in parameters that were included in the former Decree No. 8,420/2015, as well as incorporates numerous provisions that have already been included in resolutions, normative acts and internal guidelines of the Office of the Comptroller General in Brazil (CGU) and the Brazilian Federal Attorney's General Office (AGU), in addition to new provisions.

In relation to the parameters for assessing the effectiveness of integrity programmes, in addition to the parameters provided under Decree No. 8,420/2015, the new Decree No. 11,129/2022 outlines the:

- inclusion of a provision to 'foster and maintain a culture of integrity within a company's environment';
- proper resource allocation so that an integrity programme demonstrates the tone at the top;
- implementation of periodical communication actions by companies in addition to training;
- in addition to a commitment to undertake risk analysis, companies should implement 'adequate risk management, including its analysis and periodic reassessment' to enable 'necessary adaptations to its integrity program and efficient allocation of resources';
- inclusion of agents, consultants, commercial representatives and associates within the description of third parties for the purpose of conducting appropriate due diligence upon their hiring and supervision;
- inclusion of politically exposed persons and their family members, close collaborators and companies that they are part of, for the purposes of conducting appropriate due diligence upon their hiring and supervision;
- need to conduct due diligence and implementation of mechanisms for sponsorships and donations supervision;
- implementation of procedures for the treatment of complaints originating from hotlines
- inclusion as a parameter for evaluating the adequacy of an integrity programme, in addition to the number of employees (i.e., size of the company): (1) revenues to be taken into consideration whether the company is a micro or small business; and (2) the corporate governance structure (number of departments, structure and governing bodies, etc.); and
- simplified evaluation for micro and small companies.

In October 2015, the CGU published its Integrity Programme: Guidelines for Private Legal Entities (the CGU Guidelines). These Guidelines summarised the 'five pillars' of a strong Integrity Programme according to CGU:

- the commitment of senior management;
- an internal department responsible for the Integrity Programme;
- profile and risk analysis;
- the structuring of rules and instruments; and
- continuous monitoring strategies.

Besides the Brazilian legislation, the CGU Guidelines reference the UK's Bribery Act Guidance, the OECD's Good Practice Guidance on Internal Controls, Ethics and Compliance, the UN's An Anticorruption Ethics and Compliance Programme for Business: A Practical Guide, the US Sentencing Commission's Guidelines Manual and The Complete Compliance and Ethics Manual published by the Society of Corporate Compliance and Ethics.

Compliance guidelines in Colombia

Following the enactment of Brazil's Decree No. 8,420, Colombia, Mexico, Peru and Argentina also provided specific compliance standards. In general, those provisions are very similar to the FCPA and Brazil's Clean Company Act, but with particular nuances concerning the extension of requirements, enforcement and gradation of mitigation for liability.

On 2 February 2016, Colombia enacted Law No. 1,778 (the Transnational Corruption Act), in which anti-corruption mechanisms are set as relevant criteria for calculating penalties for violations. According to the Transnational Corruption Act, private companies that maintain transnational businesses and act under the supervision of the Colombian Superintendence of Corporations shall adopt compliance programmes, which shall provide internal anti-corruption mechanisms, audit policies and preventive measures, and promote transparency.

Similar to Decree No. 8420, Colombia enacted Resolution No. 100-000003 (the Transnational Corruption Act Compliance Guidelines), on 26 July 2016, to guide the implementation of compliance programmes, based on three basic principles:

The compliance programme shall be tailored based on the particular risks of each entity. Accordingly, risk assessment must be undertaken based on (1) transparency risks from the country involved in the transnational operation, (2) the specific sector – taking into consideration that energy, infrastructure and healthcare require stronger controls – and (3) the level of interaction with third parties.

Senior management shall endorse a commitment to a culture of ethical behaviour and lead measures to avoid transnational bribery and other corrupt violations.

Control mechanisms, due diligence procedures and periodic audits should be established to ensure the effective detection of violations and undertaking of mitigation actions.

Following these principles, the compliance programme shall:

- provide written compliance policies, and the code of conduct shall summarise and detail all relevant standards of conduct provided in those policies. The policies shall be translated into the language of the countries with which the company maintains transnational transactions;
- ensure wide disclosure of the compliance programme and clear communication of its requirements;
- conduct robust and periodic risk assessment concerning the hiring of third parties (due diligence) and performance of the compliance programme;
- train employees and assign responsibility, including members of senior management and boards, to detect, prevent and mitigate violations;
- implement internal control mechanisms and audit procedures to ensure precise accounting records and information; and
- require specific formal commitments concerning ethics, audit rights and termination from high-risk third parties.

To expand compliance guidelines beyond transnational operations, Colombia's Secretary of Transparency introduced a Register of Active Companies in Anti-Corruption (EAA) to promote internal best practice and prevent corruption. The EAA uses nine categories to assess the compliance programmes of private entities:

- risk assessment;
- corporate organisation and responsibilities;
- policies tailored to specific high-risk areas;
- the programme's implementation;
- financial and internal controls;
- communication and training;
- human resources policies;
- reporting of policy procedures; and
- compliance programme audit system.

Recently, following OECD guidelines,[34] Colombia has enacted two new provisions to enhance monitoring and enforcement. First, on 16 October 2020, Colombia Enacted Decree No. 1,358, which determines the debarment from public procurement procedures and public finance sources companies convicted for corruption. In addition, on 26 June 2021, Colombia enacted Decree No. 830, which includes specific guidelines related to public exposed persons (PEPs), and certain reporting obligations for and the establishment of a public registry of PEPs.

Colombia enacted its Anti-Corruption Statute in 2011 focusing on punishing individuals for corruption. In 2013, Colombia joined the OECD Anti-Bribery Convention. After some years, Colombia accepted OECD's recommendations and enacted, in 2016, a law that included corporate responsibility and effective prosecution against legal entities, leniency programmes and the obligation to adopt compliance programmes.

Compliance guidelines in Mexico

The wave of change to Mexico's legal framework against corruption started with the Constitutional Reform of 7 February 2014, which introduced transparency obligations relating to the access of information. Then, the launch of the National Anticorruption System on 27 May 2015 resulted in the enactment of a series of anti-corruption provisions.

In addition, on 18 July 2016, the General Law of Administrative Responsibility (GLAR) was enacted with the purpose of outlining compliance obligations. GLAR is very similar to Brazil's Clean Company Act and prohibits the payment of bribes to public officials, bid rigging, improper interference in public procurement processes and contracts, and other corruption violations.

Similarly, to the Brazilian and Colombian legislation, GLAR establishes that a compliance programme may be a mitigating factor of liability, provided it meets the following minimum requirements:

- to provide clear information about the organisational structure and reporting lines;
- to establish and widely discloses a code of conduct, which shall include and detail standards of ethics and procedures;

34 See the Phase 3 Two-Year Follow-up Report: Colombia, which assesses the progress made by the country concerning the implementation of the OECD anti-bribery convention and the actions it needs to be adopted to comply with it fully (https://www.oecd.org/daf/anti-bribery/Colombia-phase-3-follow-up-report-en.pdf).

- to provide adequate control, compliance and audit systems to support regular and periodic reviews of the performance of the compliance programme;
- to maintain robust hotline channels, both internally and outside the entity, and policies on investigation proceedings and disciplinary measures;
- to conduct periodic training;
- to provide human resources staff with policies and training to prevent the hiring of high-risk individuals; and
- to provide mechanisms to enhance transparency within the entity.

On 1 July 2020, the United States–Mexico–Canada Agreement (USMCA) entered into force, replacing the North America Free Trade Agreement (NAFTA) and creating a new landmark in the regional fight against corruption. Unlike NAFTA, USMCA has a chapter establishing obligations on anti-corruption efforts to benefit the three parties alike, entitled 'Transparency and anti-corruption', whose primary drive is to fight international trade and investment corruption. In addition, it provides a detailed framework for preventing and combating corruption and internal controls by requiring the countries to adopt, maintain and enforce anti-corruption measures aimed to criminalise failures regarding books and records accounting provisions and other corporate governance aspects and determining proper whistleblower protections to be put in place.[35]

Compliance guidelines in Peru

The Peruvian anti-corruption legislation (the Corporate Administrative Liability Law) was enacted on 1 April 2016 as a corporate liability extension of the crime of corruption provided in the Criminal Code. Later, in 2017, Law No. 30,424 was amended, extending such liability to other crimes, including active bribery of domestic public officials.

Under the Corporate Administrative Liability Law, the existence of an effective compliance programme can exempt an entity of penalties for a corruption violation. An effective compliance programme as outlined by the Law is significantly more straightforward than those required by legislation in other Latin American countries.

According to the Corporate Administrative Liability Law, to be regarded as 'an effective preventive mechanism', the compliance programme shall:

35 See Agreement between the United States of America, the United Mexican States, and Canada, Chapter 27, Article 27.3.

- properly map and identify an entity's activities and procedures concerning risks of corruption, money laundering and terrorism, and other violations provided in the Criminal Code;
- establish preventive policies and procedures;
- identify management, audit and accounting policies and procedures that may prevent corruption violations; and
- provide reporting mechanisms, investigative protocols and disciplinary measures.

Another milestone in the fight of the Peruvian government against corruption was the criminalisation of private corruption – approved in 2018 – that also had a great impact on the business environment.

Compliance guidelines in Argentina

Law No. 27401 (the Corporate Criminal Liability Law) was enacted on 2 March 2018 to join Latin America's efforts against corruption. It provides for local and transnational corruption violations, including bribery of public officials, fraudulent negotiations of public contracts, and fraudulent accounting reports and statements.

Under the Corporate Criminal Liability Law, an investigated entity that is proven to have an effective and appropriate compliance programme may be exempt from penalties. To qualify for the waiver, the compliance programme shall provide

- periodic risk assessment and policy review;
- support from senior management;
- hotline mechanisms;
- whistleblower protection policies;
- internal investigation protocols;
- third-party due diligence process and procedures;
- due diligence policies and procedures for corporate transactions;
- periodic and continuous monitoring; and
- assignment of a responsible officer to take charge of implementation and supervision.

The National Anti-Corruption Office also issued non-mandatory 'Guidelines for the Implementation of Integrity Programs', stating that a robust compliance programme should include internal investigation protocols. Most notably, these guidelines point towards balancing the employer's right to control and supervise its activity with the employees´ legitimate expectation of privacy.

Compliance guidelines in Chile

On 2 January 2009, Chile enacted Law No. 20,393 (the Criminal Responsibility of Legal Entities Law), which broadly sets out provisions against money laundering, terrorism financing and bribery.

The Criminal Responsibility of Legal Entities Law sets a 'crime preventive model', which must be led by a responsible officer or department (a 'preventive commissioner') with an independent reporting line and adequate human and financial resources.

The preventive commissioner will be responsible for identifying risks, setting internal policies and controls, implementing accounting controls and enforcing disciplinary measures.

Other Latin American compliance provisions

Providing adequate treatment of the anti-corruption laws of the 20 countries and six dependencies that comprise Latin America would require a separate book. However, it is noteworthy that Panama and, recently, Costa Rica have also enacted laws providing compliance guidelines. Other countries, such as Guatemala and Uruguay, define corruption violations in their criminal codes but do not provide details on compliance requirements. However, most countries follow international compliance guidelines, such as the OECD's Good Practice Guidance on Internal Controls, Ethics and Compliance.

Another step forward to corporate integrity in Latin America was the OECD decision, disclosed on 25 January 2022, to open the discussions with Argentina, Brazil and Peru regarding their access to OECD membership.

The fact that accession was also opened to three key Latin American countries may have a significant impact on the region's economic growth, as it can result in a gigantic legislative advance for the entire area and attract investors. However, the process will be tough, and it is seen as a long road ahead to be concluded. An individual roadmap for the detailed assessment process will now be prepared, provided the countries confirm their adherence to the values, vision, and priorities reflected in the OECD's 60th Anniversary Vision Statement and the Ministerial Council Statement (the OECD Statement) adopted last year. The OECD Statement includes the organisation's primary values, such as individual liberty, democracy, rule of law preservation and protection of human rights, and the value of open trading, competitive, sustainable and transparent market economies. OECD members also have to commit to promoting sustainable and inclusive economic growth and their goals to tackle climate change, including halting and reversing biodiversity loss and deforestation.

The process will include a rigorous and in-depth evaluation by more than 20 technical committees of the candidate country's alignment with OECD standards, policies and practices. As a result of these technical reviews, changes to the candidate countries' legislation, policy and practices will be required to align with OECD standards and best practices, thus serving as a powerful catalyst for reform. Therefore, it is expected that Latin America will start adopting several legislative reforms to comply with the requirements.

Future in sight

The closure of *Operation Car Wash* is emblematic for Latin America by representing what the last decade meant for the fight against corruption in the region. However, the number of new corruption investigations involving Latin America demonstrates that mere existence of a new legal panorama is not enough to prevent violations from arising, particularly in scenarios of large-scale and urgent public procurement procedures. Unfortunately, in 2022, Brazil remained the most frequently cited Latin American country in connection with ongoing FCPA-related investigations. Brazil also claimed the top spot as the country most commonly implicated in FCPA-related bribery schemes resulting in enforcement actions. Inquiries into corrupt businesses are likely to increase in Latin America.[36] Therefore, while the 2010s outlined the new legal framework for the fight against corruption in Latin America, the new decade will stake a claim for effectiveness, public governance, social responsibility and sustainability.

In Brazil, according to data released by the Federal Police in early January 2021, between April and December 2020, a total of 65 Federal Police operations (20 per cent of the 315 operations carried out in 2020) were launched to investigate the misuse of public funds to restrain the covid-19 pandemic's effects – in particular, concerning the acquisition of health-related provisions, such as personal protective equipment and ventilators and other necessary supplies. Since then, several other operations have been launched by local authorities, including the recent Operation 'Last Acts' (*Últimos Atos*, in Portuguese) that gave rise to dawn raids conducted in April 2023 to investigate diversion of funds to fight the pandemic.

36 2022 FCPA Year in Review - Foreign Corrupt Practices Act Clearinghouse (FCPAC).

Likewise, other Latin American countries have launched investigations concerning the misappropriation of covid-19 funds involving high-level public officials, such as the Colombian Minister of Agriculture, the Bolivian Health Minister, the Ecuadorian Health Ministry, the Peruvian Anti-corruption Prosecution Offices and the Honduras' Public Prosecutor's Office.

Aside from all the challenges it has presented, the covid-19 pandemic showed there were easy-to-implement alternatives to increase transparency and public spending controls, especially technological tools. The use of solutions based on open data and fraud analytics has brought positive experiences both as a remote solution for negotiations during the pandemic and as a definitive accountability solution.

A significant example was the increase in e-procurement platforms and open contracting to facilitate bidding processes and increase compliance. The adhesion of initiatives such as the Open Contracting Data Standard (OCDS) – created by the global advocacy network Open Contracting Partnership – demonstrates that technological tools can increase transparency and decrease bureaucracy in public procurement processes. The OCDS creates clear and detailed standards for monitoring procurement processes, allowing a careful oversight of these procedures' compliance and transparency. In Latin America, OCDS has already been adopted by Chile, Colombia and Paraguay.

Brazil and Colombia have developed fraud analytics platforms to leverage various datasets from multiple sources to flag corruption risks in government contracting. In Brazil, the Tender and Bidding Analyzer (Alice) is a Federal Audit Court tool to mine public procurement documents and identify inconsistencies. It captures the information from public bidding notices available on the federal government's system to screen vulnerabilities and red flags. Similarly, the Colombian Comptroller General's Office has implemented a contractual data centre platform named Océano, an analytics tool to cross-check information from public procurement online databases and detect possible irregularities. Through Océano, the Colombian Comptroller General's Office has identified suspicious transactions led by certain city councils on health emergency-related contracts, which resulted in fraud investigations.

Although Latin America certainly has structural issues that make the fight against corruption challenging, including dealing with the effects of the covid-19 pandemic, it is clear that the region has been taking steps to ensure that the past decade's progress is not lost. Still, the region demonstrates room for implementing disruptive solutions, which can help Latin America drive cultural transformation in public and corporate integrity and transparency.

The re-election of President Luiz Inácio Lula da Silva in 2022, despite his arrest for corruption some years before, is an unexpected and intriguing development in Brazil. Numerous major corruption scandals, such as the Operation Car Wash, have tarnished Lula's administration, yet the Brazilian population chose to vote for him rather than President Bolsonaro, who also has been accused of several crimes. A new head of the CGU has been appointed and is a well-respected professional who expressed his willingness to continue the fight against corruption.

Currently, the leading hot topic from a compliance perspective is the evolution from compliance programmes into ESG (environmental, social and corporate governance) structures that will likely lead debates about corporate integrity in the following years.[37]

In Latin America, the introduction of ESG as a requirement is being driven by international private companies and financial institutions concerned with reputation, ethical endeavours and the impact of their transactions. Although legislative development in this regard is still in debate in certain countries and agencies and began implementation in others, the discussion on the OECD accession may expedite the countries to adopt straightforward ESG directives.

Latin America has very protective legislation in place that favours employees, which makes it challenging for companies to implement clawback provisions and collect data from personal devices when this is necessary for an internal or government investigation.

Conclusion

In the United States and Latin America, compliance began with a focus on rules-based systems and employee training. Over time, government agencies have required, and corporations have realised, that compliance programmes serve as proactive measures to detect and prevent corruption. The evolution of compliance has gone from a poster on the wall to a dynamic programme that involves all members of an organisation and its investors, as well as advanced technology to preserve, process and analyse relevant data. Compliance is no longer about simply following the letter of the law. The bar is being raised ever higher and, in addition to government agencies watching over misbehaviour and cooperating across the

37 See Chapters 19 ('The Rise of ESG as a Social Pillar in Latin America') and 20 ('Compliance as a Foundation for ESG Oversight') of this guide.

region, media, investors, potential business partners and other stakeholders are ever-more watchful. Compliance is now evolving beyond simple legal compliance to a consideration of societal benefits and a holistic ESG approach.

CHAPTER 2

No Signs of Slowing Down: Latin America's Current Compliance Climate

Julie Bédard, Maria Cruz Melendez and Mayra Suárez[1]

Introduction

Brazil's *Operation Car Wash* investigation has dominated headlines and captured public attention across Latin America and around the world since 2014. The investigation looked into widespread bribery and corruption involving politicians and state-owned enterprises and led to the conviction (although subsequently

1 Julie Bédard and Maria Cruz Melendez are partners, and Mayra Suárez is a counsel at Skadden, Arps, Slate, Meagher & Flom LLP. The authors thank Thiago Jabor Pinheiro, Izabela Pacheco Telles, João Marcelo da Costa e Silva Lima, Thiago Luís Santos Sombra and Luiza Mussoi Cattley of Mattos, Filho, Veiga Filho, Advogados; César Coronel Jones and Maria Celeste Alvarado Herrera of Coronel & Perez; José Daniel Amado Vargas and José Luis Repetto of Miranda & Amado; Carlos Chávez and Marianela Romero of Galicia Abogados, S.C.; Mario Antonio Sáenz Marinero of Novis Estudio Legal; Jorge Luis Arenales de la Roca and Anneliss Wohlers of Arias (Guatemala); Ignacio Sanz of Zang Bergel & Viñes Abogados; Juan Carlos Tristan, Alí Didier Ordóñez and Federico Barrios of BLP Abogados; Andrés Moreno of Moreno Baldivieso; Felipe G. Ossa and Álvaro Vives of Claro y Cía; José Humberto Frías of D'Empaire Reyna Abogados; Daniel Posse, Óscar Tutasaura, Jaime Cubillos and Jordi Buitrago of Posse, Herrera & Ruiz; and Cedric Kinschots and Estif Aparicio of Arias, Fabrega & Fabrega for their contributions to this chapter.

annulled) of a former (and now current) Brazilian president[2] and the impeachment of another,[3] the guilty pleas of Brazilian and foreign companies, payments of millions of dollars in penalties and more than 250 convictions.[4]

In the wake of that unprecedented enforcement activity, legislators, enforcement agencies and judiciaries within and outside Latin America have made substantial efforts to combat corruption. The US Department of Justice (US DOJ) and US Securities and Exchange Commission (US SEC) have brought corruption-related charges against more than 100 individuals and corporations for conduct in or related to Latin America since 2018, often in collaboration with enforcement counterparts in other countries.[5]

The interest in combating corruption in the region shows no sign of abating. In March 2019, the US Federal Bureau of Investigation (FBI) announced the Miami International Corruption Squad, a task force intended to work alongside the FBI's other international corruption squads, the US SEC and the US DOJ's Fraud and Money Laundering Asset Forfeiture sections, signalling the continuing focus of US authorities on corruption in Latin America.[6] The squad has worked on several cases since its creation, including some that settled in 2020 and led to convictions in 2021 and 2022, and it has developed strong partnerships with law enforcement officials in Brazil, Colombia and Ecuador.[7]

---

2 Associated Press, 'Former Brazilian President Lula convicted in second corruption case', *Los Angeles Times* (6 February 2019) <https://www.latimes.com/world/la-fg-brazil-lula-conviction-20190206-story.html>; 'What did Lava Jato, Brazil's anti-corruption investigation, achieve?' *The Economist* (9 March 2021) <https://www.economist.com/the-economist-explains/2021/03/09/what-did-lava-jato-brazils-anti-corruption-investigation-achieve>. Following the annulment of his conviction, Luiz Inácio Lula da Silva was elected for a third term as Brazil's president.

3 Romero, Simon, 'Dilma Rousseff Is Ousted as Brazil's President in Impeachment Vote', *The New York Times* (31 August 2016) <https://www.nytimes.com/2016/09/01/world/americas/brazil-dilma-rousseff-impeached-removed-president.html>.

4 Brazil's Federal Public Prosecutor's Office, 'Caso Lava Jato – Resultados' (24 August 2021) <http://www.mpf.mp.br/grandes-casos/lava-jato/resultados>; see also Brito, Ricardo & Slattery, Gram, 'After seven years, Brazil shuts down Car Wash anti-corruption squad', *Reuters* (3 February 2021) <https://www.reuters.com/article/us-brazil-corruption/after-seven-years-brazil-shuts-down-car-wash-anti-corruption-squad-idUSKBN2A4068>.

5 See section below titled 'Recent enforcement trends.'

6 Press Release, Federal Bureau of Investigation [FBI], 'FBI Announces New International Corruption Squad in Miami Field Office' (5 March 2019) <https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-new-international-corruption-squad-in-miami-field-office>.

7 See Sun, Mengqi, 'FBI Increasingly Probes for Corruption Overseas', *The Wall Street Journal* (31 December 2020) <https://www.wsj.com/articles/fbi-increasingly-probes-

On 3 June 2021, US President Joe Biden issued a Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest.[8] Shortly thereafter, the US DOJ announced an Anticorruption Task Force aimed at combatting corruption in Central America, specifically in El Salvador, Guatemala and Honduras.[9]

In October 2021, Deputy Attorney General Lisa Monaco announced a commitment to increasing resources to DOJ prosecutors, including the establishment of a permanent squad of FBI agents within the Criminal Fraud Section, signalling a continued interest in prosecuting corporate and white-collar crime.[10] Monaco followed up with a memo in September 2022, providing guidance on how prosecutors should ensure individual and corporate accountability via criminal enforcement.[11]

---

for-corruption-overseas-11609434000>; Press Release, US DOJ, 'Former Ecuadorian Government Official Sentenced to Prison for Role in Bribery and Money Laundering Scheme' (23 March 2021) <https://www.justice.gov/opa/pr/former-ecuadorian-government-official-sentenced-prison-role-bribery-and-money-laundering>; Press Release, US DOJ, 'Former Venezuelan National Treasurer and Husband Convicted in International Bribery Scheme' (15 December 2022) <https://www.justice.gov/usao-sdfl/pr/former-venezuelan-national-treasurer-and-husband-convicted-international-bribery-sche-0>.

8 Press Release, White House, 'Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest' (3 June 2021),) <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/memorandum-on-establishing-the-fight-against-corruption-as-a-core-united-states-national-security-interest./>.

9 See Press Release, US DOJ, 'Attorney General Announces Initiatives to Combat Human Smuggling and Trafficking and to Fight Corruption in Central America' (7 June 2021) <https://www.justice.gov/opa/pr/attorney-general-announces-initiatives-combat-human-smuggling-and-trafficking-and-fight>; see also Press Release, US DOJ, 'Justice Department Anticorruption Task Force Launches New Measures to Combat Corruption in Central America' (15 October 2021) [hereinafter New Measures to Combat Corruption in Central America] <https://www.justice.gov/opa/pr/justice-department-anticorruption-task-force-launches-new-measures-combat-corruption-central>.

10 Press Release, US DOJ, 'Deputy Attorney General Lisa O. Monaco Gives Keynote Address at ABA's 36th National Institute on White Collar Crime' (28 October 2021) <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute>.

11 See Monaco, Lisa, US Department of Justice Memorandum, 'Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group' (15 September 2022) <https://www.justice.gov/opa/speech/file/1535301/download>.

Companies operating in Latin America should be mindful of recent enforcement trends and of global regulators' focus on fighting corruption in the region. This chapter reviews: recent trends in legislative and constitutional anti-corruption enforcement regimes in Latin America; and global enforcement of corruption-related conduct in Latin America.

Key legislative changes in Latin America and elsewhere

Development and strengthening of anti-corruption regimes

Corporate criminal liability

In recent years, many Latin American countries, by legislation or constitutional amendment, have established corporate criminal liability for bribery and corruption offences. For example, Mexico (May 2015 and June 2016),[12] Peru (April 2016,

12 Since 2005, the Mexican Federal Criminal Code provides for corporate criminal liability in cases of international bribery, committed in the entity's name, on its behalf, for its benefit or using means provided by the entity. See Código Penal Federal [CPF], Article 222 *bis*, Diario Oficial de la Federación [DOF] 14-08-1931, últimas reformas DOF 06-01-2023 (Mex.) <https://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Codigo_Penal_Federal.pdf>. In 2015, the Mexican Constitution was amended to mandate Congress to pass comprehensive anti-corruption legislation providing for criminal liability for corruption offences. See Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de combate a la corrupción, Diario Oficial de la Federación [DOF] 27-05-2015 (Mex.) <www.diputados.gob.mx/LeyesBiblio/proceso/docleg/62/223_DOF_27may15.pdf>. Further, in 2016, the Federal Criminal Code and the National Criminal Procedure Code were amended to extend corporate criminal liability to certain offences, including public bribery and influence peddling, provided that the entity did not have proper controls in place; see DOF 17-06-2016 (Mex.) <https://www.dof.gob.mx/nota_detalle.php?codigo=5441763&fecha=17/06/2016>; see also Decreto por el que se expide la Ley General del Sistema Nacional Anticorrupción; la Ley General de Responsabilidades Administrativas, y la Ley Orgánica del Tribunal Federal de Justicia Administrativa, Diario Oficial de la Federación [DOF] 18-07-2016 (Mex.) <https://www.diputados.gob.mx/LeyesBiblio/ref/lgsna/LGSNA_orig_18jul16.pdf>.

amended 2017 and 2018),[13] Argentina (March 2018),[14] Costa Rica (June 2019),[15] and Ecuador (February 2021)[16] now provide for corporate criminal liability for bribery of domestic public officials; in some countries, corporations can be liable for related conduct such as money laundering, commercial bribery and bribery of foreign officials.

In other Latin American countries, such as Colombia and Brazil, only individuals, not corporations, can be held criminally liable for anti-corruption violations, though companies in Colombia may be held jointly and severally liable with employees and executives who engage in corrupt conduct, and, in Brazil, corporations can be held criminally liable for environmental violations.[17]

---

13 See Law No. 30424, El Peruano (Peru) (21 April 2016) <www.leyes.congreso.gob.pe/Documentos/Leyes/30424.pdf> (providing for criminal liability for transnational bribery, committed in the name or on behalf of the legal entity for its direct or indirect benefit); Legislative Decree No. 1352 (amending Law No. 30424), El Peruano (Peru) (7 January 2017) <https://www.leyes.congreso.gob.pe/Documentos/DecretosLegislativos/01352.pdf> (delaying enactment of Law No. 30424 to 7 January 2018 and expanding criminal liability to cover the offences of bribery of domestic public officials, money laundering and financing of terrorism); Law No. 30835 (amending Law No. 30424), El Peruano (Peru) (2 August 2018) <https://www.leyes.congreso.gob.pe/Documentos/2016_2021/ADLP/Normas_Legales/30835-LEY.pdf> (modifying the name of Law No. 30424 and expanding criminal liability to cover the offences of influence peddling and collusion).

14 See Law No. 27401, Official Bulletin (Argentina) (1 December 2017) <https://www.ilo.org/dyn/natlex/docs/electronic/106245/130242/f-2006629615/ley%2027401%20argentina.pdf>. The law provides for criminal liability for offences, including foreign bribery and false books and records, committed with the company's intervention or in the company's name, interest or benefit. Penalties include fines, suspension of commercial activities, disqualification from public tenders, cancellation of corporate registration, loss of government benefits and publication of the conviction. There is no retroactive liability.

15 See Law No. 9699 de Responsabilidad de las Personas Jurídicas sobre Cohechos Domésticos, Soborno Transnacional y Otros Delitos (Costa Rica) (6 October 2019) <http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=88954>.

16 See Organic Integral Criminal Code, Official Registry (Ecuador) (10 February 2014) <https://oig.cepal.org/sites/default/files/2014_codigopenal_ecu.pdf>; see also Organic Law No. 392, "On Amendments to the Comprehensive Organic Criminal Code in Relation to Anti-Corruption," Official Registry (Ecuador) (12 February 2021) <https://lvro.finder.lexis.com.ec/?id=071BBC576F73088AA25B474286480662679664BB&type=%27%27&productName=LEXISNEWS&page=1>.

17 See Law No. 599, Official Gazette (Colombia) (24 July 2000) <https://www.refworld.org/docid/3dbd1fd94.html>; see Law No. 9605, Official Gazette (Brazil) (13 February 1998) <www.planalto.gov.br/ccivil_03/leis/l9605.htm>; see also Law No. 2195, Official Gazette (Colombia) (18 January 2022) <https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=175606> (providing for administrative sanctions of up to 200,000 million

Mandated or recommended compliance programmes and other factors in leniency determinations

Several countries have passed laws relating to corporate compliance programmes that are (1) required, (2) recommended or (3) if implemented, can entitle a company in violation of anti-corruption laws to leniency.[18]

In Brazil, compliance programmes are generally not required under federal law, unless contracting with the government, under certain circumstances. For example, Brazil's 2021 Public Procurement Law, Law No. 14133, mandates that companies that win public bids valued at over 200 million reais develop an effective compliance programme within six months of the contract's execution.[19] Also, companies that have compliance programmes in place before the tender process, all else being equal between two bids, will be awarded the contract.[20] Even where compliance programmes are not required, companies with effective compliance programmes may be entitled to a fine reduction of up to 5 per cent in

pesos (US$41 million) for corporate entities that benefit or seek to benefit from foreign bribery committed by administrators or employees).

18 Federal and certain state laws in Brazil require companies that contract with state entities to have compliance programmes. See, e.g., Federal District Law No. 6112 of 2 February 2018, Official Gazette (Brazil) (6 February 2018); Rio de Janeiro State Law No. 7753 of 17 October 2017, Official Gazette (Brazil) (18 October 2017); Rio Grande do Sul State Law No. 15228 of 25 September 2018, Official Gazette (Brazil) (26 September 2018); Amazonas State Law No. 4370 of 27 December 2018, Official Gazette (Brazil) (27 December 2018); Goiás State Law No. 20489 of 10 June 2019, Official Gazette (Brazil) (25 June 2019).

19 See Law No. 14133 of 1 April 2021, Official Gazette (Brazil) (1 April 2021) <https://www.in.gov.br/en/web/dou/-/lei-n-14.133-de-1-de-abril-de-2021-311876884> (which will replace previous Public Procurement Law No. 8666 of 21 June 1993 as of 1 April 2023).

20 *id.* Article 60.

administrative proceedings.[21] Brazil's July 2022 Decree No. 11,129 sets forth new requirements for assessing compliance programmes and calculating cooperation credit as part of leniency agreements.[22]

In August 2021, Colombia expanded the criteria used to determine which non-financial companies must adopt 'transparency and business ethics programmes;' to be deemed sufficient, the programmes now must also include a compliance officer, in addition to other requirements.[23]

Peru provides companies that have effective 'prevention models' before the commission of a crime, with the possibility to be exempt from corporate liability for corrupt conduct.[24] Similarly, under Chilean law, the adoption and implementation of 'prevention models' before the corrupt conduct may be sufficient evidence to prove the company's innocence in criminal proceedings.[25]

---

21 Law No. 12846 of 1 August 2013, Official Gazette (Brazil) (2 August 2013) <https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/30042702/do1-2013-08-02-lei-n-12-846-de-1-de-agosto-de-2013-30042696> (providing incentives for corporate compliance programmes); see Decree No. 11129 of 11 July 2022, Official Gazette (Brazil) (11 July 2022) <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11129.htm> (providing credit for effective compliance programmes, defining parameters for evaluating compliance programmes (e.g., customised to each legal entity and its activities, commitment by senior management, training) and providing for the administrative liability of legal persons for the commission of acts against public, national or foreign administrations). Securities and Exchange Commission of Brazil, Rule No. 607 establishes that any publicly held company with an effective compliance programme may have their fines reduced by up to 25 per cent. Instruction No. 607 of 17 June 2019, Official Gazette (Brazil) (18 June 2019) <www.in.gov.br/web/dou/-/instrucao-n-607-de-17-de-junho-de-2019-164059674>.

22 Decree No. 11129 (footnote 21, above).

23 See External Circular 100-000011 of 9 August 2021, Official Gazette (Colombia) (9 August 2021) <https://xperta.legis.co/visor/legcol/legcol_39161724d85b4b7f90ef9ed36194f334/coleccion-de-legislacion-colombiana/circular-externa-100-000011-de-agosto-9-de-2021>.

24 See Law No. 30424, Article 17 (footnote 13, above).

25 See Law No. 20393, Establishing the criminal responsibility of legal persons in the crimes of laundering of assets, financing of terrorism and bribery, Official Gazette (Chile) (25 November 2009) <http://www.oas.org/juridico/spanish/mesicic3_chl_ley20393.pdf> (stating that an effective prevention model includes: (1) systems to identify risks, establish specific protocols, rules and procedures to prevent the commission of said offences, and identify procedures for administrating and auditing the entity's financial resources; (2) internal administrative sanctions; (3) procedures for reporting wrongdoing; and (4) procedures to detect and correct systemic failures in the prevention model).

In Costa Rica, compliance programmes are not required by law; however, for companies that adopt them, they can serve as a mitigating factor for any criminal penalties by up to 40 per cent.[26]

In Argentina, compliance programmes are not a regulatory requirement for companies, unless contracting with the Argentine federal government; however, compliance programmes are a requisite element for obtaining a reduction of, or exemption from, anti-bribery related penalties.[27]

In Mexico, the Mexican General Administrative Liabilities Act mandates that, in assessing a corporation's liability for alleged acts of corruption, the competent court must consider whether the corporation has an integrity policy and if the policy includes: (1) a manual clearly setting forth the responsibilities of the appropriate areas and individuals within the organisation; (2) a code of conduct appropriately socialised within the organisation; (3) adequate control and audit mechanisms; (4) adequate whistleblowing mechanisms and sanctions for violating the policy; and (5) adequate training mechanisms.[28]

Some countries also provide incentives in the form of credit or leniency for disclosure of misconduct to government authorities and cooperation with investigations. For example, in Peru, the Public Prosecutor's Office can enter into leniency agreements – subject to judicial approval – with individuals and companies that are involved in the commission of certain crimes, including bribery of public officials, when the company or individual (1) voluntarily abandons the criminal activities, (2) admits freely, or does not contradict, the facts concerning the criminal conduct and (3) presents himself to the Public Prosecutor's Office, demonstrating a willingness to provide useful information.[29]

Similarly, under Ecuador's Criminal Code, individuals who engage in corrupt conduct can obtain a reduction in their sentence if they provide accurate and verifiable information that (1) clarifies facts under investigation, (2) results in the identification of culpable persons or (3) helps to prevent, neutralise or impede the commission of a crime of equal or greater significance.[30] For an individual

---

26 See Law No. 9699, Article 12 (footnote 15, above).

27 See Law No. 27401, Articles 9, 23–24, (footnote 14, above).

28 See Ley Federal de Responsabilidades Administrativas, Article 25, Diario Oficial de la Federación [DOF] 18-07-2016, latest reforms DOF 27-12-2022 (Mex.) https://www.diputados.gob.mx/LeyesBiblio/pdf/LGRA.pdf

29 See Legislative Decree No. 957, Article 472, Criminal Procedure Code (Peru) (29 July 2004) <https://www.wipo.int/wipolex/en/text/202824>.

30 See Organic Integral Criminal Code, Article 491, Official Registry (Ecuador), 3 February 2014 <https://oig.cepal.org/sites/default/files/2014_codigopenal_ecu.pdf>.

to receive cooperation credit, the prosecutor must confirm in the charging document presented to the court that the cooperation was effective.[31] Additionally, companies can mitigate criminal sanctions by (1) self-disclosing the criminal conduct before an investigation begins, (2) cooperating with the investigation, (3) compensating the damage caused by the crime before the initiation of court proceedings, and (4) having a compliance programme in place and appointed officers responsible for its implementation before the commission of the crime.[32]

Expansion of prohibited and regulated conduct

Several Latin American countries have expanded the reach of their anti-bribery statutes. In Peru and Chile, for instance, prohibited conduct extends beyond the bribery of public officials and includes commercial bribery – bribery of individuals acting in a private capacity.[33] However in Peru, private corruption charges can only be brought against individuals, not companies. Other countries, such as Argentina and Venezuela, have also criminalised bribery of foreign, not just domestic, government officials.[34]

Some countries have placed restrictions on corporate political contributions as a means to combat corruption. For example, in Chile, companies are prohibited from political contributions to electoral campaigns; these may be made by individuals only.[35] In Colombia, any company that contributes greater than 2.5 per cent of the total contribution permitted under law to any president, governor or mayor may not enter into public contracts with entities administered by the candidate while the candidate is in office.[36]

---

31 *id.* Articles. 492, 493.

32 See Organic Law No. 392, Article 1 (footnote 16, above).

33 See Law No. 21121 (amending the Criminal Code and other legal rules for the prevention, detection and prosecution of corruption), Official Gazette (Chile) (20 November 2018) <https://www.bcn.cl/leychile/navegar?idNorma=1125600>; Legislative Decree No. 1385, Criminal Code (Peru) (4 September 2018) <https://cdn.www.gob.pe/uploads/document/file/192144/DL_1385.pdf>.

34 Law No. 6155, Official Gazette (Venezuela) (19 November 2014) <https://www.legiscompliance.com.br/images/pdf/decreto_6155_lac_venezuela.pdf>.

35 See Law No. 20900 (for the strengthening and transparency of democracy), Official Gazette (Chile) (14 April 2016) <https://www.diariooficial.interior.gob.cl/media/2016/04/14/do-20160414.pdf>.

36 See Law No. 1474 of 12 July 2011, Official Gazette (Colombia) (12 July 2011) <http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/Ley%201474%20de%2012%20de%20Julio%20de%202011.pdf>.

Northern Triangle Enhanced Engagement Act[37]

Enacted by the United States in December 2020, the Act requires that the US Secretary of State and the Administrator of the US Agency for International Development devise a five-year strategy to, among other things, 'advance economic prosperity' and 'combat corruption' in El Salvador, Guatemala and Honduras.[38] Pursuant to the Act, on 1 July 2021, the US Department of State released its first iteration of the 'Engel List,' a directory of suspected corrupt and undemocratic actors in the Northern Triangle.[39] The list identified 55 individuals, largely current and former public officials, whose visas were immediately revoked and are subsequently barred from entering the United States.[40] Notably, following the publication of the first Engel List, authorities in El Salvador, Guatemala and Honduras did not initiate investigations into any of the named officials.[41] Critics say this is because the list focused mainly on 'secondary perpetrators;' high-level officials were omitted from the list.[42]

---

37 United States-Northern Triangle Enhanced Engagement Act, Pub. L. No. 116-260, Division FF, §§ 351-353, 134 Stat. 3127, 3127–31 (27 December 2020) (codified at 22 U.S.C. §§ 2277, 2277a) <https://www.govinfo.gov/content/pkg/PLAW-116publ260/pdf/PLAW-116publ260.pdf>.

38 *id.* § 352(a) (codified at 22 U.S.C. § 2277(a)).

39 See *id.* § 353(b) (codified at 22 U.S.C. § 2277a(b)); see also Press Statement, Blinken, Antony J., U.S. Secretary of State, 'U.S. Releases Section 353 List of Corrupt and Undemocratic Actors for Guatemala, Honduras, and El Salvador' (1 July 2021) <https://www.state.gov/u-s-releases-section-353-list-of-corrupt-and-undemocratic-actors-for-guatemala-honduras-and-el-salvador/>.

40 US Department of State, 'Report to Congress on Foreign Persons who have Knowingly Engaged in Actions that Undermine Democratic Processes or Institutions, Significant Corruption, or Obstruction of Investigations into Such Corruption in El Salvador, Guatemala and Honduras' (1 July 2021) <https://www.state.gov/wp-content/uploads/2021/07/Congressional-Report-Section-353-Names.pdf>.

41 See Méndez Dardón, Ana María 'Engel List: What is the United States Telling Central America?' Washington Office on Latin America (21 July 2022) <https://www.wola.org/analysis/engel-list-what-is-the-united-states-telling-central-america/>; Marroquín, César Pérez 'MP califica de falsos e infundados señalamientos de EE. UU. Para incluir a Consuelo Porras en la lista de actores corruptos,' Prensa Libre (20 September 2021) <https://www.prensalibre.com/guatemala/politica/mp-califica-de-falsos-e-infundados-senalamientos-de-ee-uu-para-incluir-a-consuelo-porras-en-la-lista-de-actores-corruptos-breaking/> (The Guatemalan government has publicly rejected and condemned the Engel List due to 'unfounded allegations').

42 See Plazas, Natalia 'Engel List': US accuses high-ranking Central American officials of corruption,' France 24 (7 February 2021) <https://www.france24.com/es/am%C3%A9rica-latina/20210702-eeuu-corrupcion-lista-triangulo-norte>.

On 20 July 2022, the US Department of State added 59 other individuals and expanded the list to include Nicaraguan officials.[43] Among those added were three officials close to President Nayib Bukele of El Salvador and Honduran officials close to the country's President Manuel Zelaya.[44]

State-owned entities

Operation Car Wash: Petrobras and beyond

After almost seven years of investigating corruption schemes in Brazil and elsewhere, *Operation Car Wash* was officially disbanded at the beginning of February 2021.[45] Although *Operation Car Wash* began with Petróleo Brasileiro SA (Petrobras), Brazil's state-controlled energy company, many other state-owned or state-controlled enterprises were implicated across Latin America. Companies interacting with state-owned or state-controlled enterprises in Latin America should scrutinise these interactions.

Between December 2016 and December 2018, at least four companies reached resolutions with the US DOJ or the US SEC (or both), acknowledging bribery payments made to or through Petrobras executives, as well as, in some instances, additional improper payments to other government or state-owned entities (SOEs) or officials.[46] The alleged misconduct spanned Latin America

---

43 See Press Statement, Blinken, Anthony J, US Secretary of State, 'Release of the Section 353 List of Corrupt and Undemocratic Actors for Guatemala, Honduras, El Salvador, and Nicaragua' (20 July 2022) <https://www.state.gov/release-of-the-section-353-list-of-corrupt-and-undemocratic-actors-for-guatemala-honduras-el-salvador-and-nicaragua/>; See § 353(b) (codified at 22 U.S.C. § 2277a(b) 'Corrupt and Undemocratic Actors Report') <https://www.state.gov/reports/section-353-corrupt-and-undemocratic-actors-report-2022/>.

44 See Gressier, Roman 'US Shows Its Teeth on Engel List,' El Faro (18 July 2022) <https://elfaro.net/en/202207/centroamerica/26278/US-Shows-Its-Teeth-on-Engel-List.htm>.

45 See Brito, Ricardo, 'After Seven Years, Brazil Shuts Down Car Wash Anti-Corruption Squad', *Reuters* (3 February 2021) <https://www.reuters.com/article/us-brazil-corruption-idUSKBN2A4068>.

46 See, e.g., Non-Prosecution Agreement, Petróleo Brasileiro S.A.–Petrobras (26 September 2018) <https://www.justice.gov/opa/press-release/file/1096706/download>; Press release, US DOJ, 'SBM Offshore N.V. and U.S.-based Subsidiary Resolve Foreign Corrupt Practices Act Case Involving Bribes in Five Countries' (29 November 2017) <https://www.justice.gov/opa/pr/sbm-offshore-nv-and-united-states-based-subsidiary-resolve-foreign-corrupt-practices-act-case>; Press release, US DOJ, 'Keppel Offshore & Marine Ltd. and U.S.-Based Subsidiary Agree to Pay $422 Million in Global Penalties to Resolve Foreign Bribery Case' (22 December 2017) <https://www.justice.gov/usao-edny/pr/keppel-offshore-marine-ltd-and-us-based-subsidiary-agree-pay-422-million-global>; Press release, US DOJ, 'Odebrecht and Braskem Plead Guilty and Agree to Pay at Least $3.5 Billion in Global Penalties to Resolve Largest Foreign Bribery Case in History' (21 December 2016) <https://www.justice.

– including alleged payments in Argentina, Brazil, Colombia, the Dominican Republic, Ecuador, Guatemala, Mexico, Panama, Peru and Venezuela. In connection with the US resolutions, Brazilian authorities were also able to secure independent settlements with all four companies.[47]

One such company was Brazilian construction conglomerate Odebrecht. Following Odebrecht's December 2016 resolution with US, Brazilian and Swiss authorities, prosecutors from Brazil and 10 other Latin American countries formed a task force to investigate potential bribes paid by the company, emphasising information sharing and cooperation in the region.[48] As a result of its efforts to cooperate, the company has reached agreements with prosecutors in at least six countries in Latin America.

On 26 September 2018, Petrobras agreed to pay US$1.78 billion – at the time, the largest single US Foreign Corrupt Practices Act (FCPA) resolution – to resolve investigations by the US DOJ, the US SEC and Brazilian authorities concerning bribery.[49] As part of its resolution, Petrobras agreed to cooperate with other investigations into related conduct.[50] Both US and Latin American authorities have been active in prosecuting companies that paid bribes to and through Petrobras executives. Since the resolution of the Petrobras investigation, the US DOJ and the US SEC have, individually or jointly, reached resolutions with at least eight additional companies for Petrobras-related misconduct.[51]

---

gov/opa/pr/odebrecht-and-braskem-plead-guilty-and-agree-pay-least-35-billion-global-penalties-resolve>.

47 See, e.g., 'Keppel Offshore & Marine Reaches Global Resolution with Authorities in the U.S., Brazil and Singapore', Keppel Offshore & Marine (23 December 2017) <https://www.keppelletourneau.com/en/article_item.aspx?sid=10072>; Press release, SBM Offshore, 'SBM Offshore achieves settlement with Dutch Public Prosecutor's Office over alleged improper payments. United States Department of Justice closes out the matter' (12 November 2014) <https://www.sbmoffshore.com/newsroom/press-releases/2014/12-11-2014/sbm-offshore-achieves-settlement-dutch-public-prosecutors>.

48 See Boadle, Anthony, 'Latin American prosecutors join forces on Odebrecht bribes', *Reuters* (17 February 2017) <https://www.reuters.com/article/idUSL1N1G200Y>.

49 Press release, US DOJ, 'Petróleo Brasileiro S.A.–Petrobras Agrees to Pay More Than $850 Million for FCPA Violations' (27 September 2018) [hereinafter 'Petrobras Agrees to Pay More Than $850 Million'] <https://www.justice.gov/opa/pr/petr-leo-brasileiro-sa-petrobras-agrees-pay-more-850-million-fcpa-violations>; Press release, US SEC, 'Petrobras Reaches Settlement With SEC for Misleading Investors' (27 September 2018) [hereinafter 'Petrobras Reaches Settlement With SEC'] <https://www.sec.gov/news/press-release/2018-215>.

50 *id.* at 3.

51 Press release, US SEC, 'Vantage Drilling International Agrees to Settle FCPA Charges' (19 November 2018) <https://www.sec.gov/enforce/34-84617-s>; Press release, US DOJ, 'Samsung Heavy Industries Company Ltd Agrees to Pay $75 Million in Global Penalties

Other SOEs

Operation Car Wash led investigators far beyond Petrobras. In April 2015, Brazilian prosecutors reported evidence of fraud at the country's health ministry and at state-owned bank Caixa Econômica Federal.[52] In October 2020, J&F Investimentos S.A. (J&F), a Brazil-based investment company, as well as its subsidiary JBS S.A., resolved enforcement actions with both the US DOJ and US SEC. The company admitted to making nearly US$150 million in corrupt payments to high-ranking Brazilian government officials, including almost US$25 million to a member of the legislative branch of the Brazilian government, in exchange for securing hundreds of millions in financing from Caixa

---

to Resolve Foreign Bribery Case' (22 November 2019) <https://www.justice.gov/opa/pr/samsung-heavy-industries-company-ltd-agrees-pay-75-million-global-penalties-resolve-foreign>; Press release, US DOJ, 'TechnipFMC Plc and U.S.-Based Subsidiary Agree to Pay Over $296 Million in Global Penalties to Resolve Foreign Bribery Case' (25 June 2019) <https://www.justice.gov/opa/pr/technipfmc-plc-and-us-based-subsidiary-agree-pay-over-296-million-global-penalties-resolve#:~:text=(Technip%20USA)%2C%20have%20agreed,the%20United%20States%20and%20Brazil.&text=Technip%20USA%20and%20Technip's%20former,in%20connection%20with%20the%20resolution>; Deferred Prosecution Agreement at A-15, A-18, *United States v. Vitol Inc.*, No. 20-539 (E.D.N.Y. 3 December 2020) [hereinafter Vitol Deferred Prosecution Agreement] <https://www.justice.gov/criminal-fraud/file/1346651/download>; Press release, US DOJ, 'Sargeant Marine Inc. Pleads Guilty and Agrees to Pay $16.6 Million to Resolve Charges Related to Foreign Bribery Schemes in Brazil, Venezuela, and Ecuador' (22 September 2020) [hereinafter Sargeant Marine Press Release] <https://www.justice.gov/opa/pr/sargeant-marine-inc-pleads-guilty-and-agrees-pay-166-million-resolve-charges-related-foreign>; Press release, US DOJ, 'Amec Foster Wheeler Energy Limited Agrees to Pay Over $18 Million to Resolve Charges Related to Bribery Scheme in Brazil' (25 June 2021) <https://www.justice.gov/opa/pr/amec-foster-wheeler-energy-limited-agrees-pay-over-18-million-resolve-charges-related-bribery>; Press release, US SEC, 'SEC Charges Honeywell with Bribery Schemes in Algeria and Brazil' (19 December 2022) <https://www.sec.gov/news/press-release/2022-230>; Press release, US SEC, 'Press Release SEC Charges Global Steel Pipe Manufacturer with Violating Foreign Corrupt Practices Act' (2 June 2022) <https://www.sec.gov/news/press-release/2022-98>.

52 Jelmayer, Rogerio & Magalhaes, Luciana, 'CEO of Brazil's Eletronuclear Arrested in Wide Corruption Probe', *The Wall Street Journal* (28 July 2015) [hereinafter 'CEO of Brazil's Eletronuclear Arrested in Wide Corruption Probe'] <https://www.wsj.com/articles/brazil-car-wash-corruption-probe-spreads-to-eletrobras-1438091569?mod=article_inline>.

Econômica Federal.[53] J&F also made bribe payments to an executive at Banco Nacional de Desenvolvimento Econômico e Social (BNDES), another Brazilian state-owned and -controlled bank.[54]

Brazil's formerly state-owned electric utility, Centrais Eletricas Brasileiras SA (Eletrobras), has also been the focus of anti-corruption investigations by both Brazilian and US authorities.[55] In July 2015, Brazilian authorities arrested the chief executive of Eletrobras and executed nearly two dozen related search warrants.[56] In October 2016, Eletrobras disclosed that it was cooperating with the US DOJ, the US SEC, Brazilian authorities and others.[57] In August 2018, Eletrobras disclosed that the US DOJ declined to prosecute the company for FCPA violations but, in December 2018, Eletrobras paid US$2.5 million to settle US SEC charges that it violated the books and records and internal controls provisions of the FCPA.[58]

Operation Car Wash also brought investigators to state-owned enterprises in other countries. For example, Petróleos Mexicanos (PEMEX) CEO Emilio Lozoya was arrested in connection with crimes identified by *Operation Car Wash*.[59]

---

53 Press Release, US DOJ, 'J&F Investimentos S.A. Pleads Guilty and Agrees to Pay Over $256 Million to Resolve Criminal Foreign Bribery Case' (14 October 2020) [hereinafter J&F Press Release, 14 October 2020] <https://www.justice.gov/opa/pr/jf-investimentos-sa-pleads-guilty-and-agrees-pay-over-256-million-resolve-criminal-foreign>; Press Release, US SEC, 'SEC Charges Brazilian Meat Producers With FCPA Violations' (14 October 2020) [hereinafter SEC Charges Brazilian Meat Producers With FCPA Violations'] <https://www.sec.gov/news/press-release/2020-254>.

54 *id.*

55 Eletrobras became a private company on 9 June 2022. Andrade, Vinicius & Viotti Beck, Martha, 'Brazil Set to Privatize Power Firm Eletrobras in $7 Billion Deal', *Bloomberg* (9 June 2022) <https://www.bloomberg.com/news/articles/2022-06-09/brazil-set-to-privatize-power-giant-in-tk-billion-stock-sale?leadSource=uverify%20wall>.

56 'CEO of Brazil's Eletronuclear Arrested in Wide Corruption Probe' (footnote 52, above).

57 Eletrobras, Annual Report (Form 20-F) (11 October 2016) <https://www.sec.gov/Archives/edgar/data/0001439124/000119312516735791/d204633d20f.htm>.

58 Press release, US SEC, 'SEC Charges Eletrobras with Violating Books and Records and Internal Accounting Controls Provisions of the FCPA' (26 December 2018) <https://www.sec.gov/enforce/34-84973-s>.

59 See Petróleos Mexicanos (Form 6-K) (11 September 2019) <https://www.pemex.com/ri/reguladores/Informacion%20SEC/Form%206-K%20A,%20filed%20Sep11,%202019.pdf>; Associated Press 'Judge in Mexico orders ex-head of state oil company jailed' (3 November 2021) <https://apnews.com/article/business-mexico-caribbean-mexico-city-e2fde527b27b7083c1cee9fa12ef86c5>.

PEMEX stated that it was cooperating with Mexican, US and other government authorities in connection with the investigation.[60] As of February 2023, Lozoya is in prison awaiting trial.[61]

During the past few years, US authorities have undertaken sweeping investigations of alleged corruption at state-owned and state-controlled entities in Venezuela and Ecuador. These have largely resulted in individual enforcement actions, including indictments against 42 individuals in connection with bribery at Petróleos de Venezuela S.A. (PdVSA),[62] a Venezuelan state-owned and

60 Petróleos Mexicanos (Form 20-F) (8 May 2020) <https://www.pemex.com/ri/reguladores/ReportesAnuales_SEC/20-F%202019%20PDF.pdf>.

61 'Audiencia de Emilio Lozoya por el caso Agronitrogenados se difiere al 27 de abril', 24 Horas (16 February 2023) <https://www.24-horas.mx/2023/02/16/audiencia-de-emilio-lozoya-por-el-caso-agronitrogenados-se-difiere-al-27-de-abril/>.

62 See 'FCPA Matter Information Multiple Parties' Involvement with PDVSA in Venezuela between 2008 and 2017', Stanford Law School: Foreign Corrupt Practices Act Clearinghouse (24 November 2015) <https://fcpa.stanford.edu/fcpa-matter.html?id=289>; Press Release, US DOJ, 'Two Financial Asset Managers Charged in Alleged $1.2 Billion Venezuelan Money Laundering Scheme' (12 July 2022) <https://www.justice.gov/opa/pr/two-financial-asset-managers-charged-alleged-12-billion-venezuelan-money-laundering-scheme>; Press Release, US DOJ, 'Two Former Senior Venezuelan Prosecutors Charged for Receiving Over $1 Million in Bribes' (8 March 2022) <https://www.justice.gov/opa/pr/two-former-senior-venezuelan-prosecutors-charged-receiving-over-1-million-bribes>; Press Release, US DOJ, 'Executive Arrested and Charged for Bribery and Money-Laundering Scheme' (4 August 2021) <https://www.justice.gov/opa/pr/executive-arrested-and-charged-bribery-and-money-laundering-scheme>; Press Release, US DOJ, 'Former Venezuelan Official Pleads Guilty in Connection with International Bribery and Money Laundering Scheme' (23 March 2021) <https://www.justice.gov/opa/pr/former-venezuelan-official-pleads-guilty-connection-international-bribery-and-money>; Press Release, US DOJ, 'Venezuelan Business Executive Charged in Connection with International Bribery and Money Laundering Scheme' (25 November 2020) <https://www.justice.gov/opa/pr/venezuelan-business-executive-charged-connection-international-bribery-and-money-laundering>; Sargeant Marine Press Release (footnote 51, above); Press Release, US DOJ, 'Texas Businessman Sentenced to 70 Months in Prison for Role in Venezuela Bribery Scheme and Obstruction of Justice' (19 February 2020) <https://www.justice.gov/opa/pr/texas-businessman-sentenced-70-months-prison-role-venezuela-bribery-scheme-and-obstruction>; Press Release, US DOJ, 'Florida Businessman Sentenced to 48 Months in Prison for Role in Venezuela Bribery Scheme' (8 January 2020) <https://www.justice.gov/opa/pr/florida-businessman-sentenced-48-months-prison-role-venezuela-bribery-scheme>; Press Release, US DOJ, 'Business Executive Pleads Guilty to Foreign Bribery Charges in Connection with Venezuela Bribery Scheme' (29 May 2019) <https://www.justice.gov/opa/pr/business-executive-pleads-guilty-foreign-bribery-charges-connection-venezuela-bribery-scheme>; Press Release, US DOJ, 'Two Businessmen Charged with Foreign Bribery in Connection with Venezuela Bribery Scheme' (26 February 2019) <https://www.justice.gov/opa/pr/two-businessmen-charged-foreign-bribery-connection-venezuela-bribery-scheme>;

state-controlled oil company, as well as indictments in connection with alleged corruption at Corporación de Abastecimiento y Servicios Agrícola (CASA),[63] Venezuela's state-owned food corporation; Comité Local de Abastecimiento y Producción (CLAP),[64] a Venezuelan state-controlled food and medicine distribution programme; and Petropiar,[65] a joint venture between Venezuela's state-owned and state-controlled energy company and an American oil company. Similarly, the US DOJ has prosecuted individuals for paying bribes to officials at Empresa

---

Press Release, US DOJ, 'Texas Businessman Pleads Guilty to Money Laundering Charges in Connection with Venezuela Bribery Scheme' (30 October 2018) <https://www.justice.gov/opa/pr/texas-businessman-pleads-guilty-money-laundering-charges-connection-venezuela-bribery-scheme>; Press Release, US DOJ, 'Two Members of Billion-Dollar Venezuelan Money Laundering Scheme Arrested' (25 July 2018) <https://www.justice.gov/opa/pr/two-members-billion-dollar-venezuelan-money-laundering-scheme-arrested>; Press Release, US DOJ, 'Businessman Pleads Guilty to Foreign Bribery and Tax Charges in Connection with Venezuela Bribery Scheme' (16 June 2018) <https://www.justice.gov/opa/pr/businessman-pleads-guilty-foreign-bribery-and-tax-charges-connection-venezuela-bribery-scheme>; Press Release, US DOJ, 'Five Former Venezuelan Government Officials Charged in Money Laundering Scheme Involving Foreign Bribery' (12 February 2018) <https://www.justice.gov/opa/pr/five-former-venezuelan-government-officials-charged-money-laundering-scheme-involving-forei-0>; Press Release, US DOJ, 'Florida Businessman Pleads Guilty to Foreign Bribery Charges in Connection With Venezuela Bribery Scheme' (11 October 2017) <https://www.justice.gov/opa/pr/florida-businessman-pleads-guilty-foreign-bribery-charges-connection-venezuela-bribery-scheme>; Press Release, US DOJ, 'Two Businessmen Plead Guilty to Foreign Bribery Charges in Connection with Venezuela Bribery Schemes' (10 January 2017) <https://www.justice.gov/opa/pr/two-businessmen-plead-guilty-foreign-bribery-charges-connection-venezuela-bribery-schemes>; Press Release, US DOJ, 'Miami Businessman Pleads Guilty to Foreign Bribery and Fraud Charges in Connection with Venezuela Bribery Scheme' (23 March 2016) <https://www.justice.gov/opa/pr/miami-businessman-pleads-guilty-foreign-bribery-and-fraud-charges-connection-venezuela>.

63 See Press Release, US DOJ, 'Executive Arrested and Charged for Bribery and Money-Laundering Scheme' (4 August 2021) <https://www.justice.gov/opa/pr/executive-arrested-and-charged-bribery-and-money-laundering-scheme>; Indictment, United States v. Naman Wakil, No. 21-20406-CR (S.D. Fla. 29 July 2021) <https://www.justice.gov/criminal-fraud/file/1430096/download>.

64 See Press Release, US DOJ, 'Five Individuals Charged with Money Laundering in Connection with Alleged Venezuela Bribery Scheme' (21 October 2021) <https://www.justice.gov/opa/pr/five-individuals-charged-money-laundering-connection-alleged-venezuela-bribery-scheme>.

65 See Press Release, US DOJ, 'Venezuelan Businessman Charged in Bribery and Money Laundering Scheme' (24 August 2022) <https://www.justice.gov/opa/pr/venezuelan-businessman-charged-bribery-and-money-laundering-scheme>.

Pública de Hidrocarburos del Ecuador (PetroEcuador),[66] a state-owned oil company in Ecuador, and Ecuador's state-owned insurance companies, Seguros Sucre S.A. and Seguros Rocafuerte S.A.[67]

While the US DOJ has not yet prosecuted PetroEcuador, it resolved two corporate investigations involving corrupt payments to PetroEcuador.[68] One of the cases also involved alleged payments to PDVSA officials.[69] Additionally, in June 2019, Citgo Petroleum Corp (Citgo) confirmed that it received a subpoena requesting information relating to bribery in Venezuela.[70] Citgo has been implicated in certain individuals' guilty pleas, but has not been publicly charged, nor has it reached a public corporate resolution.[71]

Coordination among US enforcement agencies

In May 2018, the US DOJ formalised its position on coordination among US law enforcement and regulatory agencies and their non-US counterparts in a policy requiring US DOJ attorneys to coordinate with other law enforcement partners in the United States and counterparts abroad (the Anti-Piling On Policy).[72] The

66 See Press Release, US DOJ, 'Businessman Sentenced for Foreign Bribery and Money Laundering Scheme Involving PetroEcuador Officials' (28 January 2021) <https://www.justice.gov/opa/pr/businessman-sentenced-foreign-bribery-and-money-laundering-scheme-involving-petroecuador>; Press Release, US DOJ, 'Financial Advisor Pleads Guilty to Money Laundering Charge in Connection With Bribery Scheme Involving Ecuadorian Officials' (11 September 2018) <https://www.justice.gov/opa/pr/financial-advisor-pleads-guilty-money-laundering-charge-connection-bribery-scheme-involving>.

67 See Press Release, US DOJ. 'Three Men Charged in Ecuadorian Bribery and Money Laundering Scheme' (19 July 2022) <https://www.justice.gov/opa/pr/three-men-charged-ecuadorian-bribery-and-money-laundering-scheme>.

68 See Vitol Deferred Prosecution Agreement (footnote 51, above); Sargeant Marine Press Release (footnote 51, above).

69 See Sargeant Marine Press Release (footnote 51, above).

70 See Wethe, David; Kassai, Lucia, 'Citgo Gets U.S. Subpoena Related to Venezuela Bribery Probe', *Bloomberg* (3 June 2019) <https://www.bloomberg.com/news/articles/2019-06-03/citgo-gets-u-s-subpoena-related-to-venezuela-bribery-probe>.

71 *id.*; see, e.g., Press Release, US DOJ, 'Former Venezuelan Official Pleads Guilty in Connection with International Bribery and Money Laundering Scheme' (23 March 2021) <https://www.justice.gov/opa/pr/former-venezuelan-official-pleads-guilty-connection-international-bribery-and-money>; Indictment, *United States v. Jose Luis De Jongh-Atencio*, No. 4:20-CR-305 (S.D. Tex. 16 July 2020) <https://www.justice.gov/criminal-fraud/file/1307276/download>.

72 US DOJ, Justice Manual §§ 1-12.100 – Coordination of Corporate Resolution Penalties in Parallel and/or Joint Investigations and Proceedings Arising from the Same Misconduct (May 2018) [hereinafter Justice Manual 1-12.100] <https://www.justice.gov/jm/jm-1-12000-coordination-parallel-criminal-civil-regulatory-and-administrative-proceedings#1-12.100>.

Anti-Piling On Policy recognises that coordination among regulators avoids 'unfair duplicative penalties' that 'deprive a company of the benefits of certainty and finality ordinarily available through a full and final settlement.'[73] The policy does not require the US DOJ to refrain from imposing its own penalties. Instead, it merely requires prosecutors to consider whether multiple resolutions are necessary.[74] To date, the Biden Administration has not signalled an intention to depart from the policy.[75]

Companies whose shares or American Depositary Receipts (ADRs) are publicly traded in the United States are subject to US SEC regulation. These companies may be subject to investigations and penalties by both the US DOJ and US SEC for the same alleged violations of the FCPA. The Anti-Piling On Policy may provide a basis for such companies to contend that the imposition of substantial penalties by both agencies is unnecessary and unwarranted.

Recent enforcement actions suggest that the US DOJ has a continued willingness to decline to prosecute cases involving resolutions with other regulators. For example, of the nine companies to which the US DOJ has issued formal declinations since 2018, five involved publicly traded US companies that reached resolutions with the US SEC,[76] two involved companies that were under investi-

---

73 Deputy Attorney General Rod Rosenstein, Remarks as Prepared for the New York City Bar White Collar Crime Institute, New York (9 May 2018) [hereinafter Rosenstein Remarks, 9 May 2018] <https://www.justice.gov/opa/speech/deputy-attorney-general-rod-rosenstein-delivers-remarks-new-york-city-bar-white-collar>.

74 See, e.g., Dobrik, Adam 'Beam Suntory case highlights piling-on tension' (5 November 2020) <https://globalinvestigationsreview.com/just-anti-corruption/beam-suntory-case-highlights-piling-tension>.

75 See Press Release, US DOJ 'Deputy Assistant Attorney General Lisa H. Miller Delivers Remarks at the University of Southern California Gould School of Law on Corporate Enforcement and Compliance' (16 February 2023) <https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-lisa-h-miller-delivers-remarks-university-southern>.

76 See, e.g., Letter from Robert Zink, Chief, Fraud Section, US DOJ, to Mark Schamel et al., Womble Bond Dickinson LLP (5 August 2020) <https://www.justice.gov/criminal-fraud/file/1301826/download>; Letter from Matthew Kruger [sic], US Attorney, E.D. Wis. and Robert Zink, Chief, Fraud Section, US DOJ, to David W Simon et al., Foley & Lardner LLP (19 September 2019) <https://www.justice.gov/criminal-fraud/file/1205341/download>; Letter from Sandra Moser, Acting Chief, Fraud Section, US DOJ, to Caz Hashemi, Wilson Sonsini Goodrich & Rosati, and Rohan Virginkar, Foley & Lardner LLP (20 December 2018) [hereinafter Letter from Sandra Moser to Caz Hashemi] <https://www.justice.gov/criminal-fraud/file/1122966/download>; Letter from Craig Carpentino [sic], US Attorney, Dist. of N.J., and Sandra Moser, Acting Chief, Fraud Section, Criminal Division, US DOJ, to Peter Spivack, Hogan Lovells (23 April 2018) <https://www.justice.gov/criminal-fraud/file/1055401/download>.

gation by UK authorities,[77] and one by German authorities.[78] Even when the US DOJ provides a formal declination, however, it may still require a company to disgorge ill-gotten profits.[79]

Notwithstanding the Anti-Piling On Policy, the potential for overlapping enforcement remains. The United States Commodity Futures Trading Commission (CFTC) recently entered the foreign-corruption space, despite its stated intention to avoid 'pil[ing] onto other existing investigations.'[80] In March 2019, the CFTC issued an Enforcement Advisory regarding 'self-reporting and cooperation for violations of the Commodity Exchange Act (CEA) involving foreign corrupt practices' and indicated that the agency would pursue foreign

77 Letter from Daniel S Kahn, Deputy Chief, US DOJ, to Matthew Reinhard, Miller & Chevalier Chartered (20 August 2018) <https://www.justice.gov/criminal-fraud/page/file/1088621/download> (noting that one reason for declination was 'the fact that [Guralp Systems Limited], a U.K. company with its principal place of business in the U.K., is the subject of an ongoing parallel investigation by the U.K.'s Serious Fraud Office for violations of law relating to the same conduct and has committed to accepting responsibility for that conduct with the SFO'). The final declination involved a Barbados-based company that earned less than US$100,000 in illicit profits from the bribery scheme and voluntarily self-disclosed the conduct. Following the declination, US DOJ charged the company's former Chief Executive Officer and Senior Vice President; Letter from Joseph S. Beemsterboer, US DOJ, to F. Joseph Warin, Gibson, Dunn & Crutcher LLP (18 March 2022) <https://www.justice.gov/criminal-fraud/file/1486266/download>.

78 Letter from Glenn S Leon, US DOJ, to Peter Spivack, Hogan Lovells US LLP (21 December 2022) <https://www.justice.gov/criminal-fraud/file/1559236/download>.

79 See Letter from Craig Carpenito, US Attorney, District of N.J., and Robert Zink, Acting Chief, Fraud Section, Criminal Division, US DOJ, to Karl H Buch and Grayson D Stratton, DLA Piper LLP, and Kathryn H Ruemmler and Douglas N Greenburg, Latham & Watkins LLP (13 February 2019) <https://www.justice.gov/criminal-fraud/file/1132666/download>; Letter from Sandra Moser to Caz Hashemi (footnote 76, above).

80 CFTC Director of Enforcement James M. McDonald, 'Remarks as Prepared for the American Bar Association's National Institute on White Collar Crime' (6 March 2019) <https://www.cftc.gov/PressRoom/SpeechesTestimony/opamcdonald2>.

corruption that affected commodities and derivatives markets.[81] Since December 2020, the CFTC has brought two enforcement actions related to foreign corruption.[82] Two other companies have disclosed ongoing investigations.[83]

Similarly, *Operation Car Wash* resulted in substantial and, at times, overlapping corporate fines and penalties imposed by US, Latin American and other enforcement and regulatory entities, raising questions about the benefits of the policy when applied in practice. Because Latin American authorities do not have policies similar to the Anti-Piling On Policy, companies that resolve their potential liability in the US without resolving their exposure throughout Latin America may find themselves subject to crippling additional fines and penalties for largely similar or related conduct.[84]

---

81 Press Release, CFTC, 'CFTC Division of Enforcement Issues Advisory on Violations of the Commodity Exchange Act Involving Foreign Corrupt Practices' (6 March 2019) <https://www.cftc.gov/PressRoom/PressReleases/7884-19>.

82 Press Release, CFTC, 'CFTC Orders Vitol Inc. to Pay $95.7 Million for Corruption-Based Fraud and Attempted Manipulation' (3 December 2020) <https://www.cftc.gov/PressRoom/PressReleases/8326-20>; Press Release, 'CFTC Orders Glencore to Pay $1.186 Billion for Manipulation and Corruption' (24 May 2022) <https://www.cftc.gov/PressRoom/PressReleases/8534-22>.

83 See Tokar, Dylan, 'Derivatives Regulator Uses Dodd-Frank Rule to Target Foreign Bribery', *The Wall Street Journal* (22 December 2020) <https://www.wsj.com/articles/derivatives-regulator-uses-dodd-frank-rule-to-target-foreign-bribery-11608633001>; Kagubare, Ines, 'CFTC investigates another commodity trader in PetroEcuador scheme' (30 September 2021) <https://globalinvestigationsreview.com/just-anti-corruption/bribery/cftc-investigates-another-commodity-trader-in-petroecuador-scheme>.

84 Brazil has begun to coordinate penalties among internal regulators, which may signal a willingness to adopt an anti-piling policy. See, e.g., Federative Republic of Brazil, "Acordo de Cooperação Técnica que Entre si Celebram o Ministério Público Federal, a Controladoria-Geral da União (CGU), a Advocacia Geral da União (AGU), o Ministério da Justiça e Segurança Pública (MJSP) e o Tribunal de Contas da União (TCU) em Matéria de Combate à Corrupção no Brasil, Especialmente em Relação aos Acordos de Leniência da Lei No. 12.846, de 2013" [Technical Cooperation Agreement Among the Federal Public Prosecutor's Office, Comptroller-General's Office (CGU), Attorney General's Office (AGU), Ministry of Justice and Public Security (MJSP), and Federal Court of Accounts (TCU) Regarding Anti-Corruption in Brazil, Particularly Leniency Agreements Under Law No. 12.846 of 2013] (6 August 2020) <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/Acordo6agosto.pdf>.

Global coordination

During the past several years, there has also been an increase in global anti-corruption enforcement coordination, particularly with respect to investigations involving Latin America.[85] As Assistant Attorney General Kenneth A Polite acknowledged in January 2023, '[t]he vast majority of our FCPA resolutions in recent years are the result of cooperation and coordination with foreign and domestic authorities.'[86] Since 2020, the US DOJ and US SEC reportedly received cooperation from approximately 31 countries in cases brought under the FCPA.[87] Since 2014, Brazil has assisted in at least 21 US DOJ or US SEC investigations that resulted in corporate resolutions. In some instances, the US DOJ has deferred to foreign authorities' investigations and prosecutions, or credited companies for fines paid to foreign authorities for related conduct.[88]

Recent resolutions of corruption investigations involving conduct in Latin America, including conduct uncovered during *Operation Car Wash*, reflect this increased cooperation. For example, in September 2022, GOL Linhas Aéreas Inteligentes S.A. (GOL) agreed to pay over US$41 million to resolve parallel investigations by the US SEC, US DOJ, and Brazilian authorities relating to

---

85 Allen II, Warren T; Bosworth, B Michelle, 'Multi-Jurisdictional Anti-Corruption Investigation and Enforcement Trends and Developments' in The Review of Securities & Commodities Regulation, Vol. 51, No. 17 (2018).

86 Kenneth A Polite, Jr, Remarks at Georgetown Law Center, 'Revisions to the Criminal Division's Corporate Enforcement Policy' (17 January 2023) <https://www.justice.gov/opa/speech/assistant-attorney-general-kenneth-polite-jr-delivers-remarks-georgetown-university-law>.

87 Press Release, US DOJ, Former Comptroller General of Ecuador Indicted for Alleged Bribery and Money Laundering Scheme (29 March 2022) <https://www.justice.gov/opa/pr/former-comptroller-general-ecuador-indicted-alleged-bribery-and-money-laundering-scheme> (Ecuador, Brazil, Panamá and Curaçao); *United States v. Stericycle, Inc*., No. 8:22-cr-00345 (D. Md.) (Brazil); *United States v. ABB South Africa (PTY) Ltd.*, No. 1:22-CR-222 (E.D. Va. Dec. 2, 2022) (South Africa); *United States v. Glencore International A.G.* (United Kingdom and Switzerland); *United States v. Goldman Sachs* (Singapore, Malaysia, China); *United States v. Airbus SE*, No. 20-cr-21 (D.D.C. Jan. 31, 2020) (France).

88 See, e.g., Press Release, US DOJ, 'Rolls-Royce plc Agrees to Pay $170 Million Criminal Penalty to Resolve Foreign Corrupt Practices Act Case' (17 January 2017) [hereinafter US DOJ Press Release, 17 January 2017] <https://www.justice.gov/opa/pr/rolls-royce-plc-agrees-pay-170-million-criminal-penalty-resolve-foreign-corrupt-practices-act>; Press Release, US DOJ, 'Keppel Offshore & Marine Ltd and U.S. Based Subsidiary Agree to Pay $422 Million in Global Penalties to Resolve Foreign Bribery Case' (22 December 2017) [hereinafter US DOJ Press release, 22 December 2017] <https://www.justice.gov/opa/pr/keppel-offshore-marine-ltd-and-us-based-subsidiary-agree-pay-422-million-global-penalties>.

improper conduct in Brazil.[89] Similarly, in April 2022, Stericycle, Inc. agreed to pay more than US$84 million to resolve parallel investigations by the US SEC, US DOJ and Brazilian authorities regarding misconduct in Argentina, Brazil and Mexico.[90]

In January 2020, Airbus SE agreed to pay combined penalties of more than US$3.9 billion to resolve charges with the United States, France and the United Kingdom, arising out of a scheme to use third-party business partners to bribe government officials and non-government airline executives.[91] The investigations spanned conduct in more than a dozen countries, including Brazil, Colombia and Mexico. Notably, the UK Serious Fraud Office (SFO) and the French National Financial Prosecutor's Office (PNF) entered into a joint investigation agreement to facilitate their investigations, with each office focusing on conduct in different countries.[92] Given that Airbus is not a US issuer or domestic concern and that there was only limited territorial contact over the corrupt conduct, the US authorities gave Airbus credit for any payments to the SFO and the PNF.[93] To date, Latin American authorities have not publicly announced investigations or charges against Airbus.

---

89 Press Release, US DOJ, 'GOL Linhas Aéreas Inteligentes S.A. Will Pay Over $41 Million in Resolution of Foreign Bribery Investigations in the United States and Brazil' (15 September 2022) <https://www.justice.gov/opa/pr/gol-linhas-reas-inteligentes-sa-will-pay-over-41-million-resolution-foreign-bribery>.

90 Press Release, US DOJ, 'Stericycle Agrees to Pay Over $84 Million in Coordinated Foreign Bribery Resolution' (20 April 2022) <https://www.justice.gov/opa/pr/stericycle-agrees-pay-over-84-million-coordinated-foreign-bribery-resolution>.

91 Press release, US DOJ, 'Airbus Agrees to Pay over $3.9 Billion in Global Penalties to Resolve Foreign Bribery and ITAR Case' (31 January 2020) [hereinafter US DOJ Press release, 31 January 2020] <https://www.justice.gov/opa/pr/airbus-agrees-pay-over-39-billion-global-penalties-resolve-foreign-bribery-and-itar-case>.

92 Statement of Facts Prepared Pursuant to Paragraph 5(1) of Schedule 17 to the Crime and Courts Act 2013, *Regina v. Airbus SE* (filed 31 January 2020) <www.tisrilanka.org/wp-content/uploads/2020/01/R-v-Airbus-Statement-of-Facts.pdf>. ('The PNF focused its investigations more particularly on Airbus and its divisions' conduct in the following countries: United Arab Emirates, China, South Korea, Nepal, India, Taiwan, Russia, Saudi Arabia, Vietnam, Japan, Turkey, Mexico, Thailand, Brazil and Kuwait. The SFO focused its investigations on Airbus and its divisions' conduct in the following countries: South Korea, Indonesia, Sri Lanka, Malaysia, Taiwan, Ghana, Colombia and Mexico. Within this scope, the PNF and SFO selected a representative sample of the markets and concerns involved.').

93 Deferred Prosecution Agreement Paragraph 4, *United States v. Airbus SE*, No. 1:20-cr-00021-TFH (D.D.C. 28 January 2020) <https://www.justice.gov/criminal-fraud/file/1242051/download> (noting that Airbus 'is neither a U.S. issuer nor a domestic concern and the territorial jurisdiction over the corrupt conduct is limited; in addition . . . France's and the United Kingdom's interests over the Company's corruption-related conduct, and

Coordination between countries has moved beyond coordinated enforcement and into legislative alignment. Chapter 27 of the United States-Mexico-Canada Agreement (USMCA), which went into effect on 1 July 2020,[94] requires not only cross-border cooperation between the countries' respective enforcement authorities, but for each country to 'adopt or maintain legislative and other measures' that criminalise bribery, solicitation or acceptance of a bribe and embezzlement or misappropriation of public funds, among other measures.[95] Each country is generally bound to enforce its anti-corruption laws, but retains discretion with respect to the particular enforcement, and parties do not have a real recourse if they believe another party has failed to enforce its anti-corruption laws in compliance with the USMCA.[96]

Similarly, in November 2021, the Organisation for Economic Co-operation and Development (OECD) Council adopted the 2021 Recommendation for Further Combating Bribery of Foreign Public Officials in International Business Transactions.[97] With this Recommendation, the forty-four countries party to the OECD Anti-Bribery Convention, including seven Latin American countries, agree to new measures geared toward 'strengthening enforcement of foreign bribery laws, addressing the demand side of foreign bribery, enhancing international co-operation, introducing principles on the use of non-trial resolutions in foreign bribery cases, incentivising anti-corruption compliance by companies, and providing comprehensive and effective protection for reporting persons.'[98]

---

jurisdictional bases for a resolution, are significantly stronger, and thus the [DOJ has] deferred to France and the United Kingdom to vindicate their respective interests as those countries deem appropriate, and the [DOJ has] taken into account these countries' determination of the appropriate resolution into all aspects of the U.S. resolution[.]').

94 Office of the US Trade Representative, U.S. Mex. Can. Agreement <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement>.

95 Office of the US Trade Representative, 'U.S.-Mex.-Can. Agreement, Chapter 27, Article 27.3-1: Measures to Combat Corruption' <https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/27_Anticorruption.pdf>.

96 Id. at Articles 27.6.1-2 and 27.8.1-3.

97 OECD, 2021 OECD Anti-Bribery Recommendation (26 November 2021) [hereinafter 2021 OECD Anti-Bribery Recommendation] <https://www.oecd.org/corruption/2021-oecd-anti-bribery-recommendation.htm>.

98 *id.*

Individuals

US enforcement

The US DOJ and the US SEC continue to prioritise individual accountability in enforcing the FCPA for conduct in Latin America and elsewhere. US DOJ policy emphasises the importance of pursuing individual criminal liability as the strongest deterrent against future corporate wrongdoing and requires companies to identify individuals who were 'substantially involved in or responsible for the criminal conduct' to earn cooperation credit.[99] In January 2023, Assistant Attorney General Kenneth A Polite remarked, 'Our number one goal in this area – as we have repeatedly emphasized – is individual accountability. And we can hold accountable those who are criminally culpable – no matter their seniority – when companies come forward and cooperate with our investigation.'[100]

This prioritisation has led to an overall increase in FCPA charges against individuals since 2007. In 2022, the US DOJ and US SEC publicly announced 13 charges against individuals.[101] Those numbers were 18 in 2021 and 32 in 2020.[102] Even though 13 is substantially below the historical high of 43 in 2019, the US DOJ has charged an average of 23 individuals per year in the past 10 years, up significantly from just nine individuals in 2007.

The US DOJ and the US SEC also continue to rely on cooperating companies to assist in individual prosecutions, a factor the US DOJ has cited in declining to bring corporate criminal charges or in providing cooperation credit.[103] In October 2021, Deputy Attorney General Monaco announced a more stringent requirement that companies must 'identify all individuals involved in the misconduct'

---

99 Rosenstein, Rod J, Deputy Attorney General, Remarks as Prepared for the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act (29 November 2018) <https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0>; see Justice Manual, 9-28.210 – Focus on Individual Wrongdoers <https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations#9-28.210>.

100 Remarks by Kenneth A Polite, Jr (footnote 86, above).

101 Stanford Law School Foreign Corrupt Practices Act Clearinghouse, 2022 FCPA Year in Review (2023) <https://fcpa.stanford.edu/fcpac-reports/2022-fcpa-year-in-review.pdf>.

102 *id.*

103 See, e.g., Letter from Richard P Donoghue, US Attorney, E.D.N.Y. and Sandra L Moser, Acting Chief, Fraud Section, Criminal Division, US DOJ, to Adam B Siegel, Freshfields Bruckhaus Deringer US LLP (23 August 2018) <https://www.justice.gov/criminal-fraud/page/file/1089626/download> ('[T]he Department has decided to close its investigation of this matter based on a number of factors, including . . . the fact that the Department has been able to identify and charge the culpable individuals.'); Remarks by Kenneth A Polite, Jr (footnote 86, above).

and provide 'all non-privileged information about individual wrongdoing' to be eligible for any cooperation credit.[104] Under the prior administration's policy, qualifying companies could get cooperation credit for identifying only individuals that were 'substantially involved' in or responsible for potential criminal misconduct.[105] Deputy Attorney General Monaco explained that the prior policy was rescinded because it was vague and 'afford[ed] companies too much discretion in deciding who should and should not be disclosed to the government.'[106]

Of the 73 companies that reached large,[107] FCPA-related resolutions with the US SEC or the US DOJ (or both) between 2015 and February 2023, the US government pursued at least 49 individuals related to the conduct of at least 21 companies. Most of the individuals were employed by the settling company or its subsidiaries, held senior positions or were directly involved in authorising, causing or concealing bribe payments. Those individuals prosecuted by the US DOJ who were not directly employed by the settling company were generally third-party consultants who paid bribes on behalf of the company.[108]

The United States is also increasingly using sanctions as a tool to curb corruption in Latin America. In particular, the Office of Foreign Assets Control (OFAC) of the US Department of the Treasury can prohibit individuals from entering the US, freeze US assets and prohibit companies owned by sanctioned individuals from conducting business in the US or with US persons or companies.[109] The US Department of State can also bar foreign government officials

104 Remarks by Lisa Monaco, 28 October 2021 (footnote 10, above).

105 *id.*

106 *id.*

107 Combined monetary payments of US$9,875,000 or greater.

108 See, e.g., *Rolls-Royce PLC* (Petros Contoguris, Andreas Kohler).

109 See Exec. Order No. 13818, 82 Fed. Reg. 60839 (Dec. 20, 2017); see also Press Release, U.S. Department of the Treasury, 'Combating Global Corruption and Human Rights Abuses' (9 December 2022) ('All property and interests in property of individuals or entities . . . that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to [OFAC.] In addition, any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons are also blocked . . . [and] all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons are prohibited. The prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any blocked person or the receipt of any contribution or provision of funds, goods, or services from any such person.').

involved in 'significant corruption' and their immediate family members from entering the US.[110] The sanctions are meant to support democratic institutions by 'encourag[ing] a positive change of behaviour by the identified persons'.[111]

For example, the US Department of State imposed visa restrictions on the former president of Paraguay, Horacio Cartes Jara, and the current vice-president Hugo Velazquez Moreno, in July and August 2022, respectively.[112] Subsequently, in January 2023, OFAC sanctioned both individuals, noting the United States' 'continued commitment to combatting systemic corruption, addressing state capture, bolstering democratic institutions and promoting accountability in Paraguay.'[113] Also in January 2023, the US Department of State designated former President of Panama, Ricardo Alberto Martinelli Berrocal, for accepting bribes in exchange for government contracts while he was President.[114] OFAC has also levied sanctions against current and former government officials in Nicaragua, El Salvador and Guatemala.[115]

---

110 Section 7031(c) of the Department of State, Foreign Operations and Related Programs Appropriations Act, 2018 Pub. L. 115-141, Div. K., 132 Stat. 348 (23 March 2018).

111 Press Release, US Department of the Treasury, 'Treasury Sanctions Six Nicaraguan Officials Ahead of Ortega-Murillo Sham Inauguration' (10 January 2022) <https://home.treasury.gov/news/press-releases/jy0552>.

112 Press Release, US Embassy in Paraguay, 'Designation of Former Paraguayan President Horacio Cartes for Involvement in Significant Corruption' (22 July 2022) <https://py.usembassy.gov/designation-of-former-paraguayan-president-horacio-manuel-cartes-jara-for-involvement-in-significant-corruption/>; see also Press Release, US Embassy in Paraguay 'Designation of Paraguayan Vice President Hugo Velazquez and EBY Legal Counsel Juan Carlos Duarte for Involvement in Significant Corruption' (22 July 2022) <https://py.usembassy.gov/designation-of-paraguayan-vice-president-hugo-velazquez-and-eby-legal-counsel-juan-carlos-duarte-for-involvement-in-significant-corruption>.

113 Press Release, US Department of State, 'Sanctioning Senior Paraguayan Officials for Corruption' (26 January 2023) <https://www.state.gov/sanctioning-senior-paraguayan-officials-for-corruption/>.

114 Press Release, US Department of State, 'Designation of Former President of Panama Ricardo Alberto Martinelli Berrocal for Involvement in Significant Corruption' (25 January 2023) <https://www.state.gov/designation-of-former-president-of-panama-ricardo-alberto-martinelli-berrocal-for-involvement-in-significant-corruption/>.

115 See Press Release (footnote 111, above) (announcing sanctions of 6 Nicaraguan officials); see also Press release, US Department of the Treasury, 'Treasury Sanctions Over 40 Individuals and Entities Across Nine Countries Connected to Corruption and Human Rights Abuse' (9 December 2022) <https://home.treasury.gov/news/press-releases/jy1155> (announcing sanctions of officials from Guatemala and El Salvador for their role in corrupt practices while in office).

Local enforcement in Latin America

While US agencies have pursued bribe payers and facilitators, as well as employees of state-owned enterprises, Latin American authorities have aggressively prosecuted politicians and high-level government officials. In efforts to ensure accountability of government officials, prosecutors have sought to hold former senior politicians in pretrial detention, try them in absentia or imprison them after their conviction is upheld by an appellate court. The latter practice, however, was rejected in Brazil in 2019, when the then-former president, Luiz Inácio Lula da Silva, was released from prison on the basis of a Brazilian Supreme Court decision that defendants cannot be imprisoned until they fully exhaust their appeals, which can take years.[116] The Supreme Federal Court quashed Lula's sentence in 2021, and annulled the investigation because the former judge was not considered to be impartial.[117] Three years after his imprisonment, Lula was re-elected to serve a third term as president of Brazil.[118]

Still, aggressive prosecution of high-level officials continues across Latin America. In Peru, for example, every president elected from 1985 to December 2022, 'with the exception of one interim leader who served for just eight months– has either been impeached, imprisoned or sought in criminal investigations.'[119] For instance, in February 2023, the Attorney General's Office opened an investigation

116 See Federal Supreme Court (Brazil) (7 November 2019) <http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=464261&ori>; Boadle, Anthony, 'Top Brazil court ends early prison rule in decision that could free Lula', *Reuters* (7 November 2019) <https://www.reuters.com/article/us-brazil-corruption-court/top-brazil-court-ends-early-prison-rule-in-decision-that-could-free-lula-idUSKBN1XI02O>.

117 'Brazil: Criminal Proceedings Against Former President Lula da Silva Violated Due Process Guarantees, UN Human Rights Committee Finds', UN (28 April 2022) <https://www.ohchr.org/en/press-releases/2022/04/brazil-criminal-proceedings-against-former-president-lula-da-silva-violated>.

118 Rocha, Camilo, 'Lula da Silva Will Return To Brazil's Presidency In Stunning Comeback', CNN (31 October 2022) <https://www.cnn.com/2022/10/30/americas/brazil-election-lula-da-silva-wins-intl/index.html>.

119 Bristow, Matthew, 'Impeached, Jailed, Wanted: President Is a Dangerous Job in Peru', *Bloomberg* (9 December 2022) <https://www.bloomberg.com/news/articles/2022-12-09/impeached-jailed-wanted-president-is-a-dangerous-job-in-peru>. The list of presidents in the last four decades that has either been impeached, imprisoned or sought in criminal investigations includes Pedro Castillo (2021-2022), Manuel Merino (Nov. 10-15, 2020), Martin Vizcarra (2018-2020), Pedro Pablo Kuczynski (2016-2018), Ollanta Humala (2011-2016), Alan Garcia (1985-1990/2006-2011), Alejandro Toledo (2001-2006) and Alberto Fujimori (1990-2000).

against former president Pedro Castillo for corruption dating back to 2021.[120] Castillo has been accused of influence peddling, organized crime and being an accomplice to collusion during his administration.[121] Castillo has been detained since December 2022, after he attempted to dissolve congress and was ousted.[122] Also, in February 2023, the US Department of State agreed to extradite former President Alejandro Toledo to Peru, where he faces corruption charges.[123] Toledo was said to have taken a US$20 million bribe during his term as president.[124]

In Argentina, Cristina Fernández de Kirchner (former President and Senator and current Vice President) was found guilty on 6 December 2022 in a US$1 billion fraud case, was sentenced to six years in prison and given a lifelong ban on holding public office.[125] Fernández de Kirchner has temporary immunity due to her current role as vice-president and will not immediately go to jail, but she can appeal her conviction.[126] A separate case against Fernández de Kirchner was announced in August 2018, triggered by the publication of several notebooks written by the driver of a high-ranking public official in Argentina (*Los Cuadernos*: the *Notebooks* scandal). The notebooks allegedly detail bribes paid to

120 Madry, Kylie, 'Peru's Top Prosecutor Opens Corruption Probe of Ex-President Castillo', *Reuters* (21 February 2023) <https://www.reuters.com/world/americas/perus-top-prosecutor-opens-corruption-probe-ex-president-castillo-2023-02-21/>.

121 Severi, Misty, 'Peru Launches Collusion Investigation Into Former President Pedro Castillo', Washington Examiner (22 February 2023) <https://www.washingtonexaminer.com/news/crime/peru-launches-collusion-investigation-into-former-president>.

122 See *id.*

123 O'Boyle, Brendan, 'U.S. Agrees To Extradite Former Peruvian President Toledo, Says Peru', Reuters (21 February 2023) <https://www.reuters.com/world/americas/us-agrees-extradite-former-peruvian-president-toledo-peru-attorney-generals-2023-02-22/>.

124 'U.S. judge orders release of Peru ex-president on bail due to coronavirus outbreak', *Reuters* (19 March 2020) <https://www.reuters.com/article/us-peru-corruption-toledo-idUSKBN21703W>.

125 Booth, Amy, 'Argentina's Cristina Fernández Sentenced To Six Years In $1bn Fraud Case' (6 December 2022) <https://www.theguardian.com/world/2022/dec/06/cristina-fernandez-de-kirchner-argentina-sentenced-prison-fraud-case>.

126 Akbarzai, Sahar, 'Argentina's Cristina Fernández De Kirchner Sentenced To Six Years In Prison For Corruption', CNN (7 December 2022) <https://www.cnn.com/2022/12/07/americas/argentina-vice-president-fernndez-de-kirchner-sentenced-intl-hnk/index.html>.

public officials in connection with contracts for public works.[127] The scandal has implicated dozens of public officials and business owners. This case is expected to go to trial, possibly in 2023.[128]

In Bolivia, prosecutors issued an arrest warrant for former president Evo Morales, who resigned in October 2019, following a disputed election,[129] although the arrest warrant was annulled a year later.[130] In January 2020, the interim government opened a corruption investigation into almost 600 former Morales officials, including the former president.[131] On 4 January 2023, former Bolivian minister of government Arturo Carlos Murillo Prijic was sentenced to 70 months in prison for conspiracy to commit money laundering after he received bribes in exchange for helping a US company win a contract from the Bolivian government.[132]

In Mexico, the Special Prosecutor's Office for Combating Corruption opened 1,668 investigations between March 2019 and March 2021. Only 2.3 per cent of the complaints it received, though, name a private corporation as an alleged offender.[133] The Special Prosecutor's Office has not published additional information regarding the investigations.

---

127 Do Rosario, Jorgelina; Gillespie, Patrick, 'Why Kirchner's Comeback Goes Through Argentine Court', *Bloomberg* (12 August 2019) <https://www.bloomberg.com/news/articles/2019-05-30/why-kirchner-s-comeback-goes-through-argentine-court-quicktake>.

128 Elliott, Lucinda, 'Argentina's Cristina Fernández de Kirchner convicted of corruption', *Financial Times* (6 December 2022) <https://www.ft.com/content/553db204-5f14-4f23-b995-616788973cc7>.

129 'Bolivia issues arrest warrant for Evo Morales', *Financial Times* (8 December 2019) <https://www.ft.com/content/aa5ace2e-21e6-11ea-b8a1-584213ee7b2b>.

130 'Juez boliviano anula orden de arresto contra exlíder Morales', *Reuters* (26 October 2020) <https://www.reuters.com/article/justicia-bolivia-morales-idLTAKBN27C02G>.

131 'Bolivia opens probe into 600 former Morales officials', France24 (8 January 2020) <https://www.france24.com/ en/20200108-bolivia-opens-probe-into-600-former-morales-officials>.

132 Press release, US DOJ, 'Former Bolivian Minister of Government Sentenced for Bribery Conspiracy' (4 January 2023) <https://www.justice.gov/opa/pr/former-bolivian-minister-government-sentenced-bribery-conspiracy>.

133 'Informe Anual de Actividades y Resultados 2021', Fiscalía Especializada en Combate a la Corrupción (11 March 2021) <https://sna.org.mx/wp-content/uploads/2021/03/INFORME_ANUAL_2020-2021_FISCAL%C3%8DA_ANTICORRUPCI%C3%93N_2021.pdf>.

In Ecuador, the former vice-president Jorge Glas was sentenced to six years in prison in December 2017 for corruption unearthed by *Operation Car Wash*.[134] He was released from prison on 28 November 2022, after a local judge approved alternative corrective measures.[135] As of November 2019:

> *the Attorney General's Office had indicted twenty-four former government and private-sector officials, including [former President] Correa and Glas, in an investigation of an alleged bribery scheme called the '2012–2016 Bribes', involving the Brazilian Odebrecht company and other firms that allegedly financed political party activities and campaigns during the Correa government in exchange for government contracts.*[136]

Correa was convicted in April 2020, sentenced to eight years in prison and banned from serving in politics for 25 years.[137] Additionally, in February 2022, Ecuador's attorney general announced that she will seek corruption charges against former president Lenín Moreno and 36 others over the construction of the Coca Codo Sinclair hydroelectric plant.[138] Moreno has denied wrongdoing and called the charges a political distraction.[139]

In Panama, several former ministers and two sons of former president Ricardo Martinelli are currently on trial in connection with bribery and money laundering charges regarding the use of Panamanian corporations to hide bribes to various highly placed government officials of the Martinelli administration.[140]

---

134 'Ecuador's Vice President Sentenced to 6 Years in Corruption Case' (*Reuters*), *The New York Times* (13 December 2017) <https://www.nytimes.com/2017/12/13/world/americas/ecuadors-vice-president-sentenced-to-6-years-in-corruption-case.html>.

135 Correa, Tito, 'Former Ecuador VP released from prison for second time', *Reuters* (28 November 2023) <https://www.reuters.com/world/americas/former-ecuador-vp-released-prison-second-time-2022-11-29/>.

136 '2019 Country Reports on Human Rights Practices: Ecuador', US Department of State, Bureau of Democracy, Human Rights and Labor <https://www.state.gov/reports/2019-country-reports-on-human-rights-practices/ecuador/>.

137 Cabrera, José Maria León, 'Ecuador's Former President Convicted on Corruption Charges,' *The New York Times* (7 April 2020) <https://www.nytimes.com/2020/04/07/world/americas/ecuador-correa-corruption-verdict.html?searchResultPosition=1>.

138 'Ecuador prosecutor asks for corruption charges against former president,' *Reuters* (22 February 2023) <https://www.reuters.com/world/americas/ecuador-prosecutor-asks-corruption-charges-against-former-president-2023-02-22/>.

139 *id.*

140 Republica de Panama Organo Judicial, 'Juzgado Tercero Liquidador de Causas Penales Abre Causa Criminal Contra 26 Ciudadanos En El Denominado Caso "Blue Apple"' (16 November

Martinelli's sons previously served prison time in the US after pleading guilty in connection with a bribery and money laundering scheme.[141] In January 2023, the sons returned to Panama, following the completion of their sentences.[142]

Conclusion

As recent events make clear, regulators throughout Latin America are aggressively investigating allegations of corruption and prosecuting wrongdoers. Further, regulators in the United States have been working together and with Latin American counterparts to enforce anti-corruption laws in connection with allegations of legal violations in the region. Companies doing business in Latin America should ensure that they have robust anti-corruption policies and safeguards in place, be prepared to coordinate with multiple regulators from various jurisdictions and carefully consider the costs and benefits of proactive voluntary cooperation.

2021) <https://www.organojudicial.gob.pa/noticias/juzgado-tercero-liquidador-de-causas-penales-abre-causa-criminal-contra-26-ciudadanos-en-el-denominado-caso-blue-apple>.

141 Press Release, US DOJ, 'Panama Intermediaries Each Sentenced to 36 Months in Prison for International Bribery and Money Laundering Scheme' (20 May 2022) <https://www.justice.gov/opa/pr/panama-intermediaries-each-sentenced-36-months-prison-international-bribery-and-money>.

142 'Sons of Panama ex-president released from US jail, family banned', France 24 (26 January 2023) <https://www.france24.com/en/live-news/20230125-sons-of-panama-ex-president-released-from-us-jail>.

Part II

Building an Effective Compliance Programme

CHAPTER 3

The Ingredients of a Successful Compliance Department

Reynaldo Manzanarez Radilla[1]

Although there are various ways to measure success, one could say that the success of every human organisation is, in general, based on the achievement of its main purpose. When trying to achieve this purpose, organisations often aim to be as efficient and cost-effective as possible in producing the best result achievable. That premise is followed likewise by in-house departments, including compliance departments. Let's keep in mind that, when evaluating the effectiveness of corporate compliance programmes, these should basically satisfy three basic elements: whether the compliance programme is well designed, whether the programme is adequately resourced and empowered and whether the compliance programme works in practice.

An appropriate compliance programme is built upon a prior risk assessment of the business activities and the various operations conducted by any given company. The functioning of a compliance department depends significantly on the compliance programme that a company designs and ultimately implements.

An appropriate risk analysis should cover all aspects of a company, including factors such as, but not limited to, the products and services the company offers, the business model that sustain those products and services, the markets in which the company competes, whether the company conducts business with governments, the company's relationships with third parties and the company's culture.

---

1 Reynaldo Manzanarez Radilla is the head of legal affairs and compliance at Incode Technologies Inc. and a member of the company's global senior leadership team.

There is no one formula that ensures the success of a compliance department. Rather, it depends on many factors, both internal and external, including unexpected situations like those that the world experienced with the covid-19 pandemic or the restrictions imposed on Russia. These situations undoubtedly caused disruptions at all levels in many organisations, both private and public.

Considering the above, once a company has defined its compliance programme, the following steps are presented as suggestions that could facilitate organisations when establishing their compliance departments.

A successful compliance department is based on strong fundamentals that serve as pillars to drive all subsequent efforts. From these fundamentals, more specific actions can be developed that will deliver the purpose of each pillar more effectively. The following suggested pillars can provide the basis of compliance initiatives.

Tone at the top and budget definition

Nothing is more effective than leading by example. Overall, no company initiative will be successful, particularly in the long term, without the proper support of the company's leaders and management. No compliance programme can be managed effectively without this fundamental element.

There is no question that, in the current economic climate, no business organisation can maintain its success unless it has strong ethical foundations and a commitment to comply with all applicable laws and regulations. This helps to avoid situations that could adversely affect a company's reputation in the market.

The leaders of the organisation must champion the need to run the business in an ethical manner, so that everyone within the organisation follows that spirit at all levels, not least because their support will be needed whenever the company faces ethical dilemmas.

There is a big difference when all employees know that their leaders promote all sorts of compliance activities, from incentivising ethical behaviour to taking appropriate action whenever it is needed.

Compliance departments should encourage leaders to take advantage of any opportunity to spread this message, whether in a summit, an all-hands meeting or other internal communications. This type of support will certainly set the tone across the organisation and enable a compliance department to achieve its goals successfully.

Once the proper support has been received from upper management, it is also important to establish a budget. An adequate compliance budget is a significant indicator of an effective programme; otherwise, organisations will need to reverse engineer to determine how much they are spending, and that may create some

frictions internally. No corporate programme can be effective without planning and appropriate financial resources supporting it. In compliance, it is important to make sure money is well spent on critical initiatives and processes so companies are prepared whenever disruptions come into play, such as the covid-19 pandemic, the imposition of controls and sanctions, and other unexpected circumstances affecting supply chains and related revenue challenges.

Establishing a budget requires focus on what is needed to operate the programme, and it also reinforces the independence of the compliance professionals who would be otherwise required to get resources from other areas. But how does one quantify costs and allocate resources? Like any other corporate activity, the organisations will need to prioritise, so more resources are allocated in activities that carry a higher level of risk (e.g., doing business in a risky territory, doing business with governments or entering into business models where there may be a greater use of third parties). It is fundamental for the purposes of constructing a budget that the compliance department provides useful information with examples of compliance problems that other companies are experiencing, industry reputational impacts and new regulations that must be observed. Then it is always a good practice to identify in advance, potential suppliers or vendors such as law firms, compliance risk providers and consulting firms to have the ability to negotiate quotes and discuss the scope of services.

This does not mean that organisations need to allocate an unrealistic level of resources. Compliance efforts and resulting expenditures can be scaled to the size, nature and complexity of the business. In smaller companies, resources should be focused on areas of greatest vulnerability. It is also critical to establish a system to identify and rank identified risk areas. This information can be used to establish a work plan with compliance priorities based on a proper assessment of potential risks. Going forward, it is also important to take into consideration contingencies that may affect budgets and keep open the door to make adjustments and renegotiate with vendors whenever situations out of the parties' control arise.

Code of conduct and ethics

Today, many companies have implemented the practice of having a code of conduct and ethics. This type of document essentially outlines the moral fibre of the company and addresses issues such as honesty, integrity, reporting procedures and corporate social responsibility.

It is indeed fundamental that an organisation should have its own code of conduct and ethics, so that its position on ethical behaviour is clear to both the members of the organisation and the market. This is also a good way to send a strong message that will inspire trust in customers and employees.

Nonetheless, simply having a code of conduct and ethics is not sufficient. It must be a living document and should be constantly reviewed and updated to properly address the changes in the various laws that may apply to the company and its business. Successful compliance departments must lead this effort and find ways to make sure the spirit of the code is followed by all members of the organisation, who should always conduct themselves in an ethical manner in all aspects of the company's business and promote compliance.

In many ways, a compliance department is the guardian of the code of conduct and ethics. For that reason, the leaders of the organisation must maintain close contact and coordination with the department.

A successful compliance department should also be responsible for measuring the effectiveness of its code of conduct and ethics and in implementing initiatives to preserve the company's ethical commitment.

Ownership and management of policies and programmes

In general, compliance programmes are based on three main objectives: prevention, detection and remediation. Further, effective compliance programmes are those that have the following characteristics:

- require conduct that applies with laws and regulations;
- promote and create a culture of honesty and integrity;
- protect the company's reputation;
- prevent illegal behaviour;
- detect compliance issues at an early stage;
- have mechanisms to correct action and remediate; and
- build employee trust and confidence.

The policies and programmes that form a compliance programme should be owned by the compliance department. These policies should be carefully designed to make sure that they deal with the most relevant risks. A successful department should have the ability to identify issues and develop appropriate mitigation plans and strategies, including the use of effective language that can be incorporated into applicable contracts so as to mitigate the organisation's exposure to identified risks.

For instance, in-house compliance professionals should analyse and vet business opportunities with government entities in advance. This is not only to identify potential corruption or the violation of procurement laws, but also to evaluate more broadly whether a particular opportunity with a government entity is consistent with the company's business models.

As an example, assume that a company is working on a business opportunity to sell specific information technologies to a government customer. That transaction may be legally viable and possible to many companies, without contravening applicable laws. However, compliance professionals should assess more thoroughly whether a transaction is appropriate, and whether the company has the ability to deliver, for instance without the need to use subcontractors, and thus avoid circumstances that could have legal consequences or damage the company's reputation. If the company is not in the business of selling information technology, it is reasonable to consider certain mechanisms (e.g., subcontracting) that might affect procurement laws by increasing the cost to the government. This type of transaction could also expose the company to other risks that may affect its reputation, even if no wrongdoing is found and, of course, the company's reputation is one of its most valuable assets. Companies should stay away even from situation that could create the appearance of wrongdoing since that may trigger not only reputational, but also legal consequences.

Furthermore, compliance departments will need to ensure that other internal departments participate in the drafting and monitoring of particular compliance policies and aspects of compliance programmes. This is especially so when a potential issue directly affects another department (e.g., reimbursement of corporate expenses). A compliance department will need to liaise with other internal departments to properly achieve its mission, whether for the purposes of putting together policy terms, drawing up training materials or conducting an investigation.

Typically, the most common policies that reside within a compliance department are those that relate to anti-corruption, money laundering prevention, anti-money laundering, anti-slavery, data privacy protection, export controls, conflicts of interest and other regulated areas; however, a compliance department should be able to assist other internal departments on other matters that may affect the ethical fibre of a company, such as general harassment or in promoting a working with respect environment.

Team of professionals

The human element is extremely relevant when building a group of professionals to manage an in-house department. They are a key asset, as they are the people who will ultimately determine its success or failure.

The skills of those professionals who will be supporting the compliance department should be aligned to what the company needs to execute its compliance programme. For instance, banking institutions will most likely require

professionals with experience in specific banking regulations (e.g., anti-money laundering), although it is also helpful to retain professionals with general experience on other matters so as to have a diverse group.

It is also a good idea to have people from different backgrounds in the department, to the extent possible, who are not necessarily only lawyers but also professionals of other types. The greater diversity of opinions a team can have, the better.

However, just having talented professionals who are skilled in the various matters that the compliance department manages may not be enough. Companies should also focus on retaining people who possess the highest level of ethics, are trustworthy and have the ability to support the various activities that the compliance department performs. For instance, whomever is responsible for preparing and delivering training to the workforce should have the ability to communicate clearly and, ideally, inspire people. Those who are in charge of conducting internal investigations should have experience in conducting interviews, drafting reports and communicating within the organisation, including to the board of directors, auditors and others.

Internal communications and continued training

Compliance departments cannot do everything. Therefore, companies should aim to have employees who see themselves as functional 'compliance professionals'. In other words, everyone within the organisation must follow the internal policies, seeking guidance if needed and reporting anything irregular. They therefore need to be fully aware of the company's activities, its business initiatives and the types of transactions being performed, so that they will notice if the company is doing business without proper contracts or if unusual payments are being made. As a former colleague Eric Diaz, once said, 'compliance starts with the people'. and so does the detection of potential issues and, therefore, prevention of those issues.

On the one hand, in addition to having leaders promoting integrity and supporting compliance initiatives, employees should also be constantly reminded about the company's moral fibre and be given training on the various policies. This is especially so when policies are supplemented or modified over time, as a result of changes in legislation or when new policies are created (e.g., when the company launches new business models or to comply with specific requirements either contractual or by statue). In this way, the spirit of compliance can be felt by everyone.

Communicating frequently with the workforce on ethical matters is a task that can be led either by senior management or the compliance department. Communications can be made through emails, posters displayed within the

premises or on the company's internal website. Some compliance departments have implemented the practice of conducting specific activities throughout the year to remind everyone that compliance is just as important as any other activity or function within the company.

On the other hand, training is not merely a means of transmitting knowledge, but also making sure companies can show the authorities or auditors, whenever necessary, that they have acted responsibly and have done their part in training their workforce.

Successful compliance departments use meaningful and business-oriented training. This is not the usual 30 to 45 slides that have been on file for years. Training must be constantly updated and, more importantly, should be designed in a format and have content that is impactful – real-life situations, videos, interactive questions, whatever works. Furthermore, those materials should be crafted in a way that can be effectively understood by people from various cultures and based in different locations.

Resources and tools

Successful compliance departments should wisely select tools that will assist them in achieving their goals. They should incentivise and promote the use of technology, not only because that could assist the company to expedite business, but more importantly, because that has proven to be an effective way to maintain records and files, which are fundamental to supporting compliance investigations and authorisations.[2]

The cost and effectiveness of tools are critical. Compliance departments should be able to understand what tools and functions are required to properly mitigate risks and ensure business continuity. For instance, many companies license screening tools to identify whether a particular third party who interacts with the business has been sanctioned by a state, meaning that doing business with that third party could constitute a problem to the company. However, vendors that license these technologies usually manage their fees based on the number of lists that are screened whenever a customer runs a search. Since there are many lists published worldwide, compliance departments need to understand what lists are required in order to manage fees.

2 See Chapter 11, 'Why Fresh Perspectives on Tech Solutions are Key to Evolving Data-Driven Compliance Monitoring', Gabriela Paredes, Dheeraj Thimmaiah, Jaime Muñoz and John Sardar.

Although the use of technological tools is highly recommended, there are other resources that can also be critical in assisting compliance departments in their function. One such resource is the use of external counsel support. This can be essential when a company is facing sensitive issues, such as government audits or when new regulations that affect the company's operations have taken effect. In this case, as often occurs, in addition to engaging external counsel, compliance departments will need to work with other critical allies within the company's organisation, such as the legal, finance or operations departments.

Implement an efficient mechanism to monitor regulations

In a global economy, companies are subject to local and international regulations such as anti-corruption and bribery, data privacy and export controls, even when they operate predominantly in local markets.

The world has seen situations disrupting supply distribution chains due to sanctions imposed on certain governments by other governments or international organisations. There is no question that today international political conflicts affect the operations of companies everywhere.

Appropriate mechanisms, in some cases with the support of outside counsel, must be implemented to monitor these regulations so companies can be ready whenever a sanction or a restriction is imposed on a particular country, company, individual or technology, since that circumstance may affect supply chains and consequently, the entire business ecosystem.

There are international associations such as the International Association of Privacy Professionals (IAPP), which provide a number of resources to stay up to date on any changes to privacy regulations across the globe and to obtain knowledge and certifications on the subject. This association also offers several seminars, courses and networking opportunities that are of great help in understating regulations and navigating day to day issues.

Appropriate preventing and monitoring mechanisms will help organisa tions avoid incurring excessive costs, customer satisfaction issues and contractual breaches due to these situations. Therefore, it is important that compliance departments play an important role in the decision-making process of the company at all times, so they can tell what type of controls should be implemented in the company's operations or provide advice whenever contracts are being drafted so these incorporate provisions that will allow the company to mitigate any negative effects such as the right to terminate these if a regulatory situation impacts performance or to obtain further certifications or representations to avoid or mitigate any potential liability.

Trusted adviser and a business partner

Compliance is a business function and a successful compliance department should be able to work that way. Compliance is designed to maintain the company's profitability, among other important objectives.

Successful departments should act in a way that shows they are no different from any other department, for instance, when finance creates a budget to avoid having to incur unanticipated expenses or when procurement selects the most efficient and cost-effective vendor alternative. All departments must consider the financial health of the company.

A compliance department should participate in all sorts of business meetings and in the design of plans to anticipate issues, create acceptable mitigation plans and deal with issues as early as possible. Successful compliance departments should be able to demonstrate their value to the company and their role in finding the most appropriate ways to secure profitable transactions creatively, thus generating revenue and value for the company. For instance, one way is by assisting the company in obtaining specific compliance certifications, such as ISO37001 on Anti-Bribery Management Systems.[3] Potentially, this can increase the value of the company and could even be used in sales proposals when pursuing business opportunities.

International operations

Today's competitive environment has compelled companies to grow internationally. Setting up a business overseas usually becomes a challenge when maintaining consistency in a compliance programme. This is for various reasons, but primarily the variety of laws and cultural behaviours that exist worldwide.

For instance, on this issue, a successful compliance programme should incorporate comprehensive programmes for mergers and acquisitions and the ability to implement business models, policies and procedures everywhere.

With the support of other areas, such as finance, human resources and legal, the compliance department should analyse the international operations of the company to determine whether the market in which operations will be implemented is new to the company or constitutes the opening of a new division or line of business in a country where the corporation has previously been established.

3 ISO 37001:2016 – Anti-bribery management systems – Requirements with guidance for use, International Organization for Standardization, https://www.iso.org/standard/65034.html.

In either case, comprehensive due diligence must be conducted to establish the risks and challenges, implement mitigation strategies and develop an appropriate integration plan.

It is critical that important issues are evaluated, such as ownership, governance, whether public investments are required (which is the case in certain sectors of some countries, such as oil or telecommunications), the need for specific permits and licences or even certain authorisations when it comes to specific industries, such as banking or pharmaceuticals.

For instance, in M&A transactions (see also Chapter 10, 'Assessing and Mitigating Compliance Risks in the Transactional Context'), due diligence must include the following:

- preparation of comprehensive questionnaires to be evaluated by the compliance department, and any other internal areas;
- review of internal policies and procedures or local laws;
- evaluation of business models and programmes to determine whether they fit with corporate policy;
- interviews with stakeholders; and
- development of background check reports (either internally or with the support of external agencies).

Finally, if the deal goes through, the company will need to have an appropriate integration plan, one that resolves issues and risks that have been identified, implements mitigation strategies (e.g., a spin-off of a particular division, procedures to address potential conflicts of interest, renegotiation or termination of certain contractual relationships or a workforce restructuring) and that appropriately rolls out all corporate policies and programmes.

It will also be important to implement an appropriate local training programme, satisfying the local needs of the business and with the right cultural approach. For instance, there are certain places where face-to-face training will be more effective than training that is provided remotely or online.

When disruptive situations take place, such as the current pandemic, and particularly when conducting operations overseas in high-risk territories, a higher level of scrutiny must be maintained within the organisations. For instance, when

bribes are inappropriately classified as facilitating payments to expedite permits and authorisations. The US Department of Justice has said, 'Labelling a bribe as a "facilitating payment" in a company's books and records does not make it one'.[4]

International organisations are also taking a stand in ensuring that the fight against corruption and bribery remains a high priority. The OECD recently issued a statement indicating:

> *As countries around the world work to combat the outbreak, the OECD Working Group on Bribery, which unites all 44 Parties to the Anti-Bribery Convention, is firmly committed to upholding its obligations to fight trans-national bribery in all its forms and across sectors.*

It also calls on all countries around the globe to respect the rule of law, ensure integrity in public procurement, transparency, the effective protection of whistle-blowers, and press freedom to fight all forms of corruption, especially corruption that could undermine the response to the pandemic.[5]

Facilitating payments are an exemption to the FCPA, not an affirmative defence. This means that the accused company can claim an alleged bribe was a facilitating payment and the burden of proof is on the government to prove otherwise.

Maintaining close contact with the workforce

Building a culture in which employees can identify issues on their own and freely deal with those issues is critical to close the loop and to ensure the compliance department can track metrics that properly evidence the reality of the business they serve. This is possible by, among other things:

- implementing mechanisms and initiatives that allow the compliance department to reach out to employees regarding their day-to-day activities; and
- having a compliance champions or ambassadors programme that allows individuals from various areas to become part of a group of in-house professionals that will serve as liaison between employees and the compliance department, to more effectively understand the needs of the business, the day-to-day realities

4 *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, Second Edition, by the Criminal Division of the US Department of Justice and the Enforcement Division of the US Securities and Exchange Commission, p. 26.

5 OECD.org, Article 22/04/2020, Statement by the OECD Working Group on Bribery.

and to cascade spread compliance initiatives and programmes down to the workforce. These professionals may also assist the compliance department with trainings and eventually some of them, even with internal investigations.

Crisis management and remediation

Many articles have been written suggesting that compliance programmes are tested not only by the problems avoided, but also by whether crises can be overcome. This is also applicable to compliance departments, since crises can happen in any company; large, profitable and successful companies are not immune. Those that overcome these situations and maintain their position in the market are the ones that have the right processes and procedures in place, with the right people to manage them.

A successful compliance department should have appropriate internal mechanisms to deal with compliance and ethics crises and must always be involved whenever they arise. Compliance departments become a great asset in those situations, primarily because crises do not suddenly emerge but rather evolve from an issue that was not well handled, or from situations not remediated on time. For this reason, early engagement is critical.

In addition to working with other critical areas, such as legal and finance, a compliance department should also advise the company about when to engage external counsel and which areas should recuse themselves (including compliance itself), to avoid situations that could cause eventual harm to the company, even in appearance. In larger organisations, this type of situation is usually handled by multidisciplinary teams specifically created to manage a crisis.

Transparency is always needed, of course; however, that does not mean openly publishing everything that is being reported or learned. Compliance departments should be able to understand how to manage the flow of information and how to properly activate certain mechanisms whenever is convenient and wherever is possible, such as legal privilege. Also, they need to understand and appropriately manage privacy and confidentiality. Therefore, compliance departments should push to have appropriate incident response procedures and incorporate these into compliance programmes.

Consistency is also needed. Successful compliance departments should be able to take appropriate action in a timely manner and in alignment with the company's ethical stand, as reflected in its code of conduct and ethics. That is the best way to send the right message out to the market and within the organisation, and to ensure the company survives in the long term, especially given that whenever these situations arise, a company should expect scrutiny not only from authorities but also from the market.

Once a crisis has passed, compliance departments are key to implementing whatever remediation measures have been adopted. These may for instance include more training or the creation of new processes and procedures, the proper implementation of data privacy protection processes and controls, the termination of contracts or even disciplinary actions. Compliance departments should lead, monitor and follow up on remedial actions until they are satisfactorily concluded.

Being ethical and ensuring compliance with all applicable laws and regulations is simply the right way to do business and the best way to protect stakeholders' interests. To facilitate this goal, companies must have an appropriate compliance programme in place and a reliable compliance department to run it. There are many challenges in daily activities that require compliance departments to step in and act effectively to prevent issues and rectify whatever has gone wrong.

The scope of this chapter does not permit detailed discussion of each of the outlined pillars, but these can be explored in more detail with the support of compliance specialists and external counsel. No successful compliance department can emerge from improvisation; a road map should always be established for better results. A successful company is likely to have a strong, effective compliance department. Companies should, therefore, take their time and be careful when developing and nurturing their compliance departments.

Designing a contingency plan and returning to normal

One of the lessons recently learned by organisations around the world is that companies must be prepared to deal with the unexpected. Compliance programmes today must include processes and procedures that ensure they can continue delivering their function at acceptable levels, following a disruptive incident. Those incidents may come not only from situations inside the organisations, but also from events caused by external factors such as the covid-19 pandemic.

The design of such a plan must be risk-based. The basic elements such plan should consider are:

- re-evaluation of risks, since the company's activities may have changed and then, conduct a new assessment of compliance priorities;
- resource allocation identifying alternatives available to the company (i.e., whenever a vendor or a system becomes unavailable for instance);
- redefining of roles and activities in case some roles are eliminated or put on furlough and liaise with other areas, such as HR, to properly support the workforce as needed;

- review of processes to define whether some of those should be adjusted while the emergency conditions last and prepare for post-crisis stages by ensuring important compliance activities (such as record-keeping) are not stopped or diminished;
- activation of other alternatives to run internal processes, in case the existent ones cannot be sustained or become unavailable (e.g., e-signatures or remote interviews) For instance, owing to covid-19, it will be important to redefine IT security measures to cover cybersecurity and data privacy protection risks, particularly with the increase in the use of IT tools and personnel working remotely; and
- constant communication within the organisation so everybody understands how the compliance programme will be run while the contingency lasts and that internal resources remain available.

This last element is very important, because more than ever, it is key for everyone in the company to understand that the programme is fully operational and that they need to engage compliance personnel early. A post-contingency plan should be designed for purposes of returning this to normal in an orderly fashion and the compliance department should be prepared to lead the organisation on compliance matters when 'returning to normal'.

CHAPTER 4

Developing a Robust Compliance Programme in Latin America

Brendan P Cullen and Anthony J Lewis[1]

For several years, there has been an ever-increasing focus on corruption in Latin America.[2] After major corruption scandals,[3] protests and calls for change,[4] governments in Latin American countries have added to or enhanced anti-corruption

---

1 Brendan P Cullen and Anthony J Lewis are litigation partners at Sullivan & Cromwell LLP. The authors thank Aviv S Halpern, Noah P Stern and Kelly H Yin for their valuable assistance in researching this chapter.

2 Congressional Research Service [CRS], 'Anti-corruption Efforts in Latin America and the Caribbean' [Anti-Corruption Efforts], p. 1 (1 February 2022), https://crsreports.congress.gov/product/pdf/IF/IF12031/2; Bantz, Phillip, 'White Collar Attys Brace for More Latin America FCPA Action,' (8 February 2023), https://www.law360.com/articles/1574007/white-collar-attys-brace-for-more-latin-america-fcpa-action (60% of US DOJ's 2022 enforcement actions involved Latin America); see also '2022 FCPA Year in Review', Stanford Law School FCPA Clearinghouse, https://fcpa.stanford.edu/fcpac-reports/2022-fcpa-year-in-review.pdf; CRS, 'Combating Corruption in Latin America: Congressional Consideration' [Combating Corruption], 7 (2019), https://crsreports.congress.gov/product/pdf/R/R45733.

3 Benjamin N Gedan, Santiago Canton, 'Radical Transparency: The Last Hope for Fighting Corruption in Latin America', *Georgetown J. In'tl Affairs*, (1 April 2022), https://gjia.georgetown.edu/2022/04/01/radical-transparency-the-last-hope-for-fighting-corruption-in-latin-america%EF%BF%BC/; see also Rodolfo Borges, Lorena Arroyo, Francesco Manetto, 'Cases Against Former Latin American Leaders: A Challenge for the Credibility of the Courts', El Pais (28 April 2021), https://english.elpais.com/usa/2021-04-28/cases-against-former-latin-american-leaders-a-challenge-for-the-credibility-of-the-courts.html; Miller, Ben; Uriegas, Fernanda, 'Latin America's Biggest Corruption Cases: A Retrospective', *Americas Quarterly* (22 July 2019), https://www.americasquarterly.org/content/decades-most-iconic-corruption-cases; CRS, Combating Corruption (footnote 2, above) Appendix C.

4 Gedan & Canton (footnote 3, above); see also Sheridan, Mary Beth, 'Why political turmoil Is erupting across Latin America', *The Washington Post* (10 October 2019), https://www.washingtonpost.com/world/the_americas/why-political-turmoil-is-erupting-across-latin-

provisions in their corporate liability schemes.[5] The covid-19 pandemic further exacerbated corruption risks by increasing financial pressure, reducing oversight and disrupting supply chains,[6] so companies should increase focus on internal compliance programmes to prepare for closer scrutiny and a more active enforcement environment.[7] For multinational companies, this can be challenging. An effective compliance programme should meet the requirements that authorities promulgated in every jurisdiction in which a company operates, and some countries' enforcement regimes apply extraterritorially. And a compliance programme must be tailored to a company's specific risks based on geography, industry and any other relevant factors.[8]

---

america/2019/10/10/a459cc96-eab9-11e9-a329-7378fbfa1b63_story.html; Daugaard, Andreas, 'Honduras: How a surge of corruption scandals has fuelled political crisis', Voices for Transparency (22 September 2019), https://voices.transparency.org/honduras-how-a-surge-of-corruption-scandals-has-fueled-political-crisis-85af16ceac85.

5 Kahn, Daniel S, 'Latin America Compliance Requirements', *Global Investigations Review* (2 September 2022), https://globalinvestigationsreview.com/guide/the-guide-compliance/first-edition/article/latin-america-compliance-requirements; Corres, Luis Dantón Martínez; et al., 'Mexico: At a Turning Point in Anti-Corruption Investigations and Enforcement' in *Americas Investigations Review 2020*, at 135, 137 to 144; Fava, Pamina; et al., 'How to Mitigate Corruption Risk When Investing in Latin America', Anti-Corruption Report (25 July 2018), https://www.anti-corruption.com/2619631/how-to-mitigate-corruption-risk-when-investing-in-latin-america.thtml.

6 See CRS, Anti-Corruption Efforts (footnote 2, above); Pitaro, Vincent, Anti-Corruption Report, 'Kroll Corruption Survey Finds ESG a Post-COVID Compliance Focus' (18 August 2021), https://www.anti-corruption.com/9150831/kroll-corruption-survey-finds-esg-a-post-covid-compliance-focus.thtml; see also CRS, 'Anti-corruption Efforts in Latin America and the Caribbean', p. 1 (1 February 2022), https://crsreports.congress.gov/product/pdf/IF/IF12031/2.

7 Bantz (footnote 2, above) (discussing US DOJ's 2022 enforcement trends and expectations for 2023); Americas Society/Council of the Americas, 'Latin America's Battle Against Corruption: A Path Forward', 7 (2018), https://www.as-coa.org/sites/default/files/CorruptionReport2018_ASCOA.pdf; Newbery, Charles, 'Compliance Is Taking Off in Latin America. Is It Effective?', *Americas Quarterly* (22 July 2019), https://www.americasquarterly.org/content/compliance-takes-latin-americ-it-working; Hamilton-Martin, Roger, 'Investigator's Guide to Brazil', Global Investigations Review (8 December 2017), https://globalinvestigationsreview.com/article/1151271/investigators-guide-to-brazil.

8 US DOJ & SEC, A Resource Guide to the U.S. Foreign Corrupt Practices Act, Second Edition at 56, 59 (3 July 2020) [2020 FCPA Resource Guide], https://www.justice.gov/criminal-fraud/file/1292051/download; see also Transparency International, 'Business Principles for Countering Bribery', at 7 (2013); Sureda, Aixa; González Soldo, Evangelina, 'Argentina', *Americas Investigations Review 2020*, Global Investigations Review (19 August 2019), https://globalinvestigationsreview.com/benchmarking/americas-investigations-review-2020/1196467/argentina.

This chapter summarises some of the key risks and challenges that a multinational corporation's compliance programme in Latin America must confront, including with respect to guidance issued by the US Department of Justice (DOJ),[9] which is one of the most active anti-corruption enforcement authorities in Latin America.[10] This chapter then discusses best practices for companies to maintain effectively tailored compliance programmes.

We begin with the baseline prevalence of corruption, which is itself highly variable.[11] As the magnitude of the risk varies dramatically from country to country, so do the types of risks.[12] Local enforcement regimes must be considered in establishing an effective compliance programme. Many countries in Latin America have recently enacted substantially tougher anti-corruption measures.[13] Still, the variances among them can be significant.[14]

---

9 US Dep't of Justice [US DOJ], Criminal Division, 'Evaluation of Corporate Compliance Programs' (March 2020) [US DOJ Guidance], https://www.justice.gov/criminal-fraud/page/file/937501/download. In July 2020, the US DOJ and the SEC also issued an updated edition of the US Foreign Corrupt Practices Act (FCPA) Resource Guide for the first time in nearly eight years, which reflects the agencies' current thinking about anti-corruption enforcement. 2020 FCPA Resource Guide (footnote 8, above).

10 See Sheehan, Evelyn B, Tuminelli, Amanda, 'Latin American Corruption in the Crosshairs of the Biden Administration,' Anti-Corruption Report (14 April 2021), https://www.anti-corruption.com/8674736/latin-american-corruption-in-the-crosshairs-of-the-biden-administration.thtml. This trend is likely to continue given new legislative changes in the United States that have created additional tools for prosecutors, including increased whistleblower rewards and expanded subpoena power over foreign bank records permitting prosecutors to subpoena foreign bank records even if local law would prohibit disclosure of those records. Id.

11 Koukios, James M; et al., 'Anti-Corruption in Latin America' in *The Guide to Corporate Crisis Management*, at 68.

12 See Tillen, James; Bates, Gregory, Miller & Chevalier, 'Managing Corruption in Latin America's Police Forces,' Anti-Corruption Report (16 September 2020), https://www.anti-corruption.com/7543846/managing-corruption-in-latin-americas-police-forces.thtml (noting that corruption risks evolve over time).

13 See Portella, Renato Tastardi, 'Managing Multi-jurisdictional Investigations in Latin America' in *Americas Investigations Review 2020*, at 53–57 (reviewing newly enacted anti-corruption laws of Brazil, Mexico, Chile, Colombia and Argentina); see also Fontán Balestra, Santiago, 'Argentina moves to modernize its AML legislation,' (27 September 2022), https://www.dlapiper.com/en/insights/publications/global-anti-corruption-perspective/global-anticorruption-perspective-q3-2022/argentina-moves-to-modernize-its-aml-legislation.

14 See Koukios (footnote 11, above), at 7071 (providing a comparison of local anti-corruption laws in Latin America). For example, some regimes permit 'facilitating payments' in limited circumstances (as does the FCPA), but they are locally prohibited in many countries. Corres (footnote 5, above), at 139 ('The prohibitions in the GLAR are rather broad and there is no facilitating payments exception.'); see also Fava (footnote 5, above).

One benefit of an effective compliance programme is detecting illicit conduct, if and when it occurs. Most countries incentivise and credit companies that maintain compliance programmes and self-report conduct to anti-corruption regulators.[15]

With this backdrop, we next address the essential elements of an effective compliance programme.

Components of an effective compliance programme

Not all countries explicitly require compliance programmes. But the US DOJ and SEC evaluate the effectiveness of a compliance programme when they are considering bringing an enforcement action and the penalty that should result, and they have used the FCPA's broad extraterritorial jurisdiction to bring enforcement actions against companies headquartered in Latin America for conduct that principally occurred there and was carried out by nationals of Latin American countries.[16] Thus, major companies in Latin America that are (or that may be) subject to US enforcement jurisdiction should take account of the anti-corruption guidance from US agencies.[17]

Compliance-programme guidance by US regulators has changed in recent years. The US DOJ promulgated new guidance in April 2019, which it updated in June 2020 and March 2023. The guidance now asks three core questions when assessing a corporation's compliance programme:

- Is the corporation's compliance programme well designed?
- Is the programme being applied earnestly and in good faith? In other words, is the programme being implemented effectively?
- Does the corporation's compliance programme work in practice?[18]

---

15 Chapter 13, 'The Advantages of a Robust Compliance Programme in the Event of an External Investigation'; see also Kahn (footnote 5, above) (reviewing compliance-related policies and statutes in Latin America); Basch, Fernando Felipe; Cargnel, Maria Emilia, 'Argentina' in *The International Investigations Review*, 41, 45, 46 (Law Business Research, Nicolas Bourtin ed., 9th ed. 2019); Bofill, Jorge; Praetorius, Daniel, 'Chile', in *The International Investigations Review*, 103 (Law Business Research, Nicolas Bourtin ed., 9th ed. 2019).

16 Sheehan, Evelyn; Short, Jason, 'DOJ's Long Arm Over Latin America: Recent Trends and Future Risks From Extraterritorial Application of U.S. Laws', Anti-Corruption Report (30 September 2020), https://www.anti-corruption.com/7640641/dojs-long-arm-over-latin-america-recent-trends-and-future-risks-from-extraterritorial-application-of-us-laws.thtml; see also Sheehan (footnote 10, above); Bantz (footnote 2, above).

17 See Tillen (footnote 12, above).

18 US DOJ Guidance (footnote 9, above).

And in other enforcement-related guidance documents, US regulators have provided a baseline criteria to receive credit for an effective compliance programme.[19] While there is no one-size-fits-all formula, below are some of the key elements, drawn from the US DOJ's relevant guidance and the compliance requirements in several Latin American countries, to consider for any compliance programme.

Tone at the top

Both senior and middle management should send a clear message that misconduct is not tolerated and that management endorses (and enforces) the policies and procedures designed to drive ethical conduct. Every opportunity should be taken to show management's commitment to compliance, and to show that misconduct or significant risks will not be tacitly or otherwise tolerated in pursuit of business goals.[20]

Risk assessment

Great emphasis should be placed on the degree to which a programme is tailored to the particular risks facing the company. Risks should be assessed based on a company's geography, its industry, its competitive and regulatory environments, who its actual or potential clients or business partners are, what sales or other agents it employs and why, what types of transactions it has or may have with government officials, and what payments or donations it makes to charities or

19 See Memorandum from Lisa A Monaco (US Deputy Attorney General) to US DOJ Criminal Division Personnel, 'Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group' [Monaco Memo] (15 September 2022), https://www.justice.gov/opa/speech/file/1535301/download; US DOJ, Criminal Division, '9-47.120–Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy' (January 2023) [US DOJ Corporate Enforcement Guidance], https://www.justice.gov/criminal-fraud/file/1562831/download; US Attorneys' Office [USAO], 'United States Attorneys' Offices Voluntary Self-Disclosure Policy' (February 2023) [USAO Guidance], https://www.justice.gov/usao-edny/press-release/file/1569406/download. Even more recent guidance documents reflect the US DOJ's recent focus on retention of electronic messaging on mobile devices and clawing back compensation by wrongdoers. See Memorandum from Kenneth A Polite, Jr (Asst. Attorney General, Criminal Division) to US DOJ Criminal Division Personnel, 'Revised Memorandum on Selection of Monitors in Criminal Division Matters' [Polite Memo] (1 March 2023), https://www.justice.gov/criminal-fraud/file/1100366/download; US DOJ, '9-28.000 Principles of Federal Prosecution of Business Organizations' [US DOJ Principles] (updated March 2023), https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.

20 See US DOJ Corporate Enforcement Guidance (footnote 20, above), at 5.

other third parties.[21] Companies should expect not only to show that they have identified and assessed these risks, but also to defend their assessment process and methodology.[22]

Resource allocation and autonomy

More than just being adequately staffed and funded, a compliance function should have sufficient resources and authority.[23] Leadership of the compliance function must have seniority in the organisation, as well as autonomy and independence from management.[24] Consideration should be given to the compliance function's place in the corporate structure, and whether any additional business-related responsibilities or reporting obligations might detract from compliance personnel's independence.

Policies and procedures

A code of conduct is a must; it should be reinforced by management and readily available and broadcast to all employees in the languages employees speak at work. There also should be broadly communicated resources that allow employees to seek guidance on issues relating to the company's code of conduct or other

---

21 US DOJ Guidance (footnote 9, above), at 3; e.g., US DOJ, Justice Manual 9-28.800 [Justice Manual], https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations#9-28.800.

22 See US DOJ Corporate Enforcement Guidance (footnote 20, above), at 5. This is one area in which innovative uses of data and machine learning can assist in developing and maintaining an effective compliance programme. See Zweibel, Megan, Cybersecurity Law Report, 'Cargill Compliance Director Discusses Putting Training Data to Work', (24 February 2021), https://www.cslawreport.com/8454981/cargill-compliance-director-discusses-putting-training-data-to-work.thtml; see also Zweibel, Megan, Anti-Corruption Report, 'AB InBev's C2CRIGHT Initiative: Can Companies Work Together to Prevent Corruption?' (13 October 2021), https://www.anti-corruption.com/18400796/ab-inbevs-c2cright-initiative-can-companies-work-together-to-prevent-corruption.thtml; see also Chapter 11, 'Why Fresh Perspectives on Tech Solutions Are Key to Evolving Data-Driven Compliance Monitoring', Gabriela Paredes, Dheeraj Thimmaiah, Jaime Muñoz and John Sardar.

23 Sufficient resource allocation and autonomy is already required in several Latin American countries, and it is a consideration by the US DOJ. See US DOJ Corporate Enforcement Guidance (footnote 20, above), at 5; Tillen, James; Montenegro Almonte, Alejandra; Hollinger, Abi; Miller & Chevalier, 'A Comparative Look at Anti-Corruption Compliance Program Expectations in Latin America', Anti-Corruption Report (28 October 2020), https://www.anti-corruption.com/7831636/a-comparative-look-at-anticorruption-compliance-program-expectations-in-latin-america.thtml.

24 See US DOJ Corporate Enforcement Guidance (footnote 20, above), at 5.

policies or procedures. And if a mistake is made, the company should have in place controls to make sure that the mistake is corrected through proper channels, even if there are negative business consequences.

Training programmes

Training, too, is a must – for directors and officers, for relevant employees, and in many cases for business partners, agents and other third parties. Of particular importance is training for gatekeepers: supervisors or control personnel, or other persons with approval authority or certification responsibilities. It should account for the audience's size, sophistication and experience with the subject matter, it should be tailored to the specific business risks employees may face, and it should evolve based on data-driven insights regarding its effectiveness.[25]

Audit function

A core compliance-programme component is its internal audit function, or comparable systems designed to test and monitor compliance, which should be mapped onto the results of periodic risks assessments and should emphasise high-risk areas. The documented results of those audits should periodically reach management and, depending on the scope or significance, management should take actions in response to audit findings.

Third-party management

One of the areas of highest risk for companies is their relationship with third parties. Third parties are a common vehicle to make or conceal illicit payments. The prevalence of this risk is illustrated by a recent US$282 million combined fine that Walmart paid to the US SEC and US DOJ for failure of various subsidiaries to effectively investigate and mitigate third-party risk, including in Brazil and Mexico.[26] Thorough vetting, due diligence and applicable controls should include an assessment of each third party's qualifications and reputation; the particular business need for their services; a specific description of the objectively verified services they will provide; a method to determine that compensation was at a fair-market price for that industry and geographical region; and verification

25 See, e.g., Zweibel (footnote 22, above).

26 Press release, US SEC, 'Walmart Charged with FCPA Violations' (20 June 2019), http://fcpa.stanford.edu/fcpac/documents/5000/003871.pdf.

that the services were performed. Also, a process should be in place to document any red flags and how they are addressed, and to retain that information to use in assessing future opportunities involving that third party.[27]

Confidential reporting structure

Confidential reporting, or whistleblowing, allows employees to report possible misconduct when they either feel they have been unsuccessful in reporting it through ordinary supervisory channels or fear they will be unsuccessful in (or will suffer negative consequences for) doing so. Whistleblowers often report misconduct or policy violations at significant personal and professional risk, so companies should widely broadcast their reporting mechanisms and consider proactive ways to foster an understanding that confidential reporting will remain as confidential as is legally permissible, that retaliation will not be permitted, and that processes are in place to protect whistleblowers.

Several countries are focusing on guidance changes designed to reinforce protections for whistleblowing, including Argentina, Brazil, Colombia, Mexico and Peru.[28] These changes have increased awareness of anonymous reporting mechanisms and encouraged their use. To illustrate, a survey tracking employees' awareness and understanding of the compliance policies and procedures implemented at their companies showed significant increases in the percentage of employees who were aware that their companies offered anonymous reporting mechanisms – in Argentina, employee awareness rose from 48 per cent in 2016 to 70 per cent in 2020, and in Peru it rose from 38 per cent in 2016 to 67 per cent in 2020.[29]

Investigation process

Although handling internal investigations is treated in detail elsewhere in this publication, a basic measure of an effective compliance programme is its process for investigating issues that arise. The compliance programme should require

27 See, e.g., Press release, US DOJ, 'Zimmer Biomet Holdings Inc. Agrees to Pay $17.4 Million to Resolve Foreign Corrupt Practices Act Charges' (12 January 2017), http://fcpa.stanford.edu/fcpac/documents/4000/003434.pdf. In 2017, Zimmer paid more than US$17 million in criminal penalties, in part, for continuing to use a Brazilian distributor that Zimmer knew had previously paid bribes on behalf of the company. The US parent was also faulted for failing to implement adequate controls at its Mexican subsidiary despite known red flags.

28 Weiss, Ed & Chung, Theodore, Principal Legal Issues—International Trends—Latin America, 3 Successful Partnering Between Inside and Outside Counsel §46C:30 (April 2021).

29 See Tillen, Montenegro Almonte, & Hollinger (footnote 23, above).

adequately tailored data retention policies, the timely completion of investigations, appropriate follow-up and, when appropriate, the consequences for persons involved in any actual misconduct.[30] When an investigation is concluded, the investigators' conclusions and the investigation's outcome should be documented, and the company should engage in a candid and thorough root cause analysis to determine whether the misconduct involved any failures in controls, and whether and how controls could be improved. A plan for remediation should be developed, documented and executed.

Incentives and discipline

Although policies can set forth the rules, a compliance programme must recognise that employees must be incentivised to engage in compliant behaviour, and there must be both positive and negative consequences for compliance or violations.[31] Thought should be given to how the company can ensure that there is consistency in how discipline or incentives are applied throughout the company – laterally through different lines of business and vertically through different layers of management. This can be done, for example, by creating compensation structures to promote compliance, a recent focus for US regulators evaluating compliance programmes.[32]

Updating

Even the best-designed compliance programme still requires periodic review and updating.[33] Those revisions begin with an assessment of the risks presented (including new or emerging risks) and should also map other changes in the

30 US DOJ Guidance (footnote 9, above) at 16–18.

31 See US DOJ Corporate Enforcement Guidance (footnote 20, above), at 5.

32 See Monaco Memo at 9-10; US DOJ Guidance (footnote 9, above) at 12-14, 18; US DOJ Principles, § 9-28.300; see, e.g., Plea, at C-5 to C-6, *United States v. Danske Bank A/S*, Case No. 22-cr-00679 (12 December 2022) https://www.justice.gov/opa/press-release/file/1557611/download (mandating the company implement a compensation structure to promote compliance). For instance, in early March 2023, the US DOJ instituted a Pilot Program Regarding Compensation Incentives and Clawbacks, a three-year initiative designed to create compensation-based compliance incentives. The Pilot Program provides for fine reduction by any amount clawed back from employees who engaged in wrongdoing in connection with the conduct under investigation, or others who had supervisory authority over the employee or business area, or who had knowledge of (or were wilfully blind to) relevant conduct. US DOJ, 'The Criminal Division's Pilot Program Regarding Compensation Incentives and Clawbacks', (March 3, 2023), https://www.justice.gov/criminal-fraud/file/1571941/download.

33 US DOJ Guidance (footnote 9, above), at 3.

company – such as structural changes to the organisation or its components, changes in the company's geographical markets or industries, and legal or regulatory developments. Mining the lessons learned from prior incidents into a compliance programme (including future training programmes, in particular) is an effective way to show that a company is learning and adapting its compliance programme overall.[34]

Mergers and acquisitions

Somewhat distinct from the compliance programme in the ordinary course is having a due diligence process in place for mergers and acquisitions activity (see also Chapter 10, 'Assessing and Mitigating Compliance Risks in the Transactional Context').[35] Subjecting a target company to adequate due diligence is not only important so that the successor or acquiror does not unwittingly inherit undisclosed risk or pay a price for a target that fails to reflect the target's actual risk level; it has also been flagged by the US DOJ as 'indicative of whether [a company's] compliance programme is, as implemented, able to effectively enforce its internal controls and remediate misconduct at all levels of the organisation.'[36] Critically, a process also should be in place to track and address any post-acquisition risks or actual misconduct identified during pre-acquisition due diligence.[37]

Compliance across multiple jurisdictions

The US DOJ's guidance documents are detailed, but a company's compliance programme must account for all jurisdictions in which it operates, some of which may conflict with one another. In some instances, Latin American countries may have particular compliance requirements that go beyond the US DOJ's core topics, like requiring external audits from an auditor with an independent duty to report apparent wrongdoing, or requiring a company's human resources function to avoid hiring employees who could risk the 'integrity of the company'.[38]

---

34 2020 FCPA Resource Guide (footnote 8, above), at 65, 67; US DOJ Guidance (footnote 9, above), at 13; US DOJ Corporate Enforcement Guidance (footnote 20, above), at 5.

35 See US DOJ Corporate Enforcement Guidance (footnote 20, above), at 4 (noting that where a company uncovers misconduct through thorough and timely due diligence or post-acquisition audits or compliance integration, it may receive a presumption of a declination if it voluntarily self-discloses the misconduct and otherwise fully cooperates and remediates).

36 US DOJ Guidance (footnote 9, above), at 8.

37 US DOJ Corporate Enforcement Guidance (footnote 20, above), at 3.

38 Tillen, Montenegro Almonte, & Hollinger (footnote 23, above); see also Kahn (footnote 5, above); Bofill and Praetorius (footnote 15, above), at 99; Rassi, João Daniel; Labate, Victor, 'Brazil' in *The International Investigations Review* (Law Business Research, Nicolas Bourtin ed., 9th ed. 2019), at 91.

Treatment of whistleblowers

As noted, whistleblowing channels are a critical element of a compliance programme. This is also an area where local attitudes can affect both the whistleblower and the behaviour of the persons receiving a whistleblower report. In this way, cultural factors can substantially alter the risk profile of a given country.[39] For instance, in certain Latin American countries, notably Brazil, there is a history of hostility towards whistleblowers and a concomitant reluctance for them to come forward.[40] In other countries (like Mexico), employees may place a lesser value on confidentiality.[41] Marrying that cultural reality to the various legal requirements can be challenging for multinational companies.

Various countries in Latin America have particular legal provisions that cover whistleblowers, but they do not all afford the same protection, if any at all.[42] And while multiple Latin American enforcement agencies have created whistleblower channels, given the considerable perceived risks in reporting misconduct, it may take time before use of whistleblower channels is ingrained in the

---

39 See KPMG International, 'Cross-border investigations: Are you prepared for the challenge?' (2013), https://assets.kpmg/content/dam/kpmg/pdf/2013/12/cross-border-investigations.pdf.

40 See Fundação Getúlio Vargas, 'Speak Now or Forever Hold Your Peace: An Empirical Investigation of Whistleblowing in Brazilian Organizations' (2012), https://pdfs.semanticscholar.org/492a/47ac593f21b7b20bc1861b50390186bcc8f8.pdf ('Brazilian organizations seem to consider whistle-blowing a taboo or a deviant behavior . . . .'); McLeod, Frances; Voss, Jenna, 'Moving Forward after an Investigation' in *Americas Investigations Review 2020*, at 86 [Moving Forward After an Investigation] ('Historical factors . . . may contribute to a heightened culture of retaliation. A whistleblower in such a society may be viewed as a traitor.'); Transparency International – Brazil, 'United Nations Convention Against Corruption,' at 38–41 (22 September 2022), https://uncaccoalition.org/wp-content/uploads/Final-Civil-Society-Parallel-Report-on-UNCAC-Implementation-in-Brazil-EN-20.05.2022.pdf.

41 Sierra, Diego, 'Mexico', in *The Practitioner's Guide to Global Investigations*, Part II, 205 (Law Business Research, Judith Seddon, et al. eds., 3rd ed. 2019) (A 'principle challenge' in cross-border investigations is 'maintaining confidentiality' during employee interviews. 'This is often an issue as there is a weak confidentiality culture in Mexico.').

42 Basch and Cargnel (footnote 14, above) (Argentina); Rassi and Labate (footnote 30, above), at 89, 99 (Brazil and Chile); see also Barcellos, Ana Paula, CEP Magazine, 'An introduction to Brazil's new whistleblower protection law' (June 2020), https://compliancecosmos.org/introduction-brazils-new-whistleblower-protection-law#:~:text=The%20new%20Brazilian%20Anticrime%20Law,%2C%20and%20government%2Dfunded%20programs (discussing new monetary rewards and protections for whistleblowers); Kolodner, Jonathan, et al., 'New Anticorruption Decree Modifies Regulation of Brazilian Clean Companies Act,' (22 July 2022), https://www.clearygottlieb.com/news-and-insights/publication-listing/new-anticorruption-decree-modifies-regulation-of-brazilian-clean-companies-act.

relevant corporate cultures.[43] By contrast, the European Union adopted a robust Directive[44] that imposes specific requirements on corporate whistleblowing channels, protecting more people from a broader range of retaliatory conduct than US or many Latin American whistleblower provisions. Companies with operations in both Latin America and the EU will need to ensure that they meet these enhanced requirements.

Best practices

As we expect has now been made clear, managing a multinational company's compliance programme in a variety of environments to meet the factors described herein is a substantial and ongoing challenge. We therefore outline some practices that companies can use to help create a compliance programme that is up to the task.

Documenting changes and successes

Not only is it important to have a documented compliance policy, but to document and record compliance processes and any changes made to the programme.

If a violation of law is discovered by (or reported to) regulators and any resulting investigation or prosecution is being resolved, a company's compliance programme will be evaluated both at the time the resolution is negotiated and at the time the offence occurred.[45] But, as the US DOJ guidance puts it, '

> *Due to the backward-looking nature of the . . . inquiry, one of the most difficult questions prosecutors must answer in evaluating a compliance program following misconduct is whether the program was working effectively at the time of the offense, especially where the misconduct was not immediately detected.*'[46]

It is similarly difficult for the company itself to look back in time to measure its compliance programme. But the US DOJ has emphasised that it is committed to credit companies for investing in an effective compliance programme even when misconduct was not prevented or detected.[47] This makes clear the importance of

43 Bofill and Praetorius (footnote 15, above), at 99.

44 Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

45 US DOJ Corporate Enforcement Guidance (footnote 20, above), at 4–5, 7.

46 US DOJ Guidance (footnote 9, above), at 13.

47 Zwiebel, Megan, 'AAG Benczkowski Wants Prosecutors to Be Compliance Sophisticates', Anti-Corruption Report (8 January 2020), https://www.anti-corruption.com/4230152/

data, documentation, tracking and preserving institutional memory. A company may make adjustments to its compliance programme diligently and in earnest, but it should also track any changes to its programme, its remediation of identified misconduct and its compliance successes in an accessible system; the value of those good measures may be lost when they are forgotten or when the memory of them leaves with the employees who implemented them.

Relatedly, when potential misconduct is brought to a company's attention, a company should examine its procedures and compliance programme to determine whether improvements can be made. Although a company might fear that making changes to a compliance programme, and documenting them, would be taken by a regulator as a concession that deficiencies exist, in reality, making changes to a programme indicates both (1) effective remediation of potential misconduct and (2) revisiting and updating of the programme. And when evaluating the form and contents of a possible criminal resolution, those factors can reduce the risk that a compliance monitor or other ongoing reporting obligations will be imposed.[48]

Broadcasting a culture of compliance

It is vital that a multinational corporation has a healthy culture of compliance and ensures that this culture is globally disseminated. As an organisation grows, cultural, linguistic and geographical barriers can hamper its ability to communicate its compliance culture outside of its home territory.[49] Effective company-wide communication begins with ensuring compliance materials are translated into the local language or dialect, but it is not only a matter of translation of the words themselves.[50] The subtleties of these issues can result in miscommunication and confusion when a compliance programme is simply exported wholesale from a home office.[51]

---

aag-benczkowski-wants-prosecutors-to-be-compliance-sophisticates.thtml?utm_source=emailArticle&utm_medium=email&utm_campaign=emailArticle.

48 Memorandum from Brian A Benczkowski (US Assistant Attorney General) to US DOJ Criminal Division Personnel, 'Selection of Monitors in Criminal Division Matters' (18 October 2018), https://www.justice.gov/opa/speech/file/1100531/download.

49 See OECD, Corporate Governance and Business Integrity: A Stocktaking of Corporate Practices 56 (2015), http://www.oecd.org/daf/ca/Corporate-Governance-Business-Integrity-2015.pdf; Sureda and González Soldo (footnote 8, above).

50 See 2020 FCPA Resource Guide at 59-60 (footnote 8, above); KPMG (footnote 38, above), at 17.

51 Tillen, James G; Delman, Sonia M, 'Lost in Translation: The Language of Bribery', *The Corporate Governance Advisor* (1 August 2010); see also DPA, *United States of America v. Orthofix International, N.V.*, 12-cr-0015 (2012) http://fcpa.stanford.edu/fcpac/

Local input and buy-in

Relatedly, local stakeholders, including local managers and employees, should be consulted and given a voice in crafting and tailoring a compliance programme for their region.[52] Cultural practices, like gift-giving, can often present a compliance risk, which an effective policy must anticipate and account for.[53] Similarly, requests for charitable donations from local officials, though unexceptional on their face and routinely permissible elsewhere, may well constitute an unmistakable demand for an illegal payment in a particular location.[54]

Involving local stakeholders has the added benefit of increasing buy-in to the programme.[55] This insight is confirmed by recent behavioural scientific research on the risks of overbearing enforcement strategies, which shows that extrinsic imposition of strict rules can alienate local employees and create 'compliance fatigue' while crowding out employees' intrinsic motivation to do the right thing, such as actively reporting compliance risks.[56] Thus, incorporating input from local managers, who often will be the people actually charged with implementing the programme, will increase their commitment to the programme and their help in implementing it.[57]

---

documents/3000/002056.pdf (describing how Orthofix promulgated its own anti-corruption policy but failed to either translate it to Spanish or ensure it would be implemented in Mexico).

52 See Transparency International (footnote 8, above), at 7; Sureda and González Soldo (footnote 8, above).

53 United Nations Global Compact, 'A Guide for Anti-Corruption Risk Assessment', 23 (2013) [UN Global Compact Report]; Tillen and Delman (footnote 49, above).

54 Baker McKenzie, 'Latin America Corporate Compliance Report: Seven Compliance Challenges and How to Overcome Them', 31 (2015), https://www.bakermckenzie.com/-/media/files/insight/publications/2015/12/spotlight-on-latin-america/la_compliancereport_english.pdf.

55 See Costa Carvalho, Isabel; et al., 'Brazil' in *The Practitioner's Guide to Global Investigations*, Part II (Judith Seddon, et al., eds., 3d ed. 2019); Moving Forward After an Investigation, at 86.

56 See Teichmann, Fabian Maximilian Johannes & Wittmann, Chiara, 'Compliance Cultures and the Role of Financial Incentives' at 3-4, J. of Fin. Crime, (16 August 2022); OECD, Behavioral Insights for Public Integrity: Harnessing the Human Factor to Counter Corruption, at 33 (2018) [OECD, Behavioral Insights], https://dx.doi.org/10.1787/9789264297067-en; Graf Lambsdorff, Johann, 'Preventing corruption by promoting trust: Insights from behavioral science', at 4-5 (Passauer Diskussionspapiere – Volkswirtschaftliche Reihe, No. V-69-15, 2015), http://hdl.handle.net/10419/125558.

57 See UN Global Compact Report (footnote 51, above), at 15-16; cf. OECD, Behavioral Insights (footnote 54, above), at 35.

Relying on local counsel

Consulting high-quality local counsel is essential to meet the challenges of a particular legal environment in a given country. Local counsel can provide insights into how a company's compliance programme should be modified to meet particular aspects of local laws.[58]

For instance, Mexico's anti-corruption law has a relatively specific list of components that must be included in a compliance programme to justify a sentence reduction.[59] Local counsel will also very often have a valuable – and external – perspective on cultural issues, or other issues peculiar to a given locale, and that advice should be taken into account alongside the voice of the company's own local personnel.[60]

Using data analytics[61]

There has been an increased emphasis on data analytics, which can take many forms, from off-the-shelf software suites to artificial intelligence.[62] Indeed, the US DOJ's 2020 update to its compliance guidance provided language that has been incorporated into at least nine deferred prosecution agreements requiring

58 See Portella and Tastardi (footnote 13, above), at 55.

59 See Corres (footnote 5, above) at 140; Portella and Tastardi (footnote 13, above), at 55-56.

60 Warin, F Joseph; et al, 'Co-operating with the Authorities: The US Perspective' in *The Practitioner's Guide to Global Investigations*, Part I (Judith Seddon et al. eds., 3d ed. 2019); Lehtman, Jeffrey A; Laporte, Margot, 'Individuals in Cross-Border Investigations or Proceedings: The US Perspective', in *The Practitioner's Guide to Global Investigations*, Part I.

61 See Chapter 11,'Why Fresh Perspectives on Tech Solutions Are Key to Evolving Data-Driven Compliance Monitoring', Gabriela Paredes, Dheeraj Thimmaiah, Jaime Muñoz and John Sardar.

62 See, e.g., Zweibel (footnote 22, above).

companies to integrate data analytics in compliance programmes.[63] The US Commodity Futures Trading Commission (CFTC) has used data analytics in its own enforcement efforts.[64]

Data analytics can assist companies in developing and tailoring their training programmes, as well as demonstrating to regulators that their programmes are robust and assess appropriate risks.[65]

Adapting to evolving legal regimes

Companies must monitor and update their programmes continually to adapt to changes in the compliance environment.[66] This is especially important given substantial uncertainty surrounding how newly enacted legislation in different countries in the region will be interpreted and applied.[67]

---

63 Kagubare Ines, 'Latest DPAs increase focus on compliance data', *Global Investigations Review* (1 October 2020), https://globalinvestigationsreview.com/just-anti-corruption/spoofing/latest-dpas-increase-focus-compliance-data; see also DPA at C-8, *United States v. Herbalife Nutrition Ltd.*, 20-CR-00443 (24 August 2020); DPA at C-8, *United States v. The Goldman Sachs Group, Inc.*, 20-CR-00437 (21 October 2020); DPA at C-8, *United States v. Beam Suntory Inc.*, 20-CR-00745 (23 October 2020); DPA at C-8, *United States v. Vitol Inc.*, 20-CR-00539 (3 December 2020); DPA, C-8, *United States v. Deutsche Bank Aktiengesellschaft*, 20-CR-00584 (7 January 2021); DPA at C-9, *United States v. Amec Foster Wheeler Energy Ltd.*, 21-CR-00298 (24 June 2021); DPA at C-9, *United States v. Credit Suisse Group AG*, 21-CR-00521 (19 October 2021); DPA, at C-9, *United States v. Stericycle, Inc.*, 22-cr-20156 (18 April 2022); DPA, at C-9, *United States v. Gol Linhas Areas Inteligentes S.A.*, 22-cr-00325 (16 September 2022).

64 See CFTC, 'FY2020 Division of Enforcement Annual Report' 8 (2020) https://www.cftc.gov/media/5321/DOE_FY2020_AnnualReport_120120/download; Memorandum from James M McDonald (Director, Division of Enforcement) to CFTC, Division of Enforcement Staff, 'Guidance on Evaluating Compliance Programs in Connection with Enforcement Matters' (10 September 2020) https://www.cftc.gov/media/4626/EnfGuidanceEvaluatingCompliancePrograms091020/download.

65 See Chapter 10, 'Embracing Technology'; see, e.g., Pitaro, Vincent, Cybersecurity Law Report, 'How Lockheed Uses Big Data to Evaluate Risk at Small Worksites', Cybersecurity Law Report (21 October 2020), https://www.cslawreport.com/7737416/how-lockheed-uses-big-data-to-evaluate-risk-at-small-worksites.thtml.

66 US DOJ Guidance (footnote 9, above), at 7, 14.

67 See OECD, Integrity for Good Governance in Latin America and the Caribbean: From Commitments to Action, at 68 (2018), https://doi.org/10.1787/9789264201866-en; Fonseca, André; Lima, Marina, 'Brazil' in *The International Comparative Legal Guide to: Corporate Investigations* (Keith D Krakaur and Ryan Junck, eds., 2018), https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1475099_1.pdf; Corres (footnote 5, above), at 137–44..

Conclusion

In summary, an effective compliance programme can save a company from considerable adverse consequences later on. It can prevent illicit conduct in the first place, it can detect it at the earliest possible stage if it does arise, and it can lessen or avoid many of the consequences that come with an enforcement action – not least of which could be a compliance monitor to help devise and implement a programme that should have been established in the first place.

CHAPTER 5

The Board's Role in Compliance: The Traditional Oversight Approach is Not Good Enough

Andrew B Jánszky[1]

Introduction

Compliance as a necessary element of corporate checks and balances has been with us for some time. It is still too often implemented gradually, grudgingly and sometimes might seem more for show than to serve the corporation and its stakeholders. Nevertheless, compliance is now an accepted part of the management structure of companies traded on the world's major exchanges.

There is, however, a worrisome fault in the design and oversight of compliance: the lack of proper attention and participation by board directors.

Board-level insouciance regarding compliance with ethical and legal standards has certainly contributed heavily to the upsurge in corruption in Latin America, as well as other regions. The aim in this chapter is to show – with some hair-raising examples – what went wrong, to argue that the traditional oversight approach is no longer sufficient to changed circumstances and expectations, and to set forth the necessary elements for effective board attention to, and oversight of, the compliance effort.

An important cause of inadequate board attention has been the general lack of consequences to directors.

---

1 Andrew Jánszky is an independent lawyer with more than 40 years' experience in international capital markets, mergers and acquisitions, corporate governance and compliance, and has served as a board member of exchange-listed companies.

For example, in a corruption case involving Embraer, the board of directors failed to take disciplinary action against a very senior executive even after the investigation showed that the executive knew of various bribes in several countries paid by employees who reported to him. The board's failure to dismiss or even discipline the executive led to additional monetary penalties and other sanctions for Embraer.[2] In another corruption case, the CEO was personally involved in bribe payments in Argentina, yet continued as CEO, which again led to more severe penalties being imposed.[3] In neither case was the board sanctioned, and based on my review of the media coverage, even criticised, for failure to act.

In fact, the board response to these sorts of failures frequently goes as follows, at the most:

- the bad thing happens: allegations of corruption, cheating on emission standards tests, a deadly dam collapse, publicity about a company's pervasive culture of sexual harassment, etc.;
- the board expresses resolute confidence in management but will 'thoroughly and independently investigate' the bad thing;
- awkward facts come to the fore and C-suite members 'resign';
- there are more awkward revelations and the CEO walks out with his head under his arm (and usually with a fat cheque in his hand); and
- finally, the board expresses its shock and dismay and appoints a new CEO, often (and with no discernible sense of shame) a member of the board of directors or an executive who was present during the whole sad affair.

A vivid example is Boeing, where the extremely 'bad thing' was the tragic crash of two planes, both of them its newest model, the 737 MAX.

On 22 October 2019, Boeing fired the head of its commercial aviation division.[4] Board chair David Calhoun said that the CEO had 'done everything right' and should not resign.[5] The CEO was sacked one month after this endorsement, replaced by Calhoun.[6] Calhoun had been a director for nine years.

---

2 *United States of America v. Embraer S.A.*, Deferred Prosecution Agreement, 24 October 2016, p. 4.

3 *United States of America v. Latam Airlines Group S.A.*, Deferred Prosecution Agreement, 25 July 2016, p. 4

4 Gelles, David; Kitroeff, Natalie, 'Boeing' Boeing ousts Top Executive as 737 MAX Crisis Swells', *The New York Times*, 22 October 2019.

5 Koening, David and The Associated Press, 'After Pressure From Congress, Boeing Chairman Says CEO Won't Get Bonus Until MAX Flies', *Fortune*, 6 November 2019.

6 Kitroeff, Natalie; Gelles, David, 'It's More Than I Imagined': Boeing's New C.E.O. Confronts its Challenges', *The New York Times*, 5 March 2020.

In many jurisdictions, the means to hold board members personally accountable are few, if any, and are difficult to assert successfully, for legal or political reasons. In Delaware, however, there are clear signs that the spotlight is now on directors too.

In *Marchand v. Barnhill*,[7] a 2019 case, on a motion appealing lower court decisions holding that the pleadings were insufficient (i.e., the facts asserted did not on their face support a finding of culpability), the Delaware Supreme Court reversed. The basic facts follow:

> *Blue Bell Creameries USA, Inc, one of the country's largest ice cream manufacturers, suffered a listeria outbreak in early 2015, causing the company to recall all its products, shut down production at all its plants and lay off over a third of its workforce. Three people died as a result of the listeria outbreak . . . [S]tockholders also suffered losses.*[8]

An aggrieved shareholder brought a derivative suit against various executives and the board of Blue Bell for breach of fiduciary duty.

The Delaware Supreme Court found that the plaintiff's alleged facts supported the necessary inferences that the board failed to implement any system to monitor food safety issues and that this 'utter failure' by the board was in breach of its duty of loyalty.

The following is a partial list of board-related shortcomings noted by the Court:

- Blue Bell manufactures only ice cream, thus making food safety a central compliance issue, yet the board did not have a food safety committee, no board-level process to address safety issues and no protocol for food safety issues to be raised to the board's attention. See the Boeing and Vale discussions below.
- For years before the 2015 listeria outbreak, safety inspectors had found troubling compliance failures. The Court mentioned six such reports.
- Tests ordered by Blue Bell in 2013 and 2014 were positive for listeria.
- The board never received any of this information.
- More negative news came to light in 2014, yet board minutes reflect no discussion of these concerns.

7 *Marchand v. Barnhill*, 212 A.3d, 805 (Del. 2019).

8 *id.* p. 807.

- On 13 February 2015, the Texas health authorities notified Blue Bell of positive listeria tests. The company itself, on 19 and 21 February, found listeria in the Texas facility. When the board met on 19 February 2015, there was no mention at all of the listeria problem.
- Only four days after the February board meeting, Blue Bell initiated a product recall. Only then did the board discuss the listeria issue, for the first time.
- Instead of then going into full disaster remediation mode, the board did not meet more frequently or receive constant updates, leaving the company's response entirely to management.

On 1 May 2020, Blue Bell pleaded guilty to two counts of distributing contaminated goods. It was fined over US$17 million and agreed to pay more than US$2 million to settle federal false claims violations. This was, at the time, the second-largest sum ever paid in a food safety case.

There have been several cases coming out of Delaware in the wake of the *Marchand* case.

The *Inter-Marketing Group* case involved responsibility for a pipeline company's disastrous oil spill. It was alleged that, as in the *Marchand* case, there was no board oversight of the company's 'intrinsically critical' business operation. Evidence showed that pipeline integrity issues were not discussed by the board and no board subcommittee existed to discuss these matters. Further, in response to the defendant's argument that the audit committee's charter required the committee to 'advise the Board with respect to policies and procedures', the court found that there was no evidence at all that the audit committee had so advised the board.[9]

In *Clovis*, the alleged oversight failures concerned the company's only product, an oncological treatment for which it was seeking regulatory approval. Company officers overstated the drug's efficacy, misapplied testing protocol standards and misled regulators and investors. In assessing the board's responsibility, the court stated that, 'when a company operates in an environment where externally imposed regulations govern its "mission critical" operations, the board's oversight function must be more rigorously exercised'.[10]

On the other hand, directors were untouched in dozens of scandals around the world, including at Volkswagen, Uber, CBS, Airbus, WeWork, Chipotle, Glencore, Theranos, FXT and Nikola, and, in Latin America at companies such

9 *Inter-Marketing Group United States v. Gregory L. Armstrong*, C.A. No. 2017-0030-TMR

10 *In Re Clovis Oncology, Inc. Derivative Litigation*, C.A. No. 2017-0222-JRS

as JBS, Biomet (later Zimmer Biomet), Biomet Argentina and Biomet 3i Mexico, Vale (more on this one later), Tyson de México, Petrobras, Odebrecht, Braskem, SQM (Chile) (and now, perhaps, Lojas Americanas in Brazil).[11]

What boards must do

Confidence in corporate governance is not high, with good reason. A recent study by professors from the University of Toronto, University of California at Berkeley and the University of Chicago finds that only about a third of corporate fraud is detected, that about 40 per cent of public companies violate accounting rules and 10 per cent or so of companies commit securities fraud every year.[12] Media attention has consequently been relentless and scathing, and activist shareholders and even stay-on-the-sidelines shareholders have increasingly made their unhappiness clear. The landscape is changing and risks for board members increasing. Many boards have taken notice, especially of the repeated exhortation that boards must set the 'tone at the top'. (Forgive whoever fell into the amatory arms of alliteration and coined the phrase.)

Unfortunately, overdone emphasis on 'tone at the top' has taken attention away from all else that the board and the C-suite must do in this regard, and lulls into contentment those who believe that setting that tone is sufficient.

---

11 Stewart, James B, 'Problems at Volkswagen Start in the Boardroom', *The New York Times*, 24 September 2015; Griswold, Alison, 'Now That Uber Has a New CEO, Employees Say Its Board Needs to 'Grow up'', *Quartz*, 2 September 2017; Kitroeff, Natalie; Gelles, David, 'Boeing Fires C.E.O. Dennis Muilenberg', *The New York Times*, 23 December 2019; Gardner, Eriq, 'CBS Faces Credibility Questions Over Leslie Moonves Investigation', *Hollywood Reporter*, 8 August 2018; 'Airbus Executives Get Swept Away by a Corruption Investigation', *The Economist*, 8 February 2018; Tan, Gillian, et al., 'WeWork Plows Ahead with IPO Plans after Reshaping Board to Counter Skepticism', *Los Angeles Times*, 13 September 2019; Carr, Austin, 'Chipotle Eats Itself', *Fast Company*, 16 October 2016; Phillips, Dom, 'The swashbucking meat tycoons who nearly brought down a government', *The Guardian*, 2 July 2019; Cassin, Richard L, 'Zimmer Biomet Holdings pays $30 million to resolve new FCPA changes', The FCPA Blog, 12 January 2017; Watson, R T, 'Vale's Management Team Is on Thin Ice After Deadly Dam Break', *BNN Bloomberg*, 28 January 2019; Neumann, William, 'Tyson Settles U.S. Charges of Bribery', *The New York Times*, 10 February 2011; Schipani, Andres, 'Petrobras in $853 million settlement of bribery case that rocked Brazil', *The Financial Times*, 27 September 2018; Presley, Linda, 'The largest foreign bribery case in history', BBC World Service, 21 April 2018; 'Chile's SQM paying $30 million to resolve U.S. corruption cases', *Reuters*, 13 January 2017; Cassin, Richard L, 'Former Chile mining executive to settle FCPA offenses', The FCPA Blog, 25 September 2018.

12 Dick, A, Morse A & Zingales, L, "How pervasive is corporate fraud?", Review of Accounting Studies, 5 January 2023

CEOs and board members have placed misguided faith in the manner and frequency with which they deliver their message, believing it to be the only contribution they needed to make. Consequently, they have not participated substantively, meaningfully, from the outset, in setting up structures and procedures to create the conditions for a compliance culture to form and take root. Those days are ending. Boards can no longer do all the talking and leave to others all the doing.

It is commonly accepted that the major duties of a board of directors are to think strategically and to keep an eye on management. This second obligation, influenced over time by practices in many countries and by jurisprudence, notably in the state of Delaware, with its development of the 'business judgement' rule to protect boards from undue second-guessing, has become defined largely by what the board ought not to do: directors should not act like executives, leaving to boards the somewhat removed task of receiving reports, asking questions and deciding matters in a reasonable, prudent manner. Consequently, boards have long been advised to maintain distance from operations, lest board members be judged by a more rigorous standard for having left their safe supervisory perch and mucked about in day-to-day affairs. Not surprisingly, boards take the attitude that risk assessment and compliance, being ongoing, everyday matters, are routine, and so left to management. That is incorrect, and dangerous.

My view may seem radical and a departure from the notion that boards should not meddle in operational matters. My answer: not only is this not radical but, in light of repeated scandals, it is necessary as part of the prudence and care that boards owe to shareholders. As for interference in operations, my proposal is to deepen board knowledge of, involvement in, and contribution to, enterprise risk management, not to supplant executive functions; this is not a difficult line to find.

A note on 'compliance'

I use 'compliance' to include anti-corruption and anti-fraud. Discrimination, harassment, conflicts of interest and related-party transactions also are the responsibility of the compliance function. But the term clearly needs to be comprehended more broadly to include all significant business-related risks. You have read of ice cream, pipelines and drugs, and you will read about dam and airplane safety, and the cheating of customers, all of which fit into this category.

I do not advocate that the assessment of all risks and the processes to address them be the responsibility of the compliance department, but there must be in place very similar structures in conception, range of activity and autonomy and independence to monitor these other areas of concern. The board cannot assume that these issues are being handled properly because they are an integral, ongoing

part of the 'business' of the company and are therefore for executives to deal with, as opposed to corruption or discrimination incidents or trademark litigation, which are not ongoing 'business' events (one hopes).

But watch for abuse of the term 'compliance'. Conveniently tagging every corporate headache that is not directly operational as compliance-related will inevitably lead to the wrong people looking at problems the wrong way.

And a related thought, on 'Board compliance oversight'. This is generally a delegated duty of the audit committee. A separate governance or compliance committee might make sense in some circumstances, but these committees could suffer from not having all the information an audit committee receives. So I see the audit committee as the board organ responsible for compliance supervision, which should at appropriate intervals fully brief the board. In turn, the board should engage actively and contribute to the compliance efforts of the committee and management. An exception to this rule might exist for an activity that is high risk and very technical, which would be watched over by board members with in-depth knowledge of the area, and perhaps even expert non-board members in an advisory capacity.[13]

Risk

To quickly and demonstrably mount or invigorate a compliance function, with new or additional codes, rules, prohibitions, remedies and punishments, companies are often tempted to skip the vital step of conducting a careful risk assessment.

This results from various attitudes: overconfidence ('we know our business, we know what needs watching'), the time required, the cost and the worry I have heard more than once that mapping of relevant risks will make management gun-shy (like disconnecting the speedometer so you don't scare yourself when driving too fast).

Risk assessment is absolutely crucial. As the 2020 US Department of Justice Guidelines puts it:[14]

13 But see: https://www.jdsupra.com/legalnews/the-importance-of-aseparate-board-12193; https://corpgov.law.harvard.edu/2019/10/15/boardoversight-of-corporate-compliance-is-it-time-for-arefresh; and https://assets.corporatecompliance.org Portals/1/PDF/Resources/past_handouts/CEI/2014/706_Handout07.pdf.

14 US Department of Justice, Criminal Division, 'Evaluation of Corporate Compliance Programs', April 2019, pp. 2 and 3.

> *The starting point for a prosecutor's evaluation of . . . a well-designed compliance program is to understand the company's business from a commercial perspective, how the company has identified, assessed, and defined its risk profile and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks.*
>
> *. . . Prosecutors may credit the quality and effectiveness of a risk-based compliance program that devotes appropriate attention and resources to high-risk transactions, even if it fails to prevent an infraction in a low-risk area.*

And yet, an EY survey of 500 CEOs and board members found that fewer than 25 per cent of directors reported being 'very satisfied' with the effectiveness of their risk assessment processes and only 20 per cent of directors were confident in risk reporting from management.[15]

A good risk assessment exercise should:

- freshly analyse the risks of the company in its significant areas of activity;
- have the collection of information thoroughly informed by what front-line managers view as their risks and with what priority. These should be validated by interviews with senior executives;
- include transaction-testing and walk-throughs to ascertain whether what should be working is, in fact, working;
- from time to time, or for certain issues, include external consultants;
- have as its analytical centre for the dimensioning of risks and assigning of priorities a committee that includes senior accounting, legal, controls, internal audit (IA) and information technology representatives, at least. This diverse group is not likely to miss anything important; and
- most of all, this work should be closely followed by at least one audit committee member. Daily participation by this member is not necessary, but frequent involvement in the data analysis and priority-setting discussions is a must.

From conception to operation

Some fundamental principles govern the construction of every good compliance programme. While adhesion to best practices from top to bottom may be ideal, it is not realistic. But the principles of independence, autonomy, structure and cultural compatibility are key to the sturdiness of the compliance edifice and how well it will successfully meld into the corporate landscape. The first two qualities ensure reliability; the correct structure separates the operational from

15 Kiemash, Stephen; Doyle, Rani, Report: 'Eight priorities for boards in 2020', EY Center for Board Matters, 19 November 2019, p. 9.

support functions and compatibility ensures that the programme fits the culture and language of the company. These principles being of the first order, the audit committee must be fully engaged in implanting and preserving them. Choices between 'best' and 'it will do for now' must be made by the audit committee and management together. Like other strategic business decisions, which routinely involve suboptimal elements and uncomfortable compromises, with potentially significant consequences, the building and oversight of the compliance function cannot be left only to executives.

Independence

I cannot overstate the importance of independence. Together with autonomy, these attributes must be self-evident and unassailable from the board down. It is not sufficient that audit committee members be considered 'independent' under relevant regulations. May a member who meets applicable requirements but who is a close, long-time friend of the CEO and other high-up executives be on the audit committee? Strictly, yes, as close friendship is not disqualifying factor under, at least, US or Brazilian regulations and most likely nowhere else either. But if that audit committee is called upon to oversee an investigation possibly involving one of these close friends, how will that appear to regulators, shareholders and the media? If the structure is not virtually immune to attack, the reliability of its findings and conclusions will be questioned from the outset.

This same care should extend to professionals hired for compliance-related work, especially investigations. I would be uncomfortable hiring a law or consulting firm for an investigation that is doing, or has recently done, considerable other work for the organisation. The justification for hiring a close professional partner ('they know us, they won't go crazy') is precisely why hiring that firm is inadvisable: it may appear as an attempt to gain an advantage. In compliance, looking bad is almost as bad as being bad.

Autonomy

A perfectly independent audit committee relying on departments that have compromising or conflicting vectors acting upon them is of virtually no use. It is in this area that the board must be most firm, because it is likely to require structural changes, which most companies almost instinctively resist.

Compliance and internal controls should be grouped together and its head should report directly to the CEO. Often the reporting is to the general counsel, but this confuses an operational function that is intended for the detection and avoidance of irregularities with the management charge of the legal department to protect and defend the company from legal risks. As second-line components,

these functions report to the CEO because they support the business operations. However, the department head should have regular access to the audit committee in executive sessions. Ideally, the audit committee chair should have a direct, informal relationship with the CCO. In a number of companies, the CCO reports directly to the audit committee. While I sympathise with the push for even greater independence, I am persuaded that having compliance as part of the operations of the company and not an enforcement arm of the board is the better approach. This is also the prevailing view. Compliance should be perceived by the company's employees as supporting, not policing them.

It is also important to protect the CCO from financial pressures; costcutting, downsizing and similar performance tools ought not to be used for the compliance area, and any significant deviation in compensation of the CCO compared with peers within the company should be discussed with and approved by the audit committee. Likewise, the CCO's demotion or dismissal should happen only with the committee's concurrence. The CCO and other senior executives should be very aware of these protections.

IA should report directly to the audit committee, which ought to set compensation for the IA head (in consultation with human resources). I have not heard any convincing arguments against this structure but I will give the argument in its favour anyway. IA, the last line of defence, catches what the first line thought it could live with, or get away with, and that the second line missed. To have a group with this charge subordinate to those who looked away, allowed, or worst, participated in the transgression, is folly.

Compatibility with company ways

Whether putting together a new programme or overhauling a dated or misshapen one, there is a strong but wrong-headed temptation to borrow heavily from publicly available models for reasons of speed, economy and herd safety. Here the board must be patient. First, the compliance programme will have to address effectively the many, many differences between companies: geography, products, customers, employee base, regulatory environment and so on. But that is only part of the challenge. A compliance programme that does not organically fit the mores and traditions of the organisation, that does not reflect and absorb its cultural and even linguistic individualities, will fail. It will be rejected by the organisation, not with anger but with disdain.

To avoid this, the CCO will need to understand the organisation deeply, viscerally and how best to inject compliance into its core rather than grafting it on awkwardly. This thorough understanding is also necessary for the compliance programme's designers, who must be very well informed about the company's particular risks and the best way to address them in the company's way.

To do this well, I suggest the formation of a committee. This committee, comprising senior members of internal audit, information technology, accounting, internal controls, legal and key line managers, from procurement and sales particularly, will be instrumental in helping to develop a programme that identifies the size and shape of the company's particular risks, sorts them as to importance and addresses them in the language of the company.

In the structuring, or restructuring, of the compliance functions, the participation of an audit committee member is vital. This member can contribute valuable reflection on the views and concerns of senior executives and board members, and can give political and other support to the CCO. This effort, along with the comprehensive risk assessment that is solidly based on first-line worries, will result in a programme that has a familiar tone, is focused on the right issues and is introduced to the organisation as having the collaboration and support of a broad array of respected managers. This inclusive approach will assure greater and quicker adhesion to the compliance programme.

Case studies

I will present in some detail three potently illustrative episodes of shameful board failure. Taken together they comprehend all the mistakes I have touched on, even if not explicitly called out.

Wells Fargo

Founded in 1852 as a California stagecoach service, Wells Fargo (sometimes, 'Wells') grew into a major regional bank, then embarked on a 25-year acquisition spree to become the third-largest bank in the United States, 15th in the world by total assets, and a well-respected, reliable retail bank. 'For 60 years, Wells Fargo was a feel-good brand name.'[16] Then corruption set in, and spread and spread.

16 Peters, Justin, 'How Wells Fargo Became Synonymous with Scandal', *Slate*, 28 November 2020; Phaneuf, Alicia, 'Top 10 Biggest Banks US Banks by Assets in 2022', *Insider Intelligence*, 2 January 2022; Felba, David, Ahmad, Renan, 'The world's 100 largest banks, 2021', *S&P Global Market Intelligence*, 23 April 2021.

The jaw-dropping behaviours and lapses detailed below had their inception in Wells Fargo's acquisition of Norwest Bank in 1998.

Dick Kovacevich, CEO of Norwest and later of Wells Fargo, saw banking products – accounts, cards, loans – as consumer items. So the corporate goal of eight products per customer was set.[17]

Getting to eight products (the industry average is around three per client) required an aggressive programme combining relentless pressure on the sales force, clear financial incentives for doing well and nasty consequences for falling short. Abusive sales practices began in the early years of this century, and intensified enormously in 2007 and beyond.[18]

The *Los Angeles Times* article of December 2013 that blew the lid off this scandal relates the hell that branch manager Rita Murillo was put through:

> *Regional bosses required hourly conferences on her Florida branch's progress toward daily quotas for opening accounts and selling customers extras such as overdraft protection. Employees who lagged behind had to stay late and work weekends to meet goals, Murillo said.*
>
> *Then came the threats. Anyone falling short after two months would be fired. 'We were constantly told we would end up working for McDonald's.'*[19]

Subsequent investigations and reports by US regulatory and congressional bodies revealed astonishing managerial misbehaviour, such as threatening employees who did not meet sales expectations that they would be 'transferred to a store [sic] where someone had been shot and killed'.[20]

A Board Report prepared by Shearman & Sterling at the request of the independent members of the board describes other disturbing behaviour.

The Community Bank produced daily and monthly 'Motivator' reports 'as a source of pressure', showing sales rankings down to the district level. Those reports 'ramped up' pressure on managers, some of whom 'lived and died' by them.

---

17 McLean, Bethany, 'How Wells Fargo's Cutthroat Culture Allegedly Drove Bankers To Fraud', *Vanity Fair*, 31 May 2017.

18 Office of the Comptroller of the Currency, 'Notice of Changes for Orders of Prohibition And Orders to Cease and Desist and Notice of Assessments of Civil Money Penalty', 23 Jan 2020, pp. 4–6.

19 Reckard, E Scott, 'Wells Fargo Pressure-cooker sales culture comes at cost', *Los Angeles Times*, 21 December 2013.

20 OCC, p. 20. (footnote 18 above).

The 'Jump into January' sales campaign, started in 2003, aimed to get salespeople to 'start the New Year strong' by raising daily targets even higher and rewarding more generously higher activity levels achieved.[21]

These shady practices gained Wells Fargo more than unauthorised 1.5 million accounts and more than a half a million unauthorised credit cards. (Included were 193,000 non-employee accounts opened between 2011 and 2015 where the only email address for the 'depositor' was @wellsfargo.com.[22])

In May 2015, the Los Angeles City Attorney filed suit against Wells.[23] The federal Consumer Financial Protection Bureau (CFPB) and the Office of the Controller of the Currency, a top bank regulator (OCC) also opened investigations. In September 2016, a settlement of US$185 million with the three authorities was announced.[24]

Predictably, Wells completely misunderstood the significance of these practices and the settlement. CEO John Stumpf was clear, if ungrammatical, in blaming employees: 'The 1 percent that did it wrong, who were terminated, in no way reflects our culture nor reflects the great work the vast majority of the people do. That's a false narrative.'[25]

In fact, the false narrative was Stumpf's.

---

21 Independent Directors of the Board of Wells, Fargo & Company, 'Sales Practice Investigation Report', 10 April 2017 ('Board Report'), p. 6. As mentioned, the Board Report was commissioned by the Independent Directors of the Wells Board but prepared by Shearman & Sterling. I was an associate and partner at Shearman & Sterling for 34 years, leaving for another firm some seven years before the Board Report was produced. I think it is a well-done report, with a notable exception: the board receives only three minor criticisms in the Board Report, pp. 16–17. In light of the House Report, further regulatory actions and law suits, I consider this a significant shortcoming. Others were harshly critical: the *Los Angeles Times* called it a 'whitewash' and Howell Jackson, a chaired professor at Harvard Law School, was merciless: he labelled parts describing the Board Report (which he insisted on calling the 'Shearman & Sterling Report') as 'self-serving and silly', containing at least two 'false narratives', and, 'one great big whopper' regarding when the board first had knowledge of abuses (Jackson believes it was in 2011, while the Board Report has it at 2014). Michael Hiltzik, 'Wells Fargo scandal report details board of directors' dereliction of duty, gives them a pass', *Los Angeles Times*, 10 April 2017; Howell Jackson, 'One Take on the Report of the Independent Directors of Wells Fargo: Throw the Bums Out', Harvard Law School Forum on Corporate Governance, 22 April 2017.

22 McLean (footnote 17, above).

23 Reckard, E Scott, 'L.A. Sues Wells Fargo, Alleging 'Unlawful and Fraudulent Conduct', *Los Angeles Times*, 4 May 2015.

24 Korey, James Rufus, 'Wells Fargo to pay $185 million Settlement for 'outrageous' sales culture', *Los Angeles Times*, 8 September 2016.

25 Tayan, Brian, 'The Wells Fargo Cross-Selling Scandal', Stanford Closer Look Series, p. 3.

US Senate hearings were held in September 2016. In her closing remarks, Senator Elizabeth Warren delivered this 'epic takedown':

> *You know, here's what really gets me about this, Mr. Stumpf. If one of your tellers took a handful of $20 bills out of the cash drawer, they'd probably be looking at criminal charges for theft. They could end up in prison. But you squeezed your employees to the breaking point so they would cheat customers and you could drive up the value of your stock and put hundreds of millions of dollars in your own pocket. And when it all blew up, you kept your job, you kept your multimillion dollar bonuses, and you went on television to blame thousands of $12-an-hour employees who were just trying to meet cross-sell quotas that made you rich.*[26]

Shortly after the hearing, Stumpf resigned without explanation. The board in November 2016 obtusely chose as his successor Tim Sloan, the president and chief operating officer, who had joined Wells in 1987.[27]

Before and after Sloan's appointment, the federal banking authorities continued to express clearly their concern that Wells Fargo was unable or unwilling to implement an effective risk management programme. This should have been Sloan's overriding preoccupation, but there is no evidence suggesting that was the case.

In April 2018, the OCC assessed a US$500 million fine on Wells Fargo, concurrently with a fine of US$1 billion from the CFPB. This followed action by the Federal Reserve Board applying the rarely used sanction of imposing a cap on Wells Fargo's growth until Wells cleaned up its mess.[28]

These regulatory hammerings seemed to have no effect. Notes from a 24 January 2019 meeting with Wells senior executives reflected Fed staff concerns that 'leadership seems to remain focused on lifting the asset cap by the end of the year as the primary goal and [shaping] remediation plans around that . . . affect the way management is thinking (or being asked to think) about how remediation should be shaped and accomplished.'

---

26 Egan, Matt, 'Elizabeth Warren's Epic Takedown of Well Fargo CEO', *CNN Business*, 21 September 2016.

27 'Wells Fargo Chairman CEO John Stumpt Resigns; Board of Directors Elects Tim Sloan CEO, Director; Appoints Lead Director Stephan Sanger Chairman, Director Elizabeth Duke Vice Chair', *Business Wise*, 12 October 2016; 'Tim Sloan Named Wells Fargo's President and Chief Operating Officer', https://newsroom.wf.com, 17 November 2015.

28 Office of the Controller of the Currency, 'Press Release', 28 April 2018; Board of Governors of the Federal Reserve System, 'Press Release', 2 February 2018.

Sloan received a US$2 million bonus for his performance in 2018.[29]

In March 2019, Sloan testified before Financial Services Committee of the United States House of Representatives. The chair of the Committee addressed him: 'I am simply asking whether or not the bank is in compliance [with the required remediation plans?].' Sloan replied, 'We are in compliance with those plans.' The OCC promptly advised the House Committee that Wells was not in compliance.[30]

Less than two weeks later, Sloan 'retired' from Wells of his own accord.[31]

In September 2019, the Wells board chose as Well Fargo's CEO and president Charles Scharf, formerly chair and CEO of Bank of New York Mellon.[32]

But Wells' past continued to catch up with it. On 9 September 2021, the OCC assessed another US$250 million fine against Wells.[33] In September 2021, Federal Board Chairman Jerome Powell said that the asset cap would 'stay in place until [Wells] has comprehensively fixed its problems', suggesting the bank had a way to go before it would be allowed to expand in size.[34] It is still in place.

On 20 December 2022, the CFPB issued an order against Wells for a US$1.7 billion penalty and over US$2 billion in payments to consumers, stating in a press release that 'Wells Fargo's rinse-repeat cycle' of consumer law violations has harmed 'millions of American families' through a series of other consumer frauds, including unlawfully repossessing vehicles and freezing bank accounts, wrongful foreclosures and illegal fees.[35]

---

29 The Majority Staff of the Committee on Financial Services, US House of Representatives, 'The Real Wells Fargo: Board & Management Failures, Consumer Abuses and Ineffective Regulatory Oversight', 1 March 2020 ('Wells House Report'), p. 58.

30 *id.* p. 61.

31 Merte, Renae, 'After years of apologies for customers abuses, Wells Fargo CEO Tim Sloan suddenly steps down', *The Washington Post*, 28 March 2019.

32 'Wells Fargo Names Charles W. Scharf Chief Executive Officer and President', https://newsroom.wf.com, 27 September 2019.

33 Office of the Controller of the Currency; 'Press Release'. 28 April 2018.

34 Schroeder, Pete, 'Fed's Powell says Wells Fargo cap to stay until problems fixed', *Reuters*, 22 September 2021.

35 Consumer Financial Protection Bureau, Consent Order, I*n the Matter of Wells Fargo Bank N.A.*, Administrative Proceeding, File No. 2022-CFPB-011, 20 December 2022.

I added this violation information, technically unrelated to the illegalities I focused on above, to drive home the point that by far the most difficult issue for a board, no matter how willing and determined it may be, is how quickly bad behaviour becomes normalised and pervasive.[36]

- Root causes of the scandal include:
- Performance incentives.
- Corporate structure. Wells was recklessly decentralised: Legal, risk management and human resources reported to the heads of the business units and not to corporate.
- Risk management. The Board Report found that certain of the control functions often adopted a narrow 'transactional' approach: 'They focused on the specific [issue] before them, missing opportunities to put them together in a way that might have revealed sales practice problems to be more significant and systemic.' And the Audit Department 'did not view its role to include analysing more broadly the root cause of improper conduct'.[37]
- Senior executives. The board oversaw the hiring and overcompensation of senior executives, 10 of whom were fined over US$58 million; three of them were banned for life from working in the banking industry. The 10 included Stumpf, the head of the Community Bank, chief risk officers, the chief auditor and the general counsel.

The Wells board

Throughout this years-long sordid affair, I cannot point to a single thing the board did competently. The board allowed management, for years and years, to drag its feet and mislead regulators. Moreover, the board itself was complicit in these failures.

In a November 2016 meeting with the CFPB, the CFPB and OCC, board member Quigley complained that 'the Board was spending too much time on Sales Practices and that he was looking to reduce the level of detail with a "Less

36 If you read footnotes, you deserve a bonus. Here goes. In November 2022, police in India arrested a 'top banking executive' for urinating on a 72-year old woman in the business class of a flight from New York to New Delhi. The executive worked for Wells Fargo. Yasir, Sameer, 'Bank Executive Accused of Urinating on a Fellow Airline Passenger', *New York Times*, 7 January 2023.

37 Wells Board Report, p. 14.

is More [approach] to Board materials".'[38] Interviewed by the House Committee Staff, OCC officials 'expressed concerns about Quigley's leadership' and that 'Quigley did not pose "hard questions" to management.'

Betsy Duke (then the vice-chair of the board) asked the CFPB: 'why are you sending [letters requesting actions by the Bank] to me, the board, rather than the department manager?'[39]

The House Report notes that 'From at least mid-2018 through Sloan's resignation in March 2019, concern about Sloan's performance were raised by and to Wells Fargo's board members'.[40]

The lead independent director of Wells Fargo received a letter from the board of governors of the US Federal Reserve System, finding that 'there were many pervasive and serious compliance and conduct failures during your tenure as lead independent director'. The Fed went on: 'you did not appear to initiate any serious investigation or inquiry into the sales practices problems . . . Your performance . . . is an example of ineffective oversight inconsistent with the Federal Reserve's expectations.'[41]

The Federal Reserve was also quite unhappy with the board as a whole: 'Management's reports generally lacked detail and were not accompanied by action plans and metrics to track plan performance.'[42] The Federal Reserve also roundly criticised the shoddy oversight of compensation incentives by the Wells Fargo board.[43] Four directors resigned.

The day following Sloan's testimony before the House Committee, OCC staff members met in executive session with Wells directors. Notes kept by the OCC of the meeting include this: '[W]e are also concerned that the Board has not held management appropriately accountable.' Sloan resigned on 26 March 2019.

The board of Wells Fargo, over almost 20 years, delivered this to its shareholders:

---

38 Wells House Report, p. 46.

39 *id.* p. 44.

40 The Majority Staff of the Committee on Financial Services, US House of Representatives, 'The Real Wells Fargo: Board & Management Failures, Consumer Abuses and Ineffective Regulatory Oversight', 1 March 2020 ('Wells House Report'), pp. 39, 50–58; Office of the Controller of the Currency, 'Press Release', 28 April 2018; Board of Governors of the Federal Reserve System, 'Press Release', 2 February 2018.

41 Board of Governors of the Federal Reserve System, Board Letter re: Accountability as Lead Independent Director of Wells Fargo & Company Board of Directors. Washington, DC: The Federal Reserve, 2 February 2018.

42 See also the discussion on Vale, below.

43 *id.*

- a market capitalisation loss of at least US$220 billion from the imposition of the asset cap in 2018 through May 2020;[44]
- a US$4 billion loss of profits up to only July 2020, according to a Bloomberg estimate[45] (it is fair to speculate that this number has at least doubled in the following almost three years since then);
- by my calculations, fines aggregating over US$10 billion since 2016; and a stupendous fall in reputation. In 2017, Wells was ranked last in overall reputation.[46] In 2022, it was still in last place.[47]

A well-selected board that does its job gives a company a number of persons (in the case of Wells, 16 directors in 2015) of varied experiences, professional and personal, thereby materially increasing the probability that, if management loses its way, gets unmoored, is in denial – in short, is making a mess – one or more of the directors will see the dangers and jump in to clean things up.

Not this board. Excluding two directors, who were in their first year of service, in 2016 the 14 other members averaged over 14 years on the board, 144 years total. They had a century-and-a-half of exposure to Wells Fargo, but were not moved to act even symbolically in defence of shareholders and customers of Wells.

The Wells Fargo board was clueless and hapless, truculent and self-deluding.

Vale

Vale, a Brazilian company, is, and for many years has been, one of the world's leading producers of iron ore.[48] Iron ore extraction is an environmentally hazardous business. The particular hazard we need to know about are iron ore tailings, the fine-particled slurry waste by-product of the process. This mud-like, heavy liquid is collected in tailing ponds, and contained, usually, by an earthen dam.

---

44 Ennis, Dan, '2018 asset cap has cost Wells Fargo $220B in market value', *Banking Dive*, 9 May 2020.

45 Ennis, Dan, 'Wells Fargo has missed out on $4B in profits since asset cap', *Banking Dive*, 25 August 2020.

46 Sposito, Sean, '2017 reputation survey: Banks avoid the Wells Fargo drag', *American Banker*, 27 June 2017.

47 Cross, Miriam, '2022 bank reputation survey: Payoff for thinking outside the box', American Banker, 28 November 2022.

48 NS Energy Staff Writer, 'Top Five Iron Producing Company of the World from Rio Tinto to the National Mineral Development Corporation', NS Energy, 1 September 2020.

In 2015, a dam for one of these 'ponds' near Mariana in the state of Minas Gerais, Brazil, gave way and caused 19 deaths, the greatest environmental disaster in Brazil's history to date.[49] The dam was owned by Samarco, a 50:50 joint-venture of Vale and BHP.

On 25 January 2019, a Vale tailing dam, up a hill from the small company town of Brumadinho, in the same state, collapsed, releasing 13 million cubic meters of tailings, obliterating the town, killing 252 and leaving another 18 unaccounted for. In its wake, numerous investigations were launched, resulting in the CEO of Vale and a number of other executives facing homicide charges and fines in the billions of reais being levied or negotiated.[50]

Vale itself commissioned an independent investigation, led by a former member of Brazilian's Supreme Court. In its report, the investigative team deliberately ranged broadly in its search for answers, and 'included aspects related to governance, risk management, corporate culture, [and] compensation policy and incentives'.[51]

As to these issues, after the Mariana dam failure of 2015, 'dam safety became a frequent subject at meetings of the Board [and its committees.]'[52] The investigation devotes pages to the dam safety reports made to the board and its committees. Though it carefully avoids sharp criticism, we are gently led to two conclusions:

The management reports were general and vague, focused on the fact that regulatory approvals were obtained, rather than on low safety levels at Brumadinho and other dams. '[I]t was noted that presentations on the . . . dams made to the board of directors and their [sic] Advisory Committees signalled the safety of the dams.' In other words, the board was getting sanitised information.[53]

'The review identified no evidence of discussions regarding the decision to cease disposal of tailings at [the Brumadinho facility] or its low factor of safety at the Board of Directors, [or] its Advisory Committees.'[54] It is fair to infer that

49 Relatório Final da CPI, Câmara dos Deputados, Comissão Parlamentar de Inquérito, 'Rompimento da Barragem de Brumadinho', outubro de 2019 ('CPI Report'), p.27.

50 *id.* pp. 27, 38–53.

51 Extraordinary Independent Consulting Committee for Investigation – CIAEA, Executive Summary of the Independent Investigative Report – Failure of Dam 1 of the Córrego de Feijão Mine – Brumadinho, MG, 20 Feb 2020, p.6.

52 *id.* p. 27.

53 *id.* p. 40.

54 *id.* p. 27.

management chose what data to convey, and the board chose to do what many boards are accustomed to: receive the reports, make sure that their substance is recorded in the minutes, and no more.

The report found at Vale 'a strong hierarchical structure that is resistant to the exposure of problems to higher levels . . . Furthermore, there was no incentive for questioning decisions made at higher hierarchical levels.'[55]

It also pointed to a 'siloed environment', with business units reluctant to share information with headquarters:

> *[There] was a work environment that lacked transparency and that did not encourage personnel to raise concerns and/or question leadership decisions*[56] *. . . This cloistered and closed structure led to relevant information that was understood to be unfavorable to generally remain restricted to . . . the Iron Ore Division.*[57]

Vale was, to be kind, solipsistic. Discussions of dam ruptures were framed by monetary considerations only, without taking into account the possible loss of life. They focused mostly on workplace safety, with little attention paid to risks to neighboring communities, that is, 'without the necessary focus on process safety (e.g., minimisation of large-scale risk . . . inherent to operation in a hazardous industry.)[58] . . . [M]ere regulatory compliance is rarely sufficient to generate the safety of highly complex structures.'[59]

The investigation also highlights a phenomenon prevalent at Vale, the 'normalisation of deviance', where repeated exposure to departures from standards over time inures those responsible from the need to deal with these variations. [60]

The report registers 'a major emphasis on financial aspects' of dam safety, finding little or no focus on safety measures. The report states that there were no safety goals for compensation purposes in 2018, and in 2016 and 2017, the only such goals were the completion of external audits and the obtention of favourable inspection certificates.[61]

---

55 *id.* p. 34.
56 *id.* p. 40.
57 *id.* p. 34.
58 *id.*
59 *id.*
60 *id.* p. 35.
61 *id.* p. 39.

Boeing

Another company to look at is Boeing and its troubles arising out of the crashes of two of its recently introduced MAX aircraft, in October 2018 and March 2019, resulting in the death of 346 persons.

Boeing, after decades of near-total commercial aircraft dominance, began in the mid 2000s to lose significant market share to Airbus. In 2010, it found itself in a battle with Airbus for a very large order from American Airlines, until then a loyal Boeing customer.

To satisfy American Airlines and others, the roll-out of the MAX needed to be at supersonic speed. This might seem like the maximisation of profit the stock markets generally expect, but Boeing is not a book publisher or a department store chain, so why did it behave as one, in the face of the 'mission critical' nature of safety for its commercial aviation business?

Boeing began to lose its way over 25 years ago. In 1997, it bought the failing McDonnell-Douglas aircraft manufacturer. Very quickly, the McDonnell-Douglas culture completely overwhelmed Boeing's. The joke in Seattle was that 'McDonnell Douglas bought Boeing with Boeing's money'.[62] Harry Stonecipher, the McDonnell-Douglas CEO who took over leadership of the combined entity, could not have been clearer: 'When people say I changed the culture of Boeing, that was the intent, so it's run like a business rather than a great engineering firm.'[63]

The US House of Representatives Report on the 737 MAX crashes states: 'The prowess of the engineers . . . [was] replaced by the accounting acumen and financial decisions of business executives.'[64]

A veteran business journalist, Jerry Useem, points to the move of Boeing headquarters from Seattle to Chicago in 2001, 1,700 miles from the nearest Boeing commercial airplane assembly plant. 'The isolation was deliberate.' The then-CEO said that when headquarters are close to principal facilities, 'the corporate center is inevitably drawn into day-to-day business operations.' That statement,

62 Useem, Jerry, 'The Long-Forgotten Flight That Sent Boeing Off Course', *The Atlantic,* 20 Nov 2019.

63 Callahan, Patricia, 'So why does Harry Stonecipher think he can turn around Boeing', *Chicago Tribune*, 29 Feb 2004.

64 Committee on Transportation and Infrastructure, US House of Representatives, 'The Design, Development & Certification of the Boeing 737 MAX', 2020 September ('Boeing House Report'), p. 37.

Useem observes, 'captures a cardinal truth about [Boeing]: The . . . MAX disaster can be traced back . . . to the moment Boeing leadership decided to divorce itself from the firm's own culture.'[65]

A *Los Angeles Times* journalist points to the decision in 2011 to 'tweak' the existing 737 model rather than design a new one, as Airbus was doing. The then CEO, under 'explicit pressure' from the board to 'bolster profit', chose to limit cost and accelerate the development of the MAX, which led to software solutions, including the MCAS stability software that has been identified as the determinative factor in the MAX crashes.[66]

Boeing did whatever it could to ensure that regulators not require simulator training for the MAX, as, among other issues, it had a contractual obligation to Southwest that meant up to US$400 million in penalties should simulator training be mandated.

A Boeing test pilot, after undergoing the MCAS stability exercise in a simulator, described the result as 'catastrophic'. The FAA, the US aeronautics administrator, defines catastrophic as: 'Failure conditions that are expected to result in multiple fatalities of the occupants or . . . fatal injury to a flight crewmember normally with the loss of the airplane.'[67]

Edward Pierson, a graduate of the US Naval Academy, a 30-year Navy officer, joined Boeing upon retirement from the US Navy. He was a senior leader of the MAX final assembly facility. Pierson raised his safety concerns with the general manager of the MAX project, Scott Campbell. When Pierson said that in the military, 'we would stop', Campbell retorted: 'The military is not a profit-making organization.' Pierson then wrote to the CEO and even to the entire board of directors. He never heard back.[68]

On 7 January 2021, the US Department of Justice announced that Boeing had entered into a deferred prosecution agreement in which the company had been charged with one count of conspiracy to defraud the United States through misleading statements to regulators by Boeing employees. Boeing agreed to pay over US$2.5 billion, consisting of a criminal penalty of US$243.6 million,

65 Useem (footnote 61, above).

66 Hiltzik, Michael, 'Boeing's Board Shouldn't Escape Blame in 737 MAX Scandal', *Los Angeles Times*, 3 Jan 2020. For a thorough and well-written account of the MAX fiasco, see Robinson, Peter, *Flying Blind: The 737 MAX Tragedy and the Fall of Boeing* (Doubleday, 2021).

67 Boeing House Report, p. 113.

68 *id.* pp. 165–6, 174–182.

compensation of US$1.77 million to MAX airline customers, and US$500 million for a fund to compensate the families of the 346 passengers who died in the two crashes.[69]

Pension fund shareholders filed suit in Delaware Chancery Court against Boeing's officers and directors allegedly involved in the MAX tragedies, seeking damages against those individuals for the benefit of Boeing, as shareholders in the *Blue Bell* case did. To prevail, the funds had to show that the board could not be trusted to bring the action, because of the board members' own culpability. 'This is extremely difficult to do' under Delaware law, said the court: plaintiffs had to show that a majority of Boeing's board members faced a 'substantial likelihood' of liability for Boeing's losses. This showing, under Delaware law, could be based either on the 'complete failure' of directors to establish a reporting system for safety issues, or on directors turning 'a blind eye' to red flags evidencing safety issues.[70] Unusually, the court found that plaintiff stockholders met the pleading standards for both sources of liability.

In a 102-page opinion, the judge laid out a devastating story of carelessness, wilful blindness, duplicity and even plain lying by Boeing.

The court picked up on the dramatic cultural shift after the *McDonnell/Douglas Boeing* merger where the MCD executives became the top dogs.[71]

The court describes Boeing's safety record as 'spotty,' citing recurrent battery fires with the 787 Dreamliner, and a crash of a Boeing 777. Continuing, the court cites 13 different safety issues as Boeing went into 2015 that went uncorrected. As a consequence, the FAA imposed 'historic' fines on Boeing.

The court further found, as to board oversight of airplane safety:

> *None of Boeing's Board committees were specifically tasked with overseeing airplane safety, and every committee charter was silent as to airplane safety differently from other aviation companies with board-level safety committees, such as Southwest, Delta, United, Jet Blue and Alaska.*

The Audit Committee was responsible for risk management, but its yearly updates on risk management did not address flight safety. For instance, the Audit Committee, from the inception of the MAX to its grounding, never mentioned

69 Boeing Deferred Prosecution Agreement, justice. gov., 7 Jan 2021.

70 *In Re Boeing Co. Derivative Litig.* No. 2019-0907-MTZ WL 4059934 (Del. Ch. 7 September 2021).

71 *id.* pp. 8-9.

safety. 'Rather, consistent with Boeing's emphasis on rapid production and revenues, the Audit Committee primarily focused on financial risks.' Airplane safety was not a regular set agenda item for board meetings; the board did not have a channel for receiving in-house complaints about safety.[72]

The Lion Air crash occurred on 29 October 2018. Management did not inform the board for over a week, and when it did, it asserted that the MAX was safe.[73] (I was then on the board of Gol, which flies only Boeing planes and had signed on for delivery of a very large number of MAXes. Gol's board members were told by Gol management of the crash the day after it happened.)

The court then related the underhanded manner in which Boeing tried to tamp down criticism, by denying and criticising media coverage. In a letter to the board on 18 November, the CEO 'bemoaned a steady drumbeat of media coverage and continued speculation . . . and again falsely suggested that the 737 MAX was safe'. The board of Boeing was invited to an optional meeting to be held more than a month after the Lion Air disaster. Management's 'talking points' for the meeting expressed unhappiness with people 'commenting freely, including customers, pilot unions, media and aerospace industry pundits'.[74] Imagine that: Boeing received unflattering coverage for 189 persons being driven into Earth at terminal velocity.

The board formally addressed for the first time the Lion Air crash at its regularly scheduled meeting on 16 and 17 December. Its minutes, says the opinion, reflected not safety concerns but a preoccupation with 'restoring profitability and efficiency'. During its two-day meeting, the board allocated five minutes to a four-page legal memo that included Lion Air matters, and another 10 minutes to compliance and risk management.[75]

At its next meeting, on 24 and 25 February, the board 'decided to delay any investigation until the conclusion of the regulatory investigations'.[76]

A month after the board chose to ignore the causes of the Lion Air tragedy, an Ethiopian Airline MAX crashed on 10 March 2019, killing another 157 persons. Boeing again blamed the pilots, but at that point, a third of the world-wide MAX fleet had already been grounded.

---

72 *id.* pp. 10–12.
73 *id.* pp. 12–18.
74 *id.* pp. 34.
75 *id.* p. 40.
76 *id.* p. 43.

The day that the Ethiopian crash became news, Boeing's CEO got in touch with the board in writing and assured the members about 'ongoing production operations' (that was his big worry) and that management was 'engaged in extensive outreach' with customers and regulators, 'to reinforce our confidence in the 737 MAX'.[77] On 12 March, the FAA grounded the MAX.[78]

Board members were not any more upset about the 157 deaths than about the 189 deaths five months before. Board member Giambastiani emailed the CEO to draw his attention to an article suggesting pilots were at fault in both the crashes.

On 15 March 2019, a director, Arthur Collins, summoned (presumably) all his courage and suggested a board meeting devoted to product safety. He was careful to explain, however, that: 'I recognize that this type of approach needs to be communicated carefully so as not to give the impression that the board has lost confidence in management which we haven't or that it is a systemic problem with quality.'

So: a director diffidently suggests that safety might be discussed at a board meeting, but I leave it to you, Calhoun, new lead director, and to the soon-to-be-fired CEO. 'Just a thought.'[79] Two crashes, almost 350 deaths, a confidence sinkhole of unmeasurable depth, and 'just a thought'.

Flaccid though it was, Collins' suggestion had some effect and a subsequent board meeting devoted over two hours to safety and created a board-level safety reporting function by forming a committee on Airplane Policies and Processes. Unfortunately, this only looked good on paper. Its sessions were sparsely attended, with only one board member attending more than half of the Committee's 18 sessions.[80]

The Airplane Committee in due course recommended that the board establish another committee dedicated to safety, which the board did, the Aerospace Safety Committee. This Committee very quickly suggested that the board form yet another committee, which it did, the Product and Services Safety Organization.[81] This is typical of vacuous, for-show, compliance-related responses. One committee is good, two are better. Three even more so.

But . . . hear the court: 'The Board publicly lied about if and how it monitored the 737 MAX's safety.'

---

77 *id.* p. 46.
78 *id.*
79 *id.* p. 50.
80 *id.* p. 52.
81 *id.* pp. 53–54.

The court cites Calhoun saying that, upon the Lion Air crash, the board had been notified immediately and met 'very, very quickly' thereafter; that the board participated in evaluating the MAX's safety risks; that the board considered grounding that MAX fleet after the Lion Air crash; and that the board met within 24 hours of the Ethiopian crash and recommended that the MAX be grounded. The Court: 'Each of Calhoun's representation was false.'[82]

On 19 November, Calhoun said that from the 'board's point of view, Dennis [Muilenberg] has done everything right'. After the regulators learned 'the extent of Boeing's deceit under Muilenberg's leadership', on 22 December the board terminated Muilenberg and replaced him with – yes – Calhoun, as CEO. In 33 days, Muilenberg went from doing 'everything right' to doing everything wrong.[83] So the Boeing board replaced one insider with another insider, just as the Wells board did.

The Court proceeded to rule on the claim that plaintiffs made that defendants' breached their fiduciary duty to shareholders, 'which is possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgement'. To do so plaintiffs needed to either show that (1) directors 'entirely failed to implement any reporting on information System or controls' or (2) 'having implemented such a system, the directors consciously failed to monitor or oversee its operations'. The court found that both tests were met, which is rare indeed.[84]

In November 2021, about two months after the opinion was handed down, Boeing entered into a settlement of the suit for US$237.5 million, which would be the largest monetary recovery in Delaware from allegations that directors failed to protect the company and its shareholders against the risk of harm. In addition, Boeing agreed that:

- its board would always have at least three directors with safety-related experience;
- Boeing would separate the chair and CEO functions; and
- it would for at least five years have an ombudsman programme to provide employees involved in certification work with a way to raise concerns;[85]

So now we have to change our whole culture?

---

82 *id.* pp. 55–56.

83 *id.* p. 56.

84 *id.* pp. 92–94.

85 Shepardson, David, 'Boeing directors agree to $237.5 million settlement over 737 MAX Safety Oversight', *Reuters*, 5 November 2021.

Yes, if a culture has the kinds of problems here discussed. Here are some suggestions:

- Change your board as much as you need to. The Wells Fargo board in 2021 kept only three directors (of 11) that had been on the board before 2018 and none who had been on before 2015, when the troubles became public.[86]
- Pick as CEO someone from outside. Wells did not do that, and Sloan, the 29-year Wells veteran, turned out almost immediately to be a terrible choice. Calhoun, nine years a director and then the CEO of Boeing, was found by a Delaware judge to be a liar.[87] Charles Scharf, who succeeded Sloan in 2019 at Wells from outside the culture, seems to be trying, but time will tell.
- Have the CEO turn the company upside down. Just as a crisis the size of Wells' was not brought on by relatively few branch employees, or in Boeing's case by four foreign pilots, it is also evident that a culture is not created by one or two directors or executives. Scharf has made sweeping changes at Wells, hiring nearly 90 new executives, at least. These executives came from 22 different companies.[88] Nine of the 17 executives on Wells Fargo's leadership committee are new hires. They can probably continue to shed the old culture, but let us recognise that to meld all these and many other experiences and world views together is very daunting and will take time. Wells will also need for Scharf to do more than change executives. The CEO 'should roll up his sleeves, mingle with the masses . . . to see what life is like in the rest of the company. He must communicate early, honestly and often . . . [The CEO] must set the tone by putting people first in every leadership action he takes.'[89]
- Change behaviour. It is indispensable that management consistently and committedly do the right thing. In many cases, there will be no appetite for profound change because it requires from senior staff and managers qualities that are hard to come by: humility, openness, patience, a thick skin, fair mindedness and the ability to view oneself as a colleague. Amy Edmondson, a Harvard Business School professor, in referring to the MAX accidents and problems at the Boeing 787 Dreamliner plant in South Carolina, wrote: 'This

86 Wells Fargo. 2021 'Notice of Annual Meeting and Proxy Statement'.

87 See footnote 68.

88 Ungarino, Rebecca; Johnson, Carter; Tyson Taylor, 'Wells Fargo has added nearly 90 series hires from JPM, MNY, and other firms in what Charlie Scharf has called a dramatic change to leadership. Here's our exclusive look at the stunning overhaul', *Business Insider*, 14 January 2022.

89 Kanter, Rosabeth Moss, 'It's time for Boeing's new CEO to restore trust by putting people first', CNN Business Perspectives, 15 Jan 2020.

> is a textbook case of how the absence of psychological safety – the assurance that one can speak up, offer ideas, point out problems, or deliver bad news without fear of retribution – can lead to disastrous results.' The only way to change this, according to Edmonson, is by having 'the behavior of managers up and down the line . . . vehemently and continuously supporting psychological safety'.[90]

Cast a constantly wary eye on your company or client, yourself and your colleagues. The arrogance and lack of reflection at Wells Fargo and at Boeing is evident through their handling of the affair. One of the two independent directors at Vale during the dam break crisis very sagely advises:

> *In the monitoring role, it's having a chronic unease – exercising perpetual scepticism, assuming the worse [sic.] may happen and that things may not be working . . . In the advice role, the board should be as committed and close to management as possible without interfering with management responsibilities.*[91]

This is precisely the change in approach boards need to make. The tendency to hold boards more accountable for compliance failures is clear and irreversible. Notwithstanding the protection that directors and officers insurance gives directors, and the care that legislators and the judiciary have historically taken to grant board members a lot of discretion in decision-making, these are being rebalanced to force responsibility on boards in situations such as the ones here described. Perhaps it will be in the form of fines or other sanctions implemented at the regulatory level, such as prohibiting a director, temporarily or for ever, from serving on boards. And until then, negative media coverage, excoriating criticism and relentless shaming will no doubt continue.

It is time for corporate directors everywhere to understand that expectations have changed, and to welcome becoming an active part of efforts that will help prevent the deaths of hundreds and the cheating of millions.

---

90 Edmondson, Amy C, 'Boeing and the Importance of Encouraging Employees to Speak Up', *Harvard Business Review*, 4 May 2019.

91 Davis, Stephan; Guerra, Sandra, 'Crisis – Resilient Boards: Lessons from Vale, Harvard Law School Forum on Corporate Governance', 23 February 2021.

CHAPTER 6

Best Practices for Conducting Compliance Risk Assessments

Daniel S Kahn, Tatiana R Martins and Jordan Leigh Smith[1]

Introduction

Latin America has for many years been an area of focus for US regulatory agencies, and that focus is only growing. In the anti-corruption space, improper payments to government officials in Latin America have constituted an increasingly large proportion of criminal and civil actions brought by US authorities under the US Foreign Corrupt Practices Act (FCPA), from roughly a third of FCPA actions arising from misconduct in Latin America in 2016, to more than 77 per cent in 2022.

Companies seeking to mitigate these legal and regulatory risks should implement an effective compliance programme designed to prevent and detect criminal conduct and non-compliance with corporate policies and procedures. In addition, the US Department of Justice (DOJ) and the US Securities and Exchange Commission (SEC) have continued to speak to, and release guidance regarding the importance of an effective compliance programme when they determine whether and how to enter into a corporate resolution. Indeed, DOJ recently revised its Corporate Enforcement Policy to state that a company that voluntarily self-discloses misconduct in which aggravating circumstances are present can only receive a declination if it had an effective compliance programme at the time of the misconduct. To design such a programme, it is essential to understand the risks unique to each company and tailor the compliance programme

1 Daniel S Kahn and Tatiana R Martins are partners, and Jordan Leigh Smith is counsel at Davis Polk & Wardwell LLP. The authors would like to thank associate David Feinstein and law clerk Nicole Intrieri for their assistance in the preparation of this chapter.

to address those risks. Even when misconduct occurs, the existence of a compliance programme that is thoughtfully designed to address a company's specific risk profile and one that is periodically updated is considered by regulatory authorities to be a critical mitigating factor when determining potential penalties for legal violations.

Importance of risk assessment

The starting point for designing any compliance programme

Expectations of what constitutes an effective compliance programme are well developed, particularly in the United States. The degree to which a company meets those expectations is often a significant factor in the outcome of criminal or regulatory investigations of alleged misconduct or other non-compliance. While there is no 'one-size-fits-all' compliance programme, regulators – in particular, DOJ and SEC – have promulgated different standards for assessing whether a specific programme is effective.

This includes articulating 'hallmarks' that provide detailed guidance to companies on how to implement a programme that addresses certain key principles, starting with how the company has identified, assessed and defined its risks, and the degree to which the programme devotes appropriate scrutiny and resources to the spectrum of risks.[2] A well-designed legal and regulatory compliance programme therefore should be grounded both in preventing and mitigating risks, and also in documenting the process through which risks are identified, monitored and addressed.

Overview of the risk assessment process

Organisations conduct assessments to identify a number of different types of enterprise risks, including strategic, operational, financial and compliance. Within that overall approach, a compliance risk assessment seeks to identify risks relating to a company's ability to adhere to applicable legal and regulatory regimes. Such risk assessments seek to ensure that appropriate controls are in place to reduce the likelihood or scope of a violation and corresponding regulatory action.

Understanding a company's geographic and operational footprint, and how that footprint interfaces with the relevant regulatory regimes, is the necessary starting point for any compliance risk assessment process. This will enable the company to understand the general compliance risk profile of its organisation.

2 Evaluation of Corporate Compliance Programmes, Department of Justice Criminal Division (June 2020) (ECCP).

With this general understanding, the next step in the risk assessment process is to identify the areas of the business that pose a higher likelihood of possibly violating applicable laws, and evaluate the key policies and procedures in place to control for those risks.

In undertaking this exercise, which is often referred to as 'risk mapping', companies consider the likelihood that the risk of violating the law will be realised given current controls, as well as the impact that such a violation would be expected to have on the company. Risk mapping allows companies to identify critical gaps in controls and to determine how to prioritise addressing those gaps based on the actual risks – specifically, the likelihood of a violation combined with the severity of the consequences such a violation would have on the business.

Therefore, an ideal risk assessment process seeks to identify not only the existence of a risk, but the likelihood that it may occur, its relevant vectors to the company's operations and the potential severity of its impact should that risk materialise. Although companies in the same industry and geographical region may have similar risk profiles, and can often learn from one another regarding various risks, the specific risk profile of every company is inherently unique. A company cannot effectively allocate compliance resources, design policies, procedures and controls, devise trainings for relevant employees and otherwise implement a well-functioning compliance programme absent an understanding of these unique risks.

Appropriately allocate resources and implement practical controls

The adequacy of resources allocated to a compliance programme generally, and to identify risks within that framework more specifically, is another hallmark of an effective compliance programme. The design of a corporate compliance programme should start by asking not just what the relevant risks are and how the company has elected to address them, but whether the compliance programme devotes appropriate 'scrutiny and resources' to the risks identified.

A critical aspect of a well-designed compliance programme is having the appropriate focus and resourcing on the areas of highest risk to the company, which depends in part on the initial risk assessment. Tailoring attention and resources on a risk-weighted basis is not only important to allow for internal monitoring of potential compliance lapses, but also can be critical in defending a compliance programme in the US and, increasingly, jurisdictions such as Brazil and other countries in Latin America. As discussed below, in the US, the government gives

its prosecutors authority to 'credit the quality and effectiveness of a risk-based compliance programme' that devotes resources and attention in a risk-appropriate manner, even where that programme fails to prevent an infraction.[3]

Identifying risk

Determining the inputs

A risk assessment is only as good as the inputs used to identify risk. As noted in the DOJ's Evaluation of Corporate Compliance Programmes (ECCP), an effective risk management programme is designed to detect the particular types of misconduct most likely to occur in a particular corporation's line of business.[4] In determining the likelihood of such misconduct, companies should analyse the risks based on factors such as the location of its operations, the relevant industry, the competitiveness of the market, the regulatory landscape, potential clients and business partners, transactions with foreign governments, payments to foreign officials, use of third parties, gifts, travel and entertainment expenses, and charitable and political donations.[5] This list is not exhaustive, but should be treated as a minimum standard for conducting a risk assessment.

To align with the ECCP's guidance, those conducting a risk assessment should reflect on the methodology that the company has used to identify and address the particular risks it faces. A company should pay particular attention to the types of information and metrics it has collected and analysed to detect misconduct, and how those metrics have informed the company's weighting of risks and allocation of resources.[6]

Common methods for detecting potential compliance gaps include the use of employee questionnaires and surveys, interviews with subject matter specialists and business operations personnel, and third-party diligence and audit reports. In addition, DOJ guidance specifies that the use of mechanisms for confidential internal reporting of suspected misconduct, and processes for conducting prompt internal investigations of allegations and incorporating lessons learned from those investigations into your risk assessment process, are further hallmarks of an effective compliance regime.

3 ECCP at 3.
4 *id.* at 8.
5 *id.* at 3.
6 *id.* at 2–3.

Regulatory officials have increasingly highlighted the need to use data to drive risk assessment and monitoring. As such, an effective compliance model will continually look for ways to quantify risks and monitor compliance. This does not necessarily require the application of sophisticated AI or computer modelling. Though such methods are obviously desirable where appropriate and consistent with a company's resources, core competencies and business model, there are other, less technical opportunities to use data to drive compliance efforts. Quantitative analysis can be applied to key risk assessment metrics like the volume of complaints and the speed of a company's corresponding investigation and resolution. Similarly, while information may be readily available about the volume, frequency and amount of payments to third parties acting on behalf of the company, a quantitative assessment might establish and rely on the application of averages, baselines and other metrics for identifying irregularities.

Common compliance risk vectors

Each company faces its own unique risks, and there is no universal set of criteria for assessing risk comprehensively. However, there are a number of risk vectors that are widely accepted as posing significant compliance risks.

Industry

Certain industries have been historically prone to enforcement actions for compliance failures, such as natural resources extraction and construction or engineering. The concentration of regulatory activity in these industries might be attributed in part to the geographic dispersion of their operations, as well as the frequency of interaction with government officials and state entities. In the extraction industry, obtaining business-critical permits and licences inevitably entails the involvement of government officials at the national, regional and local levels. Similarly, many large construction projects in Latin America are infrastructure projects tendered by government entities and overseen by a relatively small number of key officials. While certain industries figure more prominently in the history of government compliance enforcement actions, the DOJ and SEC are not limited to enforcement actions in those industries, and indeed are often looking for new areas in which to signal the importance of adherence to the anti-bribery laws.

Accordingly, staying abreast of developments in this space remains essential. For example, WPP plc's 2021 resolution with the SEC stemmed from an alleged bribery scheme regarding improper payments to purported vendors in connection with obtaining government contracts in Brazil, and bribes to fund

a political campaign in Peru. WPP, an international advertising and marketing conglomerate, was undertaking an aggressive global expansion by acquiring local companies in high-risk markets within Latin America.[7]

More recently, Stericycle's 2022 resolutions with DOJ and the SEC stemmed from an alleged scheme including millions of dollars in the form of hundreds of bribe payments to obtain and maintain business from government customers in Brazil, Mexico and Argentina, as well as to obtain authorisation for priority release of payments owed under government contracts. Stericycle, an international waste management network, focused primarily on medical, industrial, and maritime waste as well as document destruction, was similarly undertaking an aggressive global expansion in high-risk markets within Latin America.[8] While waste collection and advertising are less characteristically industries of focus for anti-corruption actions, rapid expansion into these markets opened Stericycle and WPP to risks that may not have historically been a touchstone in their respective industries.

Government touchpoints

As noted above, certain industries have historically been considered high-risk for compliance misconduct because they typically entail a high level of dependence on government permits, approvals and contracts. Dependence on interactions with national or local government inevitably creates a risk of corrupt activity. While observers of the compliance industry will no doubt be familiar with the *Lava Jato* investigation in Brazil and its progeny, more recent notable examples in Latin America include Tenaris's 2022 resolution with the SEC over allegations that it bribed officials at Brazil's state-owned oil company to receive confidential information and to win government contracts. Additionally, Honeywell's 2022 coordinated resolutions with DOJ and the SEC involved allegations that agents of Honeywell's subsidiary paid millions in bribes through an intermediary sales agent to a high-ranking Brazilian government official, in order to obtain and retain business from Brazil's state-owned company.

To that end, companies that engage in a high percentage of business with state-owned entities or rely on government permits should pay particular care to that aspect of their risk assessments. Beyond the payment of cash bribes, though,

7 'SEC Charges World's Largest Advertising Group with FCPA Violations' (24 September 2021), https://www.sec.gov/news/press-release/2021-191.

8 'SEC Charges Stericycle with Bribery Schemes in Latin America' (20 April 2022), https://fcpa.stanford.edu/fcpac/documents/5000/004375.pdf.

care should also be taken in assessing and addressing the risk associated with seemingly more innocuous business practices, such as offers of gifts, entertainment or travel. Though at some level these practices are standard and accepted, they can also be used to influence officials. Companies can mitigate risks associated with business travel and entertainment in many ways, but where such practices are prevalent, an effective risk assessment will seek to understand industry and local customs and regulations in service of detecting irregularities.

Other common red flags to be aware of when considering whether a gift to a government official is appropriate include if the business purpose seems incidental to an entertainment purpose; if the government official is strategically situated to award business to the company; if a travel destination may be perceived as exotic or desirable; if the official's spouse or family members are invited; if expenses are paid to the official personally; or if the official is reluctant or unwilling to get written approval.

Operations or other business conducted in high-risk countries

The Biden administration has recently signalled an increased focus on regions deemed 'high-risk' for compliance misconduct and, in particular, corruption. On 6 December 2021, the administration released the United States Strategy on Countering Corruption as its first major step pursuant to its 3 June 2021 Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest, which outlined a heightened focus on 'priority', high-risk countries.

While the administration's official documents declined to specify which countries qualify, a large proportion of recent anti-corruption resolutions and individual actions have arisen from alleged misconduct in Latin America, including resolutions with Glencore (Brazil), Stericycle (Brazil, Mexico and Argentina), Tenaris (Brazil and Panama), GOL Linhas Aéreas Inteligentes S.A. (Brazil), WPP plc (Brazil and Peru) and Jardine Lloyd Thompson Group Holdings Ltd. (Ecuador). In fact, misconduct in Brazil alone was alleged in four of the DOJ's and SEC's nine foreign corruption resolutions in 2022. Similarly, on 15 October 2021, the DOJ announced a new tip line to receive information regarding potential corruption in the Northern Triangle nations of El Salvador, Guatemala and Honduras.

The administration's clear focus on high-risk regions, combined with the frequency of enforcement actions and prosecutions predicated on conduct in Latin America, underscore the compliance risk facing companies operating in the region. As a result, such companies should ensure that their risk assessments are particularly mindful of recent regulatory news and developments, and that they have controls in place that reflect lessons learned from those matters.

Nature and extent of use of third parties

Perhaps one of the most critical factors for assessing how well a company evaluates and manages risk relates to its use of third parties such as agents, vendors, distributors and resellers. The ECCP directs prosecutors to assess a company's third-party risk management practices as a factor in determining whether a given compliance programme is in fact able to 'detect the particular types of misconduct most likely to occur in a particular corporation's line of business'.[9] Similarly, the July 2020 update to the DOJ and SEC's FCPA Resource Guide (Resource Guide) emphasised that companies must conduct 'risk-based due diligence' and monitoring of third parties, which it says are 'commonly used to conceal the payment of bribes'.[10] Additionally, the ECCP suggests that regulators will examine whether companies 'engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process'.[11]

Consequently, ongoing monitoring of third parties, including through such mechanisms as periodic renewal procedures and a risk-based third-party audit programme, are now particularly important for companies that utilise third parties to do business in Latin America. Indeed, the Resource Guide highlights that simply '[r]elying on due diligence questionnaires and anti-corruption representations is insufficient, particularly when the risks are readily apparent'.[12] To that end, regulators emphasise the importance of using data analytics to conduct ongoing monitoring of third-party payments for irregularities, and keeping track of data related to third-party due diligence and payments.

With heightened compliance risk stemming from the use of third-party agents, companies should first determine whether there is a clear business need to engage them, and be sure to document its rationale. Third parties and other intermediaries who may interact with government officials on the company's behalf must be carefully evaluated in particular, including through methods such as background and qualification checks, properly monitoring invoices and the methods and amounts of payments, and confirming that contractual protections such as audit rights and termination rights are fully utilised. By way of example, in Tenaris's 2022 resolution with the SEC, the company was credited for reducing its usage of third-party agents worldwide after allegations that it used third-party

9 ECCP at 8.

10 A Resource Guide to the US Foreign Corrupt Practices Act, Department of Justice and Securities and Exchange Commission (July 2020) (Resource Guide), 62.

11 ECCP at 8.

12 Deferred Prosecution Agreement, *United States v. UOP LLC d/b/a Honeywell UOP* (19 Dec. 2020).

agents to bribe a Brazilian-state owned entity. Similarly, in Honeywell's 2022 resolution with DOJ and the SEC, the company was likewise credited for 'taking steps to eliminate the Company's use of sales intermediaries and, in the interim, rolling out a single, automated sales intermediary due diligence tool that requires responsible managers to provide quarterly compliance certifications for all existing sales intermediaries.'[13]

Level of M&A activity (including joint ventures)

Companies active in the M&A space must be aware that the DOJ and SEC can and will hold buyers responsible for the past conduct of acquired entities, particularly when that conduct continues post-acquisition. Both agencies have emphasised that well-designed compliance programmes should include comprehensive due diligence of any acquisition targets, but also note that, when robust pre-transaction due diligence proves challenging, prompt post-acquisition diligence is expected and that, in any event, timely compliance system integration is critical.

The Resource Guide recognises the importance of the acquiring entity having 'a robust compliance programme in place and implement[ing] that programme as quickly as practicable at the merged or acquired entity'.[14] The ECCP stresses the need for a 'process for timely and orderly integration of the acquired entity into existing compliance programme structures and internal controls', as well as 'post-acquisition audits'.[15]

Thus, it is imperative that companies engaged in M&A activity seek to understand the risks they may be inheriting by conducting fulsome risk assessments (both pre- and post-transaction), as well as timely, risk-based compliance integration. DOJ has noted that prior misconduct committed by the acquired entity will be given less weight if the acquiring corporation addressed the root cause of the misconduct before the conduct currently under investigation occurred, and full and timely remediation occurred within the acquired entity before the conduct currently under investigation.

Ultimately, failure to anticipate corruption and other compliance risks in M&A transactions can have significant legal and commercial consequences. Aside from the risk of regulatory action, business that depends on unknown corrupt practices of the acquired company may be lost when those practices are eventually

13 Resource Guide at 65.
14 Resource Guide at 29.
15 ECCP at 9.

discovered (ideally through diligence and risk assessment by the acquiring entity). Additionally, contracts obtained through bribes of the acquired company may be legally unenforceable. Lastly, the continued existence of inaccurate books and records, including entries disguising past bribes or other misconduct, may raise the spectre of accounting and internal controls enforcement action directed at the successor entity.

Similarly, joint ventures have figured prominently in enforcement actions and continue to attract regulatory attention. Joint ventures present risks of both M&A transactions and classic third-party business partner arrangements, and joint venture partners may also be liable for taking any action in furtherance of a venture's improper activity, regardless of whether the company controls the joint venture. If a company is a majority owner of a joint venture (typically defined by US regulators as having majority voting power), regulators will expect that company to be in a position to dictate the joint venture company's policies and procedures. However, even non-controlling participants are required to use good faith efforts to exert their influence to prevent violations of law and ensure that an effective compliance programme is in place. As in any transaction, risk assessment and due diligence are paramount, with particular consideration given to the jurisdiction of the proposed joint venture, the business model and nature of the proposed business activity of the venture, the degree of dependence on government contracts, permits, licences and other regulatory actions, and the anticipated frequency of interactions with government officials.

Known issues

Now more than ever, companies with past or pending resolutions should be particularly focused on their risk assessments.

In a pair of speeches and accompanying memoranda in October 2021 and September 2022, US Deputy Attorney General (DAG) Lisa Monaco made clear that companies with a prior history of misconduct will be treated more harshly and will face a greater prospect of having to plead guilty in connection with new misconduct. She announced that the most significant types of prior misconduct would include criminal resolutions in the United States, prior misconduct involving the same personnel or management, and misconduct sharing the same root causes as that of prior resolutions. Additionally, dated conduct addressed by criminal resolutions finalised more than 10 years as well as civil resolutions finalised more than five years prior will generally be accorded less weight.

Similarly, failures to rectify known issues that are not yet the subject of regulatory action can have significant consequences. In WPP's 2021 resolution with the SEC, the company was cited for failing to promptly or adequately respond to

'repeated warning signs of corruption or control failures at certain subsidiaries'.[16] In Tenaris's 2022 resolution with the SEC, the SEC considered that the company had previously entered into a non-prosecution agreement (NPA) with DOJ and a deferred prosecution agreement (DPA) with the SEC, noting that '[t]his [was] not the first time Tenaris has been involved in a corruption scheme'.[17]

Existing controls and compliance programme

Part of any risk assessment involves taking a fresh look at a company's existing compliance programme. The risks identified in consultation with compliance professionals and subject matter specialists throughout the company should be mapped and tested against those existing controls. Doing so serves to identify potential areas of weakness in existing controls, as well as create opportunities to leverage or improve them. This may include other risk assessment systems at the company, its internal audit functions, and employee training or issue reporting processes.

At a minimum, testing of existing controls should be conducted with reference to the hallmarks of an effective programme as enumerated in the ECCP and other relevant guidance, as well as industry best practices and local regulator expectations. Particularly in regions deemed to present higher compliance risk, active monitoring of regulatory and industry developments and enforcement actions helps to ensure that a company's programme is not just capable of identifying the appropriate spectrum of risks, but has a documented basis for contesting charges of inadequacy, especially where the government's expectations around compliance programme design may supersede local or regional standards.

US prosecutors are also directed to consider the manner in which the company's compliance programme has been tailored based on its risk assessment. Companies should make use of risk assessments to ensure that they are giving greater scrutiny, as warranted, to higher-risk areas and transactions than more modest and routine transactions. For instance, the ECCP posits that a 'large-dollar contact with a government agency in a high-risk country' is more likely a high-risk transaction than 'more modest and routine hospitality and entertainment'.[18] Beyond that, though, companies are advised to remember that careful, documented consideration of factors (including analysis of data gathered from oversight and operations

16 See 'SEC Charges World's Largest Advertising Group with FCPA Violations,' (24 September 2021), https://www.sec.gov/news/press-release/2021-191.

17 'SEC Charges Global Steel Pipe Manufacturer with Violating Foreign Corrupt Practices Act,' (June 2, 2022), https://www.sec.gov/news/press-release/2022-98.

18 ECCP at 3.

alike) leading to risk-tailoring decisions will later prove useful in maximising any potential leniency the ECCP and other guidance permits prosecutors to exercise, should misconduct occur.

Who conducts the compliance risk assessment

In preparing to conduct or update a compliance risk assessment, what considerations about the structure and authority of that process apply? Put simply, who within the company should conduct compliance risk assessments? Ideally, such assessments are overseen by the company's compliance function, with input from relevant stakeholders within the organisation, including the business and the board of directors. It is critical that the compliance function engage with the business during this process, as the business 'owns' and is most familiar with the risks and related controls as a natural product of their direct involvement in the day-to-day operations of the company. Compliance collaborates with the business to define the risks, provide guidance on legal requirements, and monitor the risks and related controls to ensure the compliance programme is operating as intended.

As a company's key overseers, it is also essential that the board of directors or an appropriate sub-committee are involved in, or at least briefed on, both initial and ongoing risk assessments. When the DOJ resolves a financial fraud or FCPA case, it routinely includes an 'Attachment C' detailing 'Corporate Compliance Programme' requirements to be met in connection with the resolution of the case. Attachment C clarifies that responsibility for the implementation and oversight of a company's compliance code, policies and procedures – including those inherent in conducting a risk assessment – should be assigned to one or more senior executives with authority to report directly to independent monitoring bodies. To ensure the integrity and utility of that reporting line, Attachment C sets forth requirements that include the need to conduct training and effectively communicate policies and procedures not just to officers, employees and agents, but to directors as well.

Periodically updating risk assessments

Importance of renewing risk assessments periodically

While a risk assessment may be the starting point in designing a compliance programme, it is critical to understand that the process of identifying and evaluating legal and regulatory compliance risks does not end with the initial assessment. One of the hallmarks of an effective compliance programme, as enumerated in the ECCP, is that it has procedures for conducting regular and ongoing risk assessments. The DOJ directs prosecutors to evaluate a company's

'revisions to corporate compliance programmes in light of lessons learned', as an indicator of appropriate risk identification and tailoring.[19] Thus, risk assessment is not an event but a process, one that is actively monitored and evolves over time. The DOJ and SEC emphasise the importance of renewing risk assessments periodically to prevent a compliance programme from stagnating. Regulators will assess whether a company's periodic risk assessment updates are 'limited to a 'snapshot' in time' or whether updates are also triggered by events and the results of continuous monitoring. Recall that the ECCP allows prosecutors to credit the quality and effectiveness of a risk-based compliance programme that devotes appropriate attention and resources to high-risk transactions, even if it fails to prevent an infraction. As a result, efforts should be made to risk-tailor compliance programmes in light of lessons learned, not only to prevent misconduct, but as evidence of a well-functioning compliance programme. This demonstrates the importance of having a process to document and incorporate lessons learned into an ongoing risk assessment. For example, companies should ensure that they have in place a process for tracking and incorporating into their periodic risk assessments any key takeaways from both their own prior issues and from those of other companies operating in the same industry or region.[20] To the extent companies can promptly risk-tailor their compliance programmes in this way, those efforts can bolster a defence against enforcement action even if misconduct occurs.

Thus, any risk assessment should be subject to periodic review, both cyclically and as triggered by events, to ensure that the programme remains defensible and current. Any compliance programme updates should likewise incorporate new or evolved risks, whether discovered through misconduct or other periodic self-assessment activities.[21]

Triggering events for renewed assessment

As indicated, risk assessments should be renewed periodically regardless of whether there is a specific triggering event. However, there are particular events that can warrant an immediate renewal of a risk assessment process or that will be more likely to result in significant changes to the results of your risk mapping. In determining what events should trigger updates to a risk assessment, keep the following in mind.

19 ECCP at 3.

20 *id.*

21 *id.* at 15.

Change in business model, applicable regulatory scheme or operations

Changes to a company's business model will likely change the company's risks. Take, for instance, a company that formerly dealt exclusively in managing business-to-business payments, but has now expanded to provide consumer-level retail payments. Whereas the company's risk management previously may have relied on tools like audit rights in customer contracts and long-standing experience in customer industry norms and practices, in its new retail venture, these practices may be of limited value.

Additionally, updates or changes to regulatory schemes may alter a company's risk landscape. For instance, the Anti-Money Laundering Act of 2020 (AMLA) expanded the Bank Secrecy Act's definition of 'financial institution' to cover those engaged in the exchange or transmission of 'value that substitutes for currency', such as cryptocurrencies, and added further industries like antiquities dealers, advisers and consultants to the definition.[22] Doing so brings such entities within the nominal purview of extensive money laundering regulations. Coming within the scope of a new regulatory scheme imposes new compliance obligations and therefore compliance risks.

Finally, changes in a company's operations can alter the company's sources of compliance risk. For example, a company that shifts from in-house manufacturing to outsourced manufacturing in foreign countries must now develop a process for identifying new sources of risk, like sanctions risk and risks associated with reliance on foreign government interactions.

Acquisition of new entity

As noted above, companies may inherit the risks of misconduct at acquired companies. Where robust pre-transaction due diligence is possible, an acquiring company can more accurately evaluate a target's value and negotiate for the costs of any corruption or misconduct to be borne by the target. Where such diligence is challenging, there is still significant value in prompt post-acquisition efforts to integrate the new business into the compliance function, root out potential compliance failures, and self-disclose them.

Importantly, the risk assessment is not only important for the acquiring company in identifying what new exposure it now has, but also in determining how best to implement the company's policies, procedures and controls at the newly acquired entity. It is often the case that the company's compliance programme will need to be right-sized to best fit the newly acquired entity.

22 AMLA, Section 6102(d).

Internal misconduct

The existence of newly discovered violations of company policy or law constitutes an important data point for the company's risk assessment. That is, if some employees engaged in misconduct, that is one potential risk that may be exploited again. As such, each instance of internal misconduct that is identified should inform a company's risk assessment procedures going forward.

Misconduct at companies operating in similar industries or regions

Relatedly, news of alleged misconduct at companies operating in similar industries or regions marks an opportunity to re-evaluate your own risk assessment. Enforcement announcements are typically intended to trigger self-reflection at similarly situated entities. Even beyond their utility in providing information about compliance that regulators deem a high priority, staying responsive to such developments highlights senior leadership's earnestness and good faith, and conveys that an organisation can effectively adapt to changes in the business environment.

For instance, when enforcement activity begins to touch new industries, companies in that industry should expect a higher level of scrutiny and respond accordingly. Recent such signposting by the government includes the aforementioned Strategy on Countering Corruption, which named a number of particular industries that the Biden administration plans to focus its anti-corruption efforts on, including private equity, investment advisers and real estate.

Conclusion

The prospect of accurately identifying and monitoring a spectrum of risks in an ever-shifting business environment may be daunting. However, there are certain touchstone principles upon which companies can consider relying:

- Understand the risks that face the company as a result of its geographic and operational footprint.
- Design the risk assessment with all the relevant data points possible, including data relating to the company's government touchpoints, operations and business in high-risk countries, use of third parties, M&A activity, prior instances of internal misconduct, and risks that were identified in connection with regulatory actions against other companies operating in the same region or industry.
- Become knowledgeable about regulator expectations, and remain attuned to changes as reflected in guidance and the lessons of recent enforcement actions.
- Look for ways to modernise assessments of risk through data analysis and quantification of relevant inputs.

- Ensure that risk assessments are not only conducted on-cycle, but are responsive to off-cycle developments and triggering conditions.
- Focus on ensuring robust integration of – and communication between – subsidiaries and centralised compliance functions.
- Treat documentation of processes and rationales as if it were as important as the underlying compliance processes. If misconduct occurs, this material will be critical in defending a compliance programme against charges that it was inadequately designed or otherwise dysfunctional.

CHAPTER 7

Third-Party Due Diligence: Expanding Compliance Programmes to Suppliers and Clients

Palmina M Fava, G Zachary Terwilliger and Martin Pereyra[1]

The use of third parties in a company's efforts to expand its business, whether internationally, domestically or locally, is not only inevitable but necessary. From manufacturing to supply chain through to distribution and product services and support – and including many other key functions of a business previously handled internally (e.g., human resources, information technology, finance and audit) – there is a fast-growing outsourced business model that relies on third parties. Often, using third parties is cheaper, faster and more effective, rendering it a competitive necessity. Third parties can take the form of a company's agent, intermediary, supplier, consultant or joint venture partner and can provide the company with invaluable and critical services, ranging from product design or delivery to legal or tax advice to sales opportunities. For example, a third party could provide crucial transportation of goods without which a company could not bring its product to market.

The modern approach of disaggregating business functions necessarily means that doing business through a number of third parties is the norm and not the exception, resulting in a growing volume and diversity of third parties that brings inherent corruption risks. Companies must be cognisant of such risks and prepared to mitigate them to maximise the third parties' utility.

---

1 Palmina M Fava and G Zachary Terwilliger are partners, and Martin Pereyra is an attorney at Vinson & Elkins LLP.

Pursuant to the strictures of the Foreign Corrupt Practices Act (FCPA), companies are prohibited from either directly or indirectly bribing non-US government officials to obtain business. Indirect bribes expressly include payments made by third parties acting on behalf, at the direction, or with the knowledge of the company.[2] To be liable under the FCPA, a company need not explicitly authorise the payment. As long as the company had a reasonable belief that the conduct was likely to occur, it can be held liable for the third party's conduct. Knowledge of improper payments – or even the offer of anything of value – can be inferred from circumstances demonstrating a reasonable probability of illicit conduct.[3] Thus, companies cannot avoid liability by consciously disregarding or ignoring red flags suggest-ing that a bribe has been or will be offered, promised or made. Walmart's settlement with the Secu-rities and Exchange Commission (SEC) and the Department of Justice (DOJ) is a perfect example of the FCPA's unforgiving nature towards alleged deliberate ignorance.[4] In 2019, the SEC charged Walmart with violating the FCPA by failing to implement and operate a compliance programme sufficiently tailored to mitigate its risks. The order alleged that Walmart ignored red flags and corruption allegations when it expanded its business internationally, allowing its subsidiaries in Brazil, Mexico, China and India to use third-party intermediaries to make pay-ments to foreign government officials. Walmart allegedly failed to investigate and mitigate the risks and paid more than US$282 million in penalties and fines.[5]

---

2 The Foreign Corrupt Practices Act of 1977, 15 U.S.C. § 78dd-1.

3 *id.*

4 Press Release, Sec. and Exch. Comm'n, Walmart Charged With FCPA Violations (20 June 2019), https://www.sec.gov/news/press-release/2019-102; Press Release, Dep't of Justice, Walmart Inc. and Brazil-Based Subsidiary Agree to Pay $137 Million to Resolve Foreign Corrupt Practices Act Case (20 June 2019), https://www.justice.gov/opa/pr/walmart-inc-and-brazil-based-subsidiary-agree-pay-137-million-resolve-foreign-corrupt. A more recent example involves WPP's settlement with the SEC regarding allegations that WPP violated the anti-bribery, books and records, and internal accounting controls provisions of the FCPA. According to the SEC order, WPP acquired advertising agencies in high-risk areas, including India, China, Brazil and Peru, and failed to implement internal accounting controls and compliance policies to mitigate the risk of corruption. One of the allegations in the order stated that WPP received an accounting report and anonymous complaints suggesting that its subsidiary in India was engaging in corrupt practices through the use of a third-party intermediary. WPP failed to adequately respond to these warning signs. WPP paid more than US$19 million in fines and penalties to resolve the charges. See Press Release, Sec. and Exch. Comm'n, SEC Charges World's Largest Advertising Group with FCPA Violations (24 September 2021), https://www.sec.gov/news/press-release/2021-191.

5 See also Press Release, Dep't of Justice, SBM Offshore N.V. and United States-Based Subsidiary Resolve Foreign Corrupt Practices Act Cases Involving Bribes in Five Countries

A company's exposure to liability for third-party actions is not unique to the FCPA. Anti-corruption laws in most countries hold companies culpable for third-party conduct.[6] Latin American countries are no exception. For example, Mexico has enacted a number of anti-corruption laws as part of its National Anti-Corruption System.[7] Under these laws, a company can be held liable for the actions of individuals who engage in corrupt offences on behalf of the company.[8] Brazil's Clean Company Act takes this a step further. Under the Act, companies are held strictly liable for the corrupt conduct of their employees and agents.[9] Take Glencore International A.G. (Glencore) as an example. From 2007 to 2018, Glencore allegedly paid more than US$100 million to third-party intermediaries, with a portion allegedly intended to be used to reward government officials in Nigeria, Cameroon, Ivory Coast, Equatorial Guinea, Brazil, Venezuela and the Democratic Republic of the Congo.[10] The DOJ in its press release noted the involvement of high-level employees and agents of the company as an important factor in reaching the terms of the agreement.[11] In May 2022, Glencore

(29 Nov 2017), https://www.justice.gov/opa/pr/sbm-offshore-nv-and-united-states-based-subsidiary-resolve-foreign-corrupt-practices-act-case. On 29 November 2017, SBM Offshore N.V. (SBM) was assessed a criminal penalty from the DOJ in the amount of US$238 million for an alleged bribery scheme in violation of the FCPA. For approximately 16 years, SBM allegedly paid third-party intermediaries US$180 million in commissions that were used to bribe government officials in Brazil, Angola, Equatorial Guinea, Kazakhstan, and Iraq. The order found that SBM was liable because it knew that a portion of the commission payments would be used to pay these bribes for the purposes of obtaining business with state-owned oil companies.

6 For example, the United Kingdom's Bribery Act states that an organisation or company is liable for the corrupt actions taken by a person 'associated' with the company and on the company's behalf. The Act defines an associated person as one who performs services for the company, such as an employee or agent. See Bribery Act, 2010, c.23, § 7(1) (U.K.); Ministry of Justice, The Bribery Act 2010, at 16 (March 2011).

7 See Ley General Del Sistema Nacional Anticorrupción [LGSNA], Diario Oficial de la Federación [DOF], 18 July 2016.

8 *id.*

9 See Brazil Clean Company Act (Law No. 12.846/2013).

10 See Plea Agreement, *United States v. Glencore Ltd.*, 3:22-cr-00071-SVN (D. Conn. 24 May 2022), https://www.justice.gov/opa/press-release/file/1562401/download; see also Press Release, Dep't of Justice, Glencore Entered Guilty Pleas to Foreign Bribery and Market Manipulation Schemes (24 May 2022), https://www.justice.gov/opa/pr/glencore-entered-guilty-pleas-foreign-bribery-and-market-manipulation-schemes(Glencore DOJ Press Release).

11 See Glencore DOJ Press Release.

agreed to pay over US$700 million in criminal fines and disgorgement to US authorities related to the conduct of its third-party intermediaries and accepted a three-year compliance monitorship.[12]

Liability exposure heightens the need for companies to exercise control and oversight over their business partners and agents, including suppliers and, in certain circumstances, clients. Companies must take the necessary steps to expand their compliance programmes to mitigate the risks that arise from their business dealings. Among the steps utilised by many companies and expected by many regulators are conducting thorough background checks or due diligence prior to engaging a third party; educating a third party on the applicable anti-bribery and anti-corruption laws; contractually mandating a third party's compliance with the same; and monitoring the third party's actions throughout the life of the contract.[13] The level of due diligence, compliance training and monitoring to be performed by the company on the third party depends on the scope of work provided by the third party, the inherent risk of the work or the transaction, the geographic location of the deal, the industry and the compensation to be paid.[14] A company's vendor of office supplies, for example, will not be subject to the same scrutiny as the company's customs broker or freight forwarder interacting with government officials on behalf of the company.

How to assess third parties

Risk-tiered due diligence

Before engaging a third party or entering into a transaction with a customer, companies must learn about the entity on the other end of the deal to fully evaluate the potential liability risks triggered by that entity and to ensure that the internal controls built into the company's compliance programme are deployed appropriately to mitigate the risk. For example, a company may employ certain

---

12 See *id.*; see also Press Release, Sec. and Exch. Comm'n, SEC Charges Amec Foster Wheeler Limited with FCPA Violated Related to Brazilian Bribery Scheme (25 June 2021), https://www.sec.gov/news/press-release/2021-112. From 2012 to 2014, Amec Foster Wheeler Limited's (Foster Wheeler) UK subsidiary allegedly paid roughly US$1.1 million in bribes to Brazilian officials through the use of third-party agents. In June 2021, Foster Wheeler agreed to pay over US$43 million to resolve charges brought by anti-corruption authorities in the United States, Brazil, and the United Kingdom.

13 See FCPA Resource Guide at 60–61.

14 *id.*; see also Int'l Chamber of Com., ICC Anti-Corruption Third Party Due Diligence: A Guide for Small and Medium Size Enterprises, at 14–21, https://iccwbo.org/content/uploads/sites/3/2015/07/ICC-Anti-corruption-Third-Party-Due-Diligence-A-Guide-for-Small-and-Medium-sized-Enterprises.pdf (ICC Anti-Corruption Guide).

internal controls when contracting with a public sector entity, but those controls are only initiated if the entity is identified properly as public sector. If the individuals entering the information are unaware of the proper designation because no diligence is conducted, then the mechanisms to mitigate the risk of liability are not utilised. Similarly, when engaging third-party suppliers or other agents, it is critical to conduct sufficient due diligence to understand the third party's experience, beneficial owners and reputation. These efforts often take the form of risk management programmes and analysis designed to understand multiple aspects, including the entity's reputation for corrupt practices and whether the entity is designated on any sanctions lists.

Ultimately, the results of this analysis will help companies better understand, assess, and mitigate any risk that may arise throughout the course of the contractual relationship. For example, due diligence efforts could help uncover whether a third party has any familial or business connections to government officials or whether the third party is a politically exposed person. Similarly, due diligence may identify a financial institution as a publicly funded bank, thus triggering internal compliance safeguards. Uncovering these red flags early in the engagement can help inform further business dealings and save the company from future liability.

Eliminating all potential corruption risks that a third party could pose is neither possible nor required. For example, many companies distribute their product through a network of thousands of distributors and resellers, rely on dozens of manufacturers of component parts, employ consultants to provide market-relevant information, hire tax and legal advisers, use consultants with specialised technical skills, and outsource a host of other functions. Not all of these third parties present the same level and type of risk. Resources – both time and money – are limited, so vetting them all to the same degree is unrealistic. It is vitally important that any company considering its due diligence obligations intelligently allocates its resources to maximise the overall risk of those investments.

Risk-tiered due diligence helps companies focus their finite resources on those parties that present the most significant risks to the company. The extent of corruption risks varies from one third party to another, so the proportionality of the due diligence efforts applied also vary. This type of due diligence not only helps to prioritise risk monitoring, but also demonstrates that the company is taking an active and committed role to detecting and preventing corrupt practices should an investigation arise.

Risk-tiered due diligence factors to consider

Allocating risks among various third parties can often be difficult to establish and is not subject to a one-size-fits-all approach. However, there are certain factors that a company should consider when determining a third party's risk level.[15]

Interactions with government entities or public officials

Situations where the third party is either a government entity itself or works closely with a public official will give rise to increased anti-corruption enforcement scrutiny. Companies should note that a mere association with a foreign public official could lead to scrutiny and warrants heightened due diligence and internal controls around the third party's activities. While most countries impose criminal liability for all forms of bribery in a commercial context and not just bribes to public officials, the vast majority of the corruption enforcement actions that impose significant financial and business consequences involve public sector contracts. Accordingly, it is critical to understand whether a third party supplier is beneficially owned or controlled by a current or former government official or his or her close family members, and if so, to monitor closely the performance of services by that entity should the company engage it.

In September 2022, the second largest airline in Brazil, GOL Linheas Aereas Inteligentes S.A. (GOL) was charged with paying millions of dollars in bribes to Brazilian government officials allegedly in exchange for the passage of legislation that benefitted the airline. Some of the alleged payments purportedly were funnelled through fake consulting agreements with an intermediary that maintained close ties with one of the implicated Brazilian officials. In the deferred prosecution agreement (DPA) entered into with DOJ, GOL agreed to improve its controls around third-party relationships, including updated due diligence, training, auditing, and annual compliance certification controls to support ongoing monitoring of third-party relationships.[16] As another example of the importance of vetting an intermediary's ties to government officials, the

15 See FCPA Resource Guide at 60–62; OECD, OECD Due Diligence Guidance for Responsible Business Conduct (2018) (OECD Due Diligence Guide); ICC Anti-Corruption Guide, supra note 15, at 8–12.

16 See Deferred Prosecution Agreement, *United States v. Gol Linhas Aereas Inteligents S.A.S. v. GOL*, No. 22-cr-325-PJM (D. Md. 15 September 2022), https://www.justice.gov/criminal-fraud/file/1535366/download; see also Press Release, Dep't of Justice, GOL Linhas Aéreas Inteligentes S.A. Will Pay over $41 Million in Resolution of Foreign Bribery Investigations in the United States and Brazil (15 September 2022), https://www.justice.gov/opa/pr/gol-linhas-reas-inteligentes-sa-will-pay-over-41-million-resolution-foreign-bribery.

SEC's December 2022 order with Swiss-based ABB Ltd (ABB) described that, in exchange for the award of a large construction contract in South Africa, ABB executives allegedly colluded with a high-ranking government official at a state-owned electricity company to funnel US$37 million through third-party service providers with whom the government official had close personal relationships. ABB paid US$460 million to settle the related charges.[17]

Third parties engaged to interact with government officials must be subject to increased diligence and monitoring throughout the life of the contract to deter and detect potential illicit conduct. Additionally, interactions with customers beneficially owned or controlled by government entities merit enhanced scrutiny and the imposition of internal controls to mitigate risk as the liability exposure is not limited to charges of corruption, but may involve public procurement fraud or bid-rigging and misuse of taxpayer funds.

The jurisdiction

Where the third party is located and where the services are to be performed can help a company determine the level of potential risk that a third party might pose and thus, the commensurate level of due diligence required. The Corruption Perceptions Index published by Transparency International ranks the corruption levels of various countries, ranging from 'highly corrupt' to 'very clean.'[18] If the country where the third party is primarily working or in which the transaction occurs ranks as highly corrupt, then the level of due diligence applied to that third party or to that transaction should be consistent with the heightened risk presented. Moreover, if the jurisdiction is one with strong enforcement of anti-corruption laws, a company would be well advised to invest more resources in scrutinising its business dealings. A decade ago, many companies accepted excuses from third parties or customers reluctant to participate in due diligence who pointed to the differences in business customs across jurisdictions. Today, with a greater focus on the deleterious consequences of unchecked corruption,

17 See *In the matter of ABB Ltd.*, Securities Act Release No. 96444, Sec. and Exch. Comm'n (3 December 2022), https://www.sec.gov/litigation/admin/2022/34-96444.pdf; see also Press Release, Sec. and Exch. Comm'n, ABB Settles SEC Charges that It Engaged in Bribery Scheme in South Africa (3 December 2022), https://www.sec.gov/news/press-release/2022-214; Deferred Prosecution Agreement, *United States of America v. ABB LTD.*, No. 22-cr-0220-MSN (E.D. Va. 22 December 2022), https://www.justice.gov/opa/press-release/file/1556131/download (ABB DPA).

18 Transparency Int'l, Corruption Perceptions Index (2022), https://www.transparency.org/en/cpi/2022.

many countries across the world, and particularly in Latin America, are engaged in enforcement measures to reduce fraudulent and corrupt practices, thus reducing the reliability of a 'customs' excuse.

The nature of the services that the third party will provide

Some services may be more susceptible to corruption risks than others. For example, agreements where a third party is to provide a service to a public official that may be compensated through commission or success fee arrangements create more of a risk than agreements in which the third party supplies the company with printer cartridges whose pricing is more transparent. While the latter may present conflict of interest or kickback concerns if the supplier is related to the person who awarded the contract, such contracts typically do not result in large-scale investigations that distract personnel and divert resources for months. To help mitigate potential risks, companies should ensure that the scope of the services expected is clearly defined, the fees and expenses are delineated and supported by documentation, and the third party is sufficiently aware of the conduct in which he or she cannot engage.

Third-party compensation and the value of the contract

Companies should consider compensation and the overall value of the contract when allocating risk. Compensation may raise a red flag if it is disproportionate to the typical compensation received for similar services. Higher-than-normal compensation may suggest that excess payments will be used for bribes or kick-backs. As part of due diligence, companies often examine the fair market value of a transaction to evaluate whether the supplier has experience pricing similar contracts, is padding the cost to allow for improper payments, or is offering an unfair rate. Similarly, in contracts with a customer, companies examine the request for proposal or any tender documentation to substantiate discount requests or the need for third-party sales or services intermediaries. For example, sales agents often request non-standard discounts on the basis of a customer's budgetary restrictions or competitive pressures. To the extent the company has access to requests for proposal or other tender documentation, the due diligence process should include reviewing such documents to verify the veracity of the discount requests. Such documents, for example, may indicate that a tender is sole source, rendering a competitive pressure excuse invalid.

The overall value of the contract also could lead to potential risks. Higher valued contracts may tempt a third party to engage in corrupt conduct to obtain the benefits provided in the agreement. Similarly, a transaction with a percentage of the final sale as the commission payment may afford the supplier with

significant funds to make improper payments, absent heightened scrutiny of the supplier's experience, reputation, and compliance standards. Accordingly, higher-value contracts should be subject to greater internal controls and diligence to mitigate such risks. The ABB settlement discussed above illustrates this particular risk. According to the ABB DPA, certain ABB managers overrode due diligence controls, including ignoring red flags raised by ABB compliance personnel, to obtain subcontractor approval for the third parties who later funnelled payments to a South African government official allegedly in exchange for a contract worth US$160 million.[19]

The company's pre-existing relationship with the third party

A company's long-standing experience or pre-existing relationship with a third party may mitigate the risk of impropriety or it may make a company complacent. Certainly, the presence of an existing business relationship presents relevant information about the entity's experience and reputation, but if heightened risk factors are present in the transaction, companies would be well served to conduct some measure of due diligence to identify red flags and to mitigate risks should they arise. Companies also should monitor the third party throughout the life of the contract to ensure continued compliance. A long-standing relationship may make the supplier overly dependent on its business with the company such that it could be compromised by improper requests from a company sales manager, for example. Effective diligence and monitoring protects both parties in the transaction.

General due diligence factors to consider

While the level and severity of due diligence can vary, companies should seek certain background information on the following topics when conducting due diligence analysis.[20]

Beneficial ownership

Companies must know the actual identity of those with whom they are contracting. Companies should identify the third party's principal shareholders to determine who has actual control and ownership of the business. This information can be established through the third party's official company registration

19 See ABB DPA.

20 FCPA Resource Guide at 60–62; ICC Anti-Corruption Guide, supra note 14, at 14–21; OECD Due Diligence Guide, supra note 15.

documents, but, in many cases, should not be limited to a review of the incorporation certificates. For example, someone seeking to disguise the true beneficial owners may list family members or individuals whose business is to incorporate entities under local law. Accordingly, requiring potential third parties to complete a due diligence questionnaire identifying their beneficial owners is a better practice than relying simply on company registration documents. Understanding the true ownership structure will help companies avoid liability for the misconduct of hidden owners, which has recently become an area of focus in the United States.[21]

Financial background

Asking third parties to submit financial reports or statements is critical to understanding the financial health of the third party, not simply for creditworthiness purposes, but also for exposure to legal risk. Financial reports can alert the company to those entities who may be compromised or unduly influenced by improper overtures to secure business. Additionally, financial reports often reflect whether the entity maintains its books and records in a manner that provides transparency and reliability – a key factor in anti-corruption analyses and one that can create liability or serve as a useful monitoring tool. Companies should endeavour to ensure that the information in the disclosed financial reports is

21 The US has designated the fight against corruption as a 'core national security interest' and has increasingly focused on the need for transparency in financial transactions and effective third-party due diligence as a means to reduce the risk of corruption both domestically and abroad. See Joseph Biden, Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest, White House Briefing Room (3 June 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/memorandum-on-establishing-the-fight-against-corruption-as-a-core-united-states-national-security-interest. Under the Corporate Transparency Act (CTA) enacted by Congress in January 2021, certain entities will be required to report beneficial ownership information to the Financial Crime Enforcement Network. See Corporate Transparency Act, H.R. 6395 § 6403. One of the goals of the CTA is to thwart companies from concealing their ownership to 'facilitate illicit activity.' Id. § 6402(3). On 30 September, the Financial Crime Enforcement Network (FinCEN) issued a final rule requiring companies created or doing business in the US to disclose to FinCEN 'any individuals who, directly or indirectly, either exercise substantial control over a Reporting Company or who own or control at least 25% of the ownership interests of such company.' FinCEN defines 'substantial control' as one who: (1) serves as a senior officer of a Reporting Company, (2) has authority over the appointment or removal of any senior officer or a majority or dominant majority of the board of directors (or similar body) of a Reporting Company, and (3) those who direct, determine, or decide, or exercise substantial influence over, important matters affecting a Reporting Company. See Beneficial Ownership Information Reporting Requirements, 87 Fed. Reg. 59498 (proposed 30 September 2022) (to be codified at 31 C.F.R. pt. 1010).

accurate and detailed enough to allow the company to spot discrepancies or unusual payments. Moreover, the financial reports or statements may offer insight as to whether the third party is sufficiently experienced and reputable to perform the services anticipated for the company and can serve to verify the third party's declarations of prior experience in the industry. Depending on the significance and risk of the third party's activities on behalf of the company, the company's diligence may include researching, and, if possible, independently verifying the third party's financial activities to evaluate the potential sources of revenue. This independent corroboration would help guard against potential negative media narratives that unnecessarily could imperil the company's good will and reputation if, for example, the third party's revenue partially derives from criminal activities.

Third-party competency

Companies must be on alert for red flags that indicate a third party has offered to provide services in an area where it seems to lack competence. This is especially true when the services offered involve interactions with government officials. Companies should ensure the third party has the actual expertise and experience required by checking references, researching the third party's history, probing the third party's knowledge of the industry and market, and examining the third party's website for details that substantiate its declarations of experience. To avoid actual or perceived corrupt conduct, a company also should ensure that it has a legitimate business justification for entering into the agreement with the third party. A proper business justification will help mitigate the company's potential risk in the future, provided there is no readily available information which the company failed to evaluate or collect that discredits the third party's competency. The perceived lack of competency in a third-party was one of the key facts in Rio Tinto plc's (Rio Tinto) settlement with the SEC.[22] The company hired a consultant and close associate of a senior Guinean government official to help retain its mining rights in Guinea. The consultant purportedly had no direct work experience related to the mining business or Guinea specifically. The consultant was paid US$10.5 million for his services, despite red flags suggesting the consultant was providing advice to the government official and that some

22 Press Release, Sec. and Exch. Comm'n, SEC Charges Rio Tinto plc with Bribery Controls Failures (6 March 2023), https://www.sec.gov/news/press-release/2023-46.

portion of the consultant's fees allegedly would be shared with the government official. As part of the settlement, Rio Tinto agreed to pay a fine of US$15 million to the SEC.

Research the third party's history

Another measure to assess potential risks is to run an internet search to identify any available reputational information regarding the third party. Adverse news alleging that the third party or its officers, directors or employees have engaged in corrupt, fraudulent or unethical practices in the past is a clear red flag that the company should consider before entering into further business dealings. Such adverse news also may offer insight on the third party's competency. The company can conduct this research using the information provided by the third party itself or from information located in the public domain and behind relatively minor paywalls. In certain markets, this information may not be as readily available or reliable as in other jurisdictions, but, depending on the risk presented by the third party's anticipated activities, may be worth the effort to uncover. For example, a sales intermediary responsible for negotiating with potential public sector customers in Honduras should be subject to greater due diligence scrutiny than a manufacturing supplier of component parts in Chile.

The third party's reputation

A third party's reputation often can be discerned through researching its history and any adverse news through internet searches. But in higher-risk cases, due diligence efforts also should involve other means. For example, companies should seek out references who personally know or have worked with the third party in question and can speak towards the party's character, experience and past engagements. This can help establish whether the third party has engaged in corrupt practices in the past, has a propensity for behaviour that skirts the law or has a close relationship with a public official that may raise a red flag.

The third party's approach to ethics and compliance

Lastly, companies should examine the ethics and compliance policies that the third party has in place for its own business. The third party's overall tone and attitude towards compliance efforts should be noted as potential risk factors. This analysis includes inquiring whether the third party engages in its own due diligence of business partners, suppliers, contractors, and, in particular, any sub-contractors it may use in connection with the work to be performed for the company. Moreover, in many cases, this analysis includes understanding the financial and other controls in place by the third party to mitigate risks of misconduct and to monitor its employees' and agents' compliance. Additionally, with respect

to customers, this inquiry may inform whether the company has an obligation to complete certain compliance certifications or to advise the customer of certain benefits offered or provided to its personnel in connection with the negotiation or performance of the contract. For example, certain public sector entities prohibit their employees from engaging in any events or accepting any benefits, even if nominal, absent pre-approval; understanding whether such prohibitions exist is critical to ensuring the success of the customer relationship and to mitigating liability for failure to abide by these requirements.

In recent years, more Latin American countries have enhanced and enforced anti-corruption laws. Anticorruption legislation in most countries emphasises the importance of corporate compliance programmes and imposes liability when companies fail to adopt adequate internal controls, including policies, procedures and monitoring mechanisms that cover their employees and agents.[23] Accordingly, entering into a contract with an entity that has failed to adopt internal controls consistent with its risk profile and the applicable legal requirements is a key factor to consider in due diligence.

Continued monitoring

Due diligence efforts do not cease once the third party has been officially retained. Companies should continue to monitor the third party's conduct throughout the business relationship to identify and follow up on potential red flags. This may include updating due diligence practices, providing additional training, periodically auditing the third party's practices and compliance protocols, and requesting updated compliance certifications.[24]

Due diligence does more than just mitigate potential risk, however. A robust and effective programme promotes ethical conduct among the various parties to an agreement. For example, conducting third-party due diligence may require that the third party itself examine and redefine its own compliance and anti-corruption efforts to avoid risk and to better position itself to build future business relationships. Thus, taking the time to expand due diligence efforts that encompass all third-party relationships will be beneficial for both parties to the transaction.

23 See, e.g., L. 1778, 2 February 2016, Diario Oficial [D.O.] (Colom.); Brazil Clean Company Act (Law No. 12.846/2013); Law No. 20.393, 2 December 2009, Gaceta Jurídica, G.J. (Chile).

24 FCPA Resource Guide.

Approaching due diligence when negotiating and dealing with counterparties

Contracts with third-party suppliers or clients should clearly state the responsibilities of all of the parties and their compliance expectations. These contracts should reference the company's due diligence efforts to ensure that the third party abides by all applicable anti-corruption laws. Third parties should be aware of the types of risks that would give rise to enforcement scrutiny so as to help mitigate the company's potential liability should corrupt conduct occur. In most cases, the following representations and warranties should be included in the contract:

- agrees to comply with all applicable laws and policies and certifies compliance for at least the prior five years;
- certifies that no actions have been proposed or taken, directly or indirectly, that would cause a government official to benefit improperly;
- agrees to adopt (or certifies adoption of) adequate and effective compliance policies and internal controls, which include training on those policies and controls to employees;
- agrees to provide prompt notice to the company if it plans to retain other agents or representatives to assist in providing services under the contract;
- agrees to provide immediate notice to the company if it becomes aware of an allegation of a potential or actual violation of law;
- certifies that it maintains accurate, detailed, transparent, and up-to-date books and records setting forth the financial transactions related to any work conducted on behalf of the company, together with supporting documentation;
- agrees to allow the company to audit its books and records related to the contract; and
- permits the company to terminate rights under the contract in the event of a compliance breach, including a provision requiring the third party to forfeit any compensation agreed upon in the contract.

Means of mitigating potential exposure

Red flags that arise from due diligence efforts do not automatically mean that a company cannot contract with a third party. Certain risks can be mitigated to limit potential exposure.

Training third parties

Before contracting, companies should ensure that the third party is aware of the relevant anti-corruption, sanctions and other laws that affect the transaction and that it is aware of its customer's policies and practices to ensure compliance with applicable laws. One method of ensuring adequate knowledge of the applicable

laws and compliance policies is through substantive training. When investigating alleged misconduct, regulators around the world consider a company's efforts to communicate its policies effectively through trainings and certifications.[25] An effective training process takes into account the target audience.[26] For example, the information and hypotheticals should revolve around situations that the third party would likely encounter, and training materials should be provided in the local language, if applicable. The more targeted and thorough the training, the more likely a company can mitigate potential liability risks should they arise.

Implementing a third-party code of conduct

All companies should implement a general code of conduct as a foundation for their overall compliance programmes. These codes should be clear and concise, and companies should ensure that they are made available to all employees and third-party agents working on behalf of the company. This includes providing the material in the local language, if necessary. Effective codes of conduct outline the company's policies and procedures, as well as the expectations the company has in terms of compliance. When investigating alleged misconduct and imposing liability, regulators consider the effectiveness of a company's code of conduct and whether the company has provided the code to its third parties and updated the code to account for current risks.

Enforcing contractual audit clauses

As stated above, companies should ensure that they include a contractual provision requiring compliance with applicable laws. However, merely stating that a third party must follow the applicable laws is not enough to fully mitigate the risks. Companies bear the responsibility to continue monitoring third parties throughout the life of the contract to better detect any potential issues that might arise. This can be done by periodic audits of the third party's activities and invoices, as well as audits of the third party's own compliance policies as they relate to its business with the company. In the context of a contract with a customer, the company can review the request for proposal, any tender documents, and the deal booking documents to ensure that applicable laws are being satisfied. This continued monitoring, like due diligence, is tiered based on the risks presented by the third party; a majority of third-party relationships will not necessitate regular monitoring.

---

25 See *id.* at 60-61.

26 *id.*

The case of the online gaming and sports betting company Flutter Entertainment plc's (Flutter) illustrates the consequences of failing to enforce the anti-bribery and anti-corruption clauses. Flutter's predecessor-in-interest, the Stars Group, Inc. (Stars Group), acquired the Oldford Group Ltd. (Oldford Group) in 2014 and inherited Russia-based consultants responsible for promoting the legalization of poker in Russia. However, the consultants allegedly did not receive initial due diligence or maintain written contracts with the Stars Group until 2017. But, even after these contracts were in place with anti-bribery and anti-corruption provisions, Stars Group allegedly failed to enforce such provisions. For instance, consultants purportedly submitted invoices that contained vague and general statements without supporting documentation. Similarly, consultants often were reimbursed for expenses through third-party non-profit organisations without the proper supporting evidence. Flutter agreed to pay the SEC a fine of US$4 million for failing to maintain accurate books and records and internal controls.[27]

Using data analytics and artificial intelligence[28]

Enforcement agencies increasingly focus on data analytics when evaluating corporate compliance programmes. The March 2023 revision to the DOJ compliance guidelines requires prosecutors to investigate how a company is tracking the functionality of its operations and compliance efforts.[29] Part of this determination is done by looking at the company's use of data analytics. Data analytics allows a company to continuously and remotely gather data, monitor transactions and analyse risks. It provides the company with a method of analysing the effectiveness of its policies and controls to better address new concerns. This type of monitoring helps to identify risks as they emerge for compliance, auditing and investigation purposes, giving the company more time to evaluate and determine the best course of action to mitigate liability.[30]

---

27 See *In the matter of Flutter Entertainment plc, as successor-in-interest to The Stars Group, Inc.*, Securities Act Release No. 4384, Sec. and Exch. Comm'n (6 March 2023), https://www.sec.gov/litigation/admin/2023/34-97044.pdf .

28 See Chapter 11, 'Why Fresh Perspectives on Tech Solutions are Key to Evolving Data-Driven Compliance Monitoring' by Gabriela Paredes, Dheeraj Thimmaiah, Jaime Muñoz and John Sardar.

29 Dep't of Justice, Evaluation of Corporate Compliance Programs at 2–3 (Updated March 2023), https://www.justice.gov/criminal-fraud/page/file/937501/download.

30 See footnote 28.

Finding patterns of improper behaviour by third parties is increasingly complex; companies can benefit from leveraging artificial intelligence (AI) and machine learning solutions. AI can help companies to identify relevant documents, as well as corruption-related patterns, especially when dealing with large volumes of data. For example, in 2020, Microsoft partnered with the Inter-American Development Bank to advance anti-corruption, transparency, and integrity objectives across Latin America and the Caribbean through its ACTS (Anti-Corruption Technology and Solutions) initiative, which is founded on the company's cloud computing, data visualisation, AI and machine learning investments.[31]

Conclusion

The use of third parties is both beneficial and necessary for most companies. Maximising the utility of such relationships, however, requires a deliberate and focused approach to due diligence to mitigate the inherent risks. Companies should take the necessary steps to identify potential risk factors before entering into a business relationship but need not terminate a relationship if risks arise. Implementing a robust and effective compliance programme that incorporates risk-tiered due diligence efforts will help mitigate the compliance risks and allow the companies to retain the benefit of third-party services.

31 Dev Stahlkopf, Microsoft launches Anti-Corruption Technology and Solutions (ACTS), Microsoft Blog (9 December 2020), https://blogs.microsoft.com/on-the-issues/2020/12/09/microsoft-anti-corruption-technology-solutions-acts/.

CHAPTER 8

How to Build Effective Internal Communication Channels

María González Calvet, Krystal Vazquez and Baldemar Gonzalez[1]

Managing multinational workforces in an age of anti-corruption 'accretion'

Managing risk within multinational, matrixed organisations is no simple feat. The complexities that accompany risk management have only been compounded as US regulators have unveiled several pieces of policy and renewed guidance for corporate compliance programmes in early 2023 alone.

Entities that face particular challenges amid these developments include, for example, those that employ nearly 100,000 employees worldwide and that generate significant revenue through production or sales in high-risk jurisdictions that are divided into several business segments. Often, such organisations are supported by global or regional compliance professionals tasked with navigating multiple jurisdictional demands in diverse areas of risk, including anti-bribery programming, employee onboarding and training, third-party due diligence and sanctions.

Building effective communication channels to advance global initiatives to workforces across the globe requires balancing both compliance and commercial priorities. To manage this balance effectively, a compliance programme must deploy a variety of techniques to support multinational workforces while ensuring the compliance programme is oriented to actual business risk and the enforcement landscape.

---

1 María González Calvet is a partner, and Krystal Vazquez and Baldemar Gonzalez are associates, at Ropes & Gray.

After receiving its mandate from the Biden administration to 'fight' against corruption as a core national security interest,[2] the US Department of Justice (DOJ) has been committed to turning anti-corruption principles into policies in rapid succession in late 2022 and early 2023. The cascade of policy announcements surrounding anti-corruption efforts and tools to combat corporate crime more broadly have dramatically altered the enforcement landscape.

In New York in September 2022, Deputy Attorney General Lisa O Monaco (DAG Monaco or Monaco) announced policies to incentivise responsible corporate citizenship before an audience that included the Director of the Securities and Exchange Commission's (SEC) Enforcement Division, Gurbir Grewal.[3]

In Washington, DC in January 2023, Assistant Attorney General for the DOJ's Criminal Division, Kenneth A Polite, Jr (AAG Polite or Polite) unveiled the first significant changes to the Corporate Enforcement Policy (CEP) since 2017.[4] The amendments to the CEP provide a renewed framework by which the DOJ will reward companies that self-disclose misconduct, cooperate and remediate by offering increased reductions off applicable US Sentencing Guidelines ranges.[5] And for all US Attorney's Offices (USAOs) across the country, the DOJ announced a corporate Voluntary Self-Disclosure Policy (VSD Policy) in February 2023, setting nationwide incentives for voluntary corporate disclosures.[6]

---

2 In June 2021, the Biden Administration issued a memorandum highlighting the cost of corruption and declaring the fight against corruption to be a core national security interest. See The White House, Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest (3 June 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/memorandum-on-establishing-the-fight-against-corruption-as-a-core-united-states-national-security-interest.

3 See DOJ Unveils New Policies to Incentivize Responsible Corporate Citizenship and Deter Wrongdoing, Ropes & Gray LLP (16 September 2022), https://www.ropesgray.com/en/newsroom/alerts/2022/september/doj-unveils-new-policies-to-incentivize-responsible-corporate-citizenship-and-deter-wrongdoing.

4 See Ryan Rohlfsen et al., DOJ Unveils Changes to the Criminal Division's Corporate Enforcement Policy to Incentivize Voluntary Self-Disclosure and Cooperation, Ropes & Gray LLP (20 January 2023), https://www.ropesgray.com/en/newsroom/alerts/2023/01/doj-unveils-changes-to-the-criminal-divisions-corporate-enforcement-policy-to-incentivize-voluntary.

5 *id.*

6 DOJ Launches Formal Voluntary Self-Disclosure Policy for All U.S. Attorney Offices, Ropes & Gray LLP (27 February 2023), https://www.ropesgray.com/en/newsroom/alerts/2023/02/doj-launches-formal-voluntary-self-disclosure-policy-for-all-us-attorney-offices#:~:text=On%20February%2022%2C%202023%2C%20the,incentives%20for%20voluntary%20corporate%20disclosures.

In Miami in March 2023, Monaco and Polite took the stage yet again at the 38th American Bar Association's National Institute on White Collar Crime (ABA Conference) to provide greater colour on the DOJ's sweeping policy changes. In her remarks, Monaco explained that the VSD Policy had been implemented nationwide to eliminate geographic disparities and ensure a 'predictable', 'consistent' and 'transparent' approach to enforcement.[7] And Polite's keynote only amplified Monaco's message, underscoring the importance of 'marshal[ing] a variety of tools to creatively address the challenges before us'.[8]

For companies that operate across the Americas and the globe, those challenges often loom large. From the small-town hospital administrator who demands bribes in exchange for life-saving services to the globe-trotting kleptocrat who offshores an embezzled fortune to terrorist groups that accept millions in exchange for greenlighting company operations at a facility in Syria – recent remarks, policy announcements and enforcement actions are highly attuned to the cadence of corruption in the United States and abroad.

DOJ's policy announcements and remarks at the ABA Conference signal a renewed commitment to coordinating with other governments to combat corruption. Polite's spotlight on Venezuela, for example, exemplifies collaboration among the Foreign Corrupt Practices Act (FCPA) Unit, the USAO in the Southern District of Florida, the Criminal Division's Office of International Affairs (OIA) and the Policía Nacional (Spanish National Police) in the successful prosecution of Claudia Patricia Diaz Guillen, the former National Treasurer of Venezuela and resident of Spain, who accepted over US$100 million in bribes from a Venezuelan billionaire.[9] Against the backdrop of 96 per cent of Venezuelans living in poverty, DOJ considers this collaboration as the type of 'righteous' case the agency will continue to pursue.[10]

---

7 Justice Department Announces New Policies Impacting Corporate Criminal Enforcement, Ropes & Gray LLP (7 March 2023), https://www.ropesgray.com/en/newsroom/alerts/2023/03/justice-department-announces-new-policies-impacting-corporate-criminal-enforcement.

8 US DOJ, Assistant Attorney General Kenneth A. Polite, Jr. Delivers Keynote at the ABA's 38th Annual National Institute on White Collar Crime (3 March 2023), https://www.justice.gov/opa/speech/assistant-attorney-general-kenneth-polite-jr-delivers-keynote-aba-s-38th-annual-national [ABA Conference Polite Remarks].

9 US Embassy in Venezuela, Former Venezuelan National Treasurer Charged in Connection with Bribery and Money Laundering Scheme (16 December 2020), https://ve.usembassy.gov/former-venezuelan-national-treasurer-and-her-spouse-charged-in-connection-with-international-bribery-and-money-laundering-scheme/.

10 *id.*

The tone from the very top, from the highest levels of the US government itself, is reverberating with a resounding call for collaboration, creativity and claw-backs, where warranted, to achieve its commitment to combat corporate crime.

As the US government reinforces its already robust system of accountability, multinational compliance programmes must expect that they will be held to account for doing the same with their workforces. Compliance professionals will therefore need to answer the call to action this represents and work even more effectively at managing, communicating and amplifying anti-corruption efforts along with their sanctions framework, as applicable, particularly as the threat of enforcement looms.[11]

However, those who build effective internal communication channels and adapt their compliance programmes will be well positioned.

Building effective internal communication channels

One key element of corporate governance is a well-designed and well-implemented compliance programme. However, even the best programme will falter absent effective channels to diffuse the principles of an organisation's 'culture of compliance'– the norms that encourage ethical conduct and a commitment to compliance with the law. Effective internal communication facilitates smooth information flow and shapes the way employees engage with an organisation, including how employees perceive its mission and values and how they relate to its culture.

A company conveys sound communication practices through the following:

- setting the tone beyond just the top to include the entire organisation;
- delegating compliance oversight and enforcement to a dedicated function;
- implementing and publicising compliance policies, procedures and practices;
- enforcing its policies, procedures and practices;
- operating a well-functioning confidential reporting mechanism;
- collecting and analysing compliance metrics; and
- establishing training initiatives that are tailored and adapted to local laws and customs.

11 See ABA Conference Polite Remarks ('That is what I urge you all to do as well. Not just fellow prosecutors, but defense counsel, in-house professionals – use your mission to solve problems you see. Act in a way that is meaningful, sets the right tone, and leads by example.').

No one size fits all when it comes to the channels used to communicate corporate compliance. This chapter discusses general best practices across industries, but they should be individually tailored to each company's operational realities.

Tone throughout: communicating a commitment to compliance culture

Effective internal communication is multidirectional: top-down and bottom-up. Organisations comprise individual executives and employees who each should feel personally invested in ensuring and promoting compliance.[12] Consistent with this principle, regulators evaluate a company's commitment to fostering a strong culture of compliance at all levels of the company – not merely within its compliance department.[13]

Senior leadership sets the tone for the rest of the organisation. The commitment to compliance is manifested by the extent to which senior leadership articulates the company's ethical standards, conveys and disseminates those standards in clear and unambiguous terms and demonstrates rigorous adherence by example.[14] In its revised March 2023 guidance on the Evaluation of Corporate Compliance Programs (ECCP), DOJ recognised that the tone at the top must be further bolstered by the tone at the middle and beyond, which drives the compliance programme on a daily basis and invests subordinates with a sense of ethical responsibility.[15] Most employees, especially at larger organisations, have little direct contact with senior leadership and therefore are most influenced by the managers who supervise them on a regular basis.

---

12 See US DOJ, Principal Associate Deputy Attorney General Marshall Miller Delivers Live Keynote Address at Global Investigations Review (20 September 2022), https://www.justice.gov/opa/speech/principal-associate-deputy-attorney-general-marshall-miller-delivers-live-keynote-address [GIR Miller Remarks].

13 US DOJ, Memorandum from the Deputy Att'y Gen., Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group (15 September 2022), https://www.justice.gov/opa/speech/file/1535301/download [Monaco Memo].

14 See US DOJ, Crim. Div., Evaluation of Corporate Compliance Programs 9 (March 2023), https://www.justice.gov/criminal-fraud/page/file/937501/download [US DOJ ECCP]; World Bank Group, Integrity Compliance Guidelines 5 (2017), https://wallensteinlawgroup.com/wp-content/uploads/2017/12/WBG-Integrity-Compliance-Guidelines-full.pdf [World Bank Guidelines].

15 See US DOJ ECCP, at 9 ('Prosecutors should also examine how middle management, in turn, have reinforced those standards and encouraged employees to abide by them.'); US DOJ & SEC, FCPA: A Resource Guide to the U.S. Foreign Corrupt Practices Act 58 (2d ed. 2020), https://www.justice.gov/criminal-fraud/file/1292051/download [FCPA Resource Guide].

Who owns this? Assigning compliance oversight

Another hallmark of commitment to ethical practices is designating a dedicated function to implement and enforce compliance initiatives. The delegation of this core mandate should account for an organisation's size and structure and need not be a compliance officer or in-house personnel. Whichever option best complements the size and structure of an organisation, the compliance function should be independent from management and be resourced adequately in terms of budget, human capital and information technology (IT).[16]

In assessing an organisation's compliance programme, regulators ask not only whether compliance officers have 'adequate access to and engagement with' the business, management and board of directors but also whether an organisation has taken steps 'to ensure that compliance has adequate stature within the company and is promoted as a resource'.[17] US regulators are further scrutinising the qualifications and expertise of key compliance personnel, signalling a preference for chief compliance personnel to lead any presentation with regulators and to demonstrate knowledge and ownership of a company's compliance programme.[18] The overarching goal is to maintain a compliance function that is not merely a 'paper programme' but one that is well designed and equipped to handle an organisation's operational demands.[19]

Compliance policies, procedures and practices

An organisation's policies and procedures form the foundation upon which an effective compliance programme is built. These policies set forth ethical expectations, outline disciplinary procedures and, more broadly, incorporate the culture of compliance into the organisation's day-to-day operations.[20]

But policies are meaningful only if personnel know about them. Before doling out disciplinary action, for example, a company must first communicate clearly what constitutes a breach of internal policies, procedures and values and how the company will respond to such a breach. If a breach is corroborated

16 See US DOJ ECCP, at 10. Dep't of the Treasury's Office of Foreign Assets Control, A Framework for OFAC Compliance Commitments 2 (May 2019), https://home.treasury.gov/system/fi1es/126/framework_ofac_cc.pdf [OFAC Framework].

17 US DOJ, Assistant Attorney General Kenneth A. Polite Jr. Delivers Remarks at NYU Law's Program on Corporate Compliance and Enforcement (PCCE) (25 March 2022), https://www.justice.gov/opa/speech/assistant-attorney-general-kenneth-polite-jr-delivers-remarks-nyu-law-s-program-corporate [NYU PCCE Polite Remarks].

18 *id.*

19 See US DOJ ECCP, at 9.

20 See *id.*, at 4.

and repercussions are warranted, the company should issue disciplinary action promptly and consistently.[21] This communicates that misconduct will not be tolerated while also reinforcing fidelity to ethics and accountability.[22]

A company can ensure employees keep up to date with its policies by requiring periodic certification of compliance and introducing new employees to its ethical values during onboarding.[23] Relatedly, a company should inform business partners that it expects all activities carried out on its behalf to comport with internal ethics protocols and lawful business practices by seeking assurances from third parties, where appropriate, through certifications or contractual representations of reciprocal commitments.[24] These measures ensure that the compliance programme is visible, understood and followed appropriately by all relevant stakeholders. They also comport with regulators' expectation that a company implement policies that reflect the spectrum of risks posed by an evolving legal, regulatory and business landscape.[25]

Moreover, recent guidance from DOJ makes plain that prosecutors will be asked to consider 'the extent to which the company's communications convey to its employees that unethical conduct will not be tolerated and will bring swift consequences, regardless of the position or title of the employee who engages in the conduct'.[26] Compliance professionals should follow suit. Prosecutors will further be asked to consider 'whether a company has publicized disciplinary actions internally, where appropriate and possible, which can have valuable deterrent effects'.[27] Similarly, compliance professionals will need to weigh any benefits that might be gained in the publicisation of disciplinary actions for their own organisations.

---

21 See *id.*, at 6, 12–13 (adding that disciplinary action should be commensurate with the violations).

22 See *id.*, at 12–13. Some companies have even found that publicising disciplinary actions internally, where appropriate under local law, can have an important deterrent effect, warning that unethical actions have swift and sure consequences. See *id.*, at 12.

23 See OECD, Corporate Anti-Corruption Compliance Drivers, Mechanisms and Ideas for Change 39 (2020), https://www.oecd.org/corruption/Corporate-anti-corruption-compliance-drivers-mechanisms-and-ideas-for-change.pdf [OECD Compliance Drivers].

24 See World Bank Guidelines, at 10; FCPA Resource Guide, at 62.

25 See NYU PCCE Polite Remarks.

26 US DOJ ECCP, at 12; U.S.S.G. § 8B2.1(b)(6) ('[t]he organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct').

27 US DOJ ECCP, at 12.

Use of third-party messaging apps and mobile devices

The use of third-party messaging platforms (e.g., WhatsApp, WeChat) as well as ephemeral and encrypted messaging applications (e.g., Signal) for business communications increased substantially during the covid-19 pandemic due, in part, to limitations on in-person gatherings and remote work environments.[28] Although the global pandemic has waned, app-based messaging is here to stay. This is particularly true in Latin America, where WhatsApp is the most used social network in the region, with more than 94 per cent of internet users in selected countries accessing the platform.[29] And, as these messaging services continue to grow in popularity, regulators increasingly will expect companies to adapt their communication policies and practices to evolving technological realities.[30]

Though there may be legitimate reasons for the business use of these applications, they also present significant challenges for companies' ability to maintain effective internal communication channels. Such challenges include the ability to monitor the use of such devices for misconduct, diversity of retention requirements between industries and data privacy restrictions across jurisdictions. Companies operating in Latin America and elsewhere would thus benefit enormously from implementing centralised guidance on the use of third-party messaging applications to ensure that employees' business communications comport with relevant regulatory obligations and that they can be monitored and preserved, as necessary.

---

28 In one study, roughly eight in 10 people aged 25 to 34 stated that they use messaging platforms such as WhatsApp to communicate with their colleagues at least once per week. See Simon Kemp, Digital 2020: October Global Statshot DataReportal.com (20 October 2020), https://datareportal.com/reports/digital-2020-october-global-statshot. This trend existed even pre-pandemic. WeChat reported over 1.2 billion monthly active users in 2020, more than double the 550 million monthly active users it reported in 2015. See Lai Lin Thomala, Number of active WeChat messenger accounts Q2 2011–Q4 2020, Statista (7 December 2022), https://www.statista.com/statistics/255778/number-of-active-wechat-messenger-accounts. WhatsApp reported in 2020 that roughly 100 billion messages were exchanged each day on the platform, up from 30 billion messages in 2015. See L. Ceci, Number of monthly active WhatsApp users 2013-2020, Statista (27 July 2022), https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users.

29 See Tiago Bianchi, WhatsApp reach in selected Latin American countries 2021, Statista (1 August 2021) https://www.statista.com/statistics/1323702/whatsapp-penetration-latin-american-countries/.

30 See GIR Miller Remarks ('Company policies and procedures addressing the use of personal devices and third-party messaging systems for business purposes will be reviewed as part of evaluating the effectiveness of a corporation's compliance program.').

In March 2023, DOJ expounded on the significant changes introduced by DAG Monaco in a September 2022 memorandum addressing the use of communications platforms, messaging applications and mobile devices.[31] Under DOJ's revised ECCP guidance, regulators will not only ask about the electronic communication channels used by the business and their preservation settings, they will also consider how companies communicate the policies to employees and whether they enforce them on a consistent basis.[32] Regulators will inquire about the company's ability to access such communications, whether they are stored on corporate devices or servers, as well as the company's knowledge of applicable privacy and local laws. 'A company's answers – or lack of answers – may very well affect the offer it receives to resolve criminal liability'.[33]

US enforcement authorities are delivering on their recommendations and admonishments, leaving less ambiguity on their expectations for compliance with respect to communications management. In 2022, the SEC and the Commodity Futures Trading Commission collectively levied billions in fines against a number of major banks and other financial institutions for not retaining SMS texts, iMessage, and app-based communications (which the SEC deemed 'off-channel communications').[34] According to the SEC, employees routinely used off-channel communications to discuss business matters, thus impeding institutions' ability to archive business-related communications as required by securities laws.[35]

Even companies that historically have not had a legal duty to manage employees' communication platforms, such as those not regulated by securities laws, should take note of regulators' growing scrutiny of these communications

---

31 We are intentionally not referring to mobile devices as 'personal devices'. Given important legal and technical implications that apply to the different types of mobile devices, discipline should be employed when addressing this topic to note the differences between (1) corporate-issued mobile devices; (2) BYOD mobile devices; and (3) truly personal devices.

32 See US DOJ ECCP, at 17; ABA Conference Polite Remarks.

33 *id.*

34 In 2022, the SEC and the CFTC imposed fines totalling US$1.8 billion in penalties as part of a series of settlements with major financial institutions for failing to preserve off-channel communications by employees. Jon Hill, HSBC Says It's Close to Settling SEC, CFTC Texting Probes, Law360 (22 February 2023), https://www.law360.com/articles/1578980/hsbc-says-it-s-close-to-settling-sec-cftc-texting-probes. Those actions followed a US$200 million fine levied against JPMorgan Chase in late 2021 to settle similar record-keeping lapses tied to employees' messaging use. Id.

35 See Jon Hill, SEC, CFTC Messaging Probes Net $1.8B In Big Bank Penalties, Law360 (27 September 2022), https://www.law360.com/articles/1534585/sec-cftc-messaging-probes-net-1-8b-in-big-bank-penalties.

more widely.[36] As evidenced by the DOJ's articulated views, companies should proactively enhance their compliance programmes to better withstand any future scrutiny of their employees' communication channels. From the government's perspective, companies that currently have no legal requirement to preserve business-related communications are 'amply on notice' of the risks of failing to do so.[37]

Prosecutors' expectation that companies implement communications policies includes those policies that permit employees to use managed BYOD[38] devices rather than company-issued devices to access company information, known as bring-your-own-device, or BYOD, policies.[39] Many companies require work to be conducted on corporate devices; others permit the use of managed BYOD or unmanaged personal devices. A managed BYOD device is often allowed with clear limitations of use that are technologically enforced, in full or in part, by MDM or EMM.[40] They, like corporate-issued, might also have specialised apps or middleware that capture text and app-based communication content, allowing for preservation and monitoring for compliance reviews. An unmanaged personal device that is permitted for business communications will not have technological controls to assist in enforcing the company's communications policy. Such personal devices typically hold a complicated commingling of business and personal communications.

Companies may not be able to prevent every employee from using unauthorised messaging apps for business use, but they can take steps to demonstrate reasonable controls, including by maintaining a clear policy, ensuring retention capabilities, auditing employee use and incorporating information security best practices. In addition, companies should consider technological solutions to restrict employees' ability to instal unapproved apps on company-issued and managed BYOD devices and provide employee training to establish further awareness of and compliance with information security practices. For example,

---

36 See Jane Yoon & Mark Carper, Revisiting Employee Communication Policies After DOJ Memo, Law360 (13 October 2022), https://www.law360.com/articles/1538257/revisiting-employee-communication-policies-after-doj-memo.

37 *id.*

38 Here we make a distinction between a managed BYOD device from a truly personal and unmanaged device. A managed BYOD device will have some form of MDM (Mobile Device Management) or EMM (Enterprise Mobility Management), which serves to allow access to approved systems, can block the installation of unapproved systems and apps, and offers other security features. This is one reason it is important to refer to mobile devices more specifically as between corporate-issued, BYOD and personal.

39 See ABA Conference Polite Remarks.

40 See footnote 38.

some applications may delete messages as soon as they are read (i.e., ephemeral messaging) and some may automatically delete messages after a specified period unless default settings are changed by the user.[41] It is therefore critical that companies evaluate, in coordination with their local IT functions, the effect that various applications have on company data retention and information security goals.

However a company chooses to address the use of messaging platforms or mobile devices for business communications, it must strive to prevent circumvention of compliance protocols through off-system activity, preserve all key data and communications and maintain the capability to promptly produce that information for government investigations.[42]

Compliance through carrots and sticks

Good-faith enforcement of policies and expectations further communicates an organisation's culture of corporate compliance. Indeed, in analysing an organisation's commitment to corporate compliance, government authorities examine whether corporate management is enforcing the programme or tacitly encouraging employees to engage in impropriety.[43] A company can demonstrate good-faith enforcement by sanctioning misconduct and rewarding good behaviour.[44] Disciplinary action and compensation structures that impose financial penalties for misconduct can deter risky behaviour and foster a culture of corporate compliance.[45] At the same time, positive incentives, such as promotions, rewards and bonuses for improving and developing a compliance programme or demonstrating ethical leadership, can drive compliance.[46]

---

41 See Yoon & Carper, supra note 36.

42 See GIR Miller Remarks.

43 See US DOJ ECCP, at 2.

44 See US Sent'g Comm'n, Guidelines ManualU.S.S.G. § 8B2.1 (b)(6) (2021) (noting that an organisation's compliance programme should entail '('(A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct'). conduct').

45 See Monaco Memo ('Compensation systems that clearly and effectively impose financial penalties for misconduct can incentivize compliant conduct, deter risky behavior, and instill a corporate culture in which employees follow the law and avoid legal 'gray areas.'').

46 See Stephen M. Cutler, Dir., Div. of Enf't, Second Ann. Gen. Counsel Roundtable, Tone at the Top: Getting It Right, SEC (3 December 2004), http://www.sec.gov/news/speech/spch120304smc.htm ('[M]ake integrity, ethics and compliance part of the promotion, compensation and evaluation processes as well. For at the end of the day, the most effective way to communicate that 'doing the right thing' is a priority, is to reward it.').

With these principles in mind, DAG Monaco recently announced department-wide policy updates concerning corporate compensation systems, noting two significant changes in particular.

First, US prosecutors will assess a company's compensation structures when evaluating compliance programmes to determine how these structures contribute to the presence – or lack – of an effective compliance programme.[47] Is the company, for example, targeting bonuses to employees and supervisors who set the right tone, make compliance a priority and build an ethical culture? Companies should ensure that executives and employees are personally invested in promoting compliance, and 'nothing grabs attention or demands personal investment like having skin in the game' through direct and tangible financial incentives.[48]

Second, the DOJ is launching a three-year pilot programme to require, as part of a criminal resolution, that corporate compliance programmes include compensation-related criteria, and to offer fine reductions for companies that clawed back incentives paid out to employees and supervisors who engaged in or did not stop wrongdoing.[49] A company that fully cooperates with an investigation and timely and appropriately remediates the misconduct may receive an additional fine reduction if the company has implemented a programme to recoup compensation from the culpable employees.[50] 'We expect companies that use these programs to address not only employees who engaged in wrongdoing in connection with the conduct under investigation, but also those who had supervisory authority over the employees or business area engaged in the misconduct, and knew of, or were willfully blind to, the misconduct', stated the DOJ.[51]

These announcements exemplify the continuing formalisation of an existing practice of crediting companies for taking appropriate action as to culpable employees' compensation. For example, incentives for compliance-promoting behaviour were incorporated in a recent plea agreement between the DOJ and Danske Bank, the largest bank in Denmark, over alleged failures in the lender's anti-money laundering controls. As part of its agreement and in addition to

47 See ABA Conference Polite Remarks.

48 ABA Conference Monaco Remarks.

49 See ABA Conference Polite Remarks.

50 See *id.* (noting that 'prosecutors will accord an additional fine reduction equal to the amount of any compensation that is recouped' if a company has initiated the process to recover such compensation at the time of resolution); ABA Conference Monaco Remarks ('If the company succeeds and recoups compensation from a responsible employee, the company gets to keep that clawback money—and also doesn't have to pay the amount it recovered.').

51 ABA Conference Polite Remarks.

forfeiting $2 billion, Danske Bank agreed to revise its performance review and bonus system to include criteria related to compliance so that each executive is evaluated on his or her efforts to ensure that the relevant business unit is complying with internal policies and applicable laws and regulations.[52] Accordingly, Danske Bank executives with a failing score for compliance will fail to secure a bonus for that year.

Prosecutors' examination of the relationship between compensation structures and fostering responsible corporate behaviour reflects a broader commitment to finding the right incentives to support a culture of corporate compliance.[53] Companies are therefore encouraged to explore innovative, effective and targeted ways of leveraging compensation to incentivise good corporate behaviour and deter misconduct through their own mix of carrots and sticks.

Anonymous reporting mechanisms

Among the truest measures of a company's commitment to compliance is how it responds to potential misconduct. A company should have in place a well-functioning reporting mechanism for the anonymous reporting of suspected or actual breaches of internal policy.[54] An effective mechanism will facilitate the timely and thorough investigation of those reports, which includes routing complaints to proper personnel and tracking timing metrics of open and closed investigations.[55] Upon completion of a thorough probe, an organisation should document outcomes, monitor implementation of any remedial measures and share investigative findings with relevant stakeholders.[56] Should reported allegations be substantiated, best practices recommended by the DOJ dictate that the company examine what happened, why it happened (i.e., the root cause) and how to avert similar incidents moving forward (i.e., the lessons learned).[57]

---

52 See US DOJ, Plea Agreement in United States v. Danske Bank A/S C-5 (2022), https://www.justice.gov/opa/press-release/file/1557611/download.

53 See ABA Conference Monaco Remarks ('We want companies to step up and own up when they discover misconduct and to use compensation systems to align their executives' financial interests with the company's interest in good corporate citizenship.').

54 See US DOJ ECCP, at 6.

55 See *id.*

56 See FCPA Resource Guide, at 66.

57 See ABA Conference Polite Remarks (providing that prosecutors will continue to ask how companies 'learn from the issues they encounter').

But it is not enough to have such a reporting system in place without ensuring that employees and third parties know it exists.[58] Publicise the reporting system broadly, perhaps through periodic trainings or email reminders that boost its profile.[59] Hotline usage can be a good barometer of how well a company is advertising its reporting channels. Infrequent or non-use of a reporting hotline implies that employees or third parties are unaware of its existence or are aware but either lack the know-how to escalate concerns or are uncomfortable with or distrust the process.[60] In contrast, healthy hotline usage evinces a well-functioning system and constructive environment wherein individuals are empowered to 'speak up'.

Moreover, actively encouraging personnel to submit reports without fear of reprisal reinforces a corporate culture that promotes honest behaviour and incorporates reporting as part of one's ethical duties. To further signal transparency and foster trust in the process, provide detailed information on the procedural next steps after submitting a report.[61] Regulators want to see that reports 'are taken seriously, appropriately documented, investigated, and – if substantiated – remediated'.[62]

Monitoring and measuring compliance through data analytics

A staple of dynamic compliance programmes are mechanisms for collecting metrics to help detect and prevent misconduct, which also strengthen an organisation's internal communication channels more broadly. Indeed, government enforcement authorities have signalled that companies need to be collecting and analysing metrics about their programmes, emphasising the growing importance of data analytics in communicating to employees and stakeholders an organisation's commitment to maintaining an effective compliance system.[63] In October 2022,

---

58 See World Bank Guidelines, at 13.

59 See Helen Kim, Taking a Fresh Look at Hotlines: Fostering a Speak-Up Culture and Leveraging Data, Anti-Corruption Report (16 September 2020), https://www.anti-corruption.com/7543386/taking-a-fresh-look-at-hotlines-fostering-a-speakup-culture-and-leveraging-data.thtml.

60 See Vincent Pitaro, Revisiting Compliance Programs in Light of the DOJ's Updated ECCP, Anti-Corruption Report, Anti-Corruption Report (30 September 2020), https://www.anti-corruption.com/7626661/revisiting-compliance-programs-in-light-of-the-doj-s-updated-eccp.thtml.

61 See Kim, supra note 59 ('Companies should provide regular training to employees on the reporting process, not just the existence of the hotline, to set expectations and encourage continued engagement.').

62 NYU PCCE Polite Remarks.

63 See, e.g., Rebecca Hughes Parker, Using Data to Enhance Compliance Programs, Anti-Corruption Report (5 January 2022), https://www.anti-corruption.com/18633206/using-

for example, DOJ announced that it had hired Matt Galvin, former Global Vice President of Ethics and Compliance at Anheuser-Busch InBev SA, the world's largest brewery, for the new role of Compliance and Data Analytics Counsel in the Criminal Division's Fraud Section.[64] Moreover, '[o]bservers should expect Galvin to leave a mark on the DOJ similar to the one he left at AB InBev, where he transformed the company's compliance program to a data-driven machine'.[65]

Relatedly, DOJ Fraud Section Chief Glenn Leon recently announced that DOJ is gearing up to expand its use of data analytics as a key prosecutorial tool, and AAG Polite further noted that regulators have been focusing more and more on companies' use of data analytics to identify and prevent criminal wrongdoing.[66] Just as government regulators use these tools to detect and combat criminal schemes, so too are organisations increasingly expected to leverage data analytics tools within their operations to monitor compliance with laws and policies, ferret out wrongdoing, and deliver meaningful remediation.[67]

Gathering data helps organisations identify, mitigate, and respond to compliance risks in real time and diagnose behavioural compliance trends. Either internally or with external assistance, companies can optimise the utility of data analytics by tracking core compliance metrics, including due diligence reviews, hotline usage, investigations opened and closed, training completion rates, policies drafted or revised, disciplinary action and remediation status.[68] Capturing

---

data-to-enhance-compliance-programs.thtml ('The DOJ, SEC and other enforcement authorities have made clear that companies need to be gathering and analyzing data about their compliance programs, and the agencies themselves have become more sophisticated in their knowledge of data analytics.'); US DOJ, Deputy Attorney General Lisa O. Monaco Gives Keynote Address at ABA's 36th National Institute on White Collar Crime (28 October 2021), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute ('[D]ata analytics plays a larger and larger role in corporate criminal investigations, whether that be in healthcare fraud or insider trading or market manipulation.').

64 Hui Chen, New DOJ Fraud Section Data Expert Will Reshape Compliance, Law360 (7 October 2022), https://www.law360.com/articles/1537908/new-doj-fraud-section-data-expert-will-reshape-compliance.

65 *id.*

66 See Stewart Bishop, New Fraud Section Cases May Clarify Corp. Criminal Policy, Law360 (1 March 2023), https://www.law360.com/securities/articles/1581472?nl_pk=baa9efa1-db7b-4d64-bd71-9ee5a3e28f4d&utm_source=newsletter&utm_medium=email&utm_campaign=securities&utm_content=2023-03-02&nlsidx=0&nlaidx=8; ABA Conference Polite Remarks.

67 See NYU PCCE Polite Remarks.

68 See Andy Miller, How Visual Analytics Can Fuel a Compliance Program, Anti-Corruption Report (2 December 2020), https://www.anti-corruption.com/8042481/how-visual-

these metrics not only helps companies analyse patterns of misconduct and identify compliance vulnerabilities, it also helps companies demonstrate their commitment to mitigating risk when engaging with regulators in the context of government investigations.[69] As AAG Polite stated, 'When we see criminality, we will not just ask what happened. We want to understand the root causes – why it happened, and whether it will happen again'.[70] Analysing metrics further enables substantive assessment of high points and growth opportunities while offering benchmarks with which to anchor compliance targets and goals moving forward. This, in turn, breeds transparency and accountability by facilitating the reporting of actionable data to relevant stakeholders.

Adapting to local laws and customs

As if implementing a dynamic compliance programme were not already a delicate balancing act on its own, adapting programmes to address a spectrum of anti-corruption laws and other legislation adds to the challenge but is one that compliance programmes must address.

Complying with sweeping legislation across jurisdictions with varying enforcement landscapes

Distilling the vast expanse of bribery laws into manageable content for employees to understand and follow is not easy, especially with the cascade of countries that have enacted or amended a host of strong anti-corruption laws and enforcement regimes over the past decade. The FCPA, enforced by the DOJ and the SEC, is broadly applicable to US companies as well as foreign companies or persons with a nexus to the United States and their affiliates. This legislation prohibits foreign bribery of government officials but applies to the bribe payer only, whereas the UK Bribery Act (UKBA), passed in 2010, applies to both the bribe payer and the recipient. Moreover, the UKBA prohibits bribery of foreign public officials and private parties alike. These statutory regimes and the regulators who enforce them are usually well known to compliance professionals.

---

analytics-can-fuel-a-compliance-program.thtml.

69 See NYU PCCE Polite Remarks ('We want to see examples of compliance success stories—the discipline of poor behavior, the rewarding of positive behavior, the transactions that were rejected due to compliance risk, positive trends in whistleblower reporting, and the partnerships that have developed between compliance officers and the business. . . . We want to know that a company can identify compliance gaps or violations of policy or law.').

70 ABA Conference Polite Remarks.

Relatedly, the anti-corruption terrain in Latin America imposes jurisdiction-specific requirements that organisations must navigate. Various countries in Latin America, including Brazil, Colombia and Mexico,[71] have enacted corporate compliance requirements of their own in recent years, and companies engaged in those markets must be cognisant of these varying enforcement landscapes, which are also undergoing their own respective evolutions. For example, in July 2022, the Brazilian government published Federal Decree No. 11,129/2022, amending the regulation of Brazil's 2013 anti-corruption law known as the Brazilian Clean Companies Act (BCCA).[72] The decree also furnishes additional guidance related to the expectations of the Controladoria Geral da União, the entity that oversees compliance with the BCCA, in their assessment of integrity programmes and the range and application of administrative fines for violations of the law.[73] Additionally, the Chilean government even proposed new anti-corruption provisions to their constitution.[74] Though the constitutional proposal overall was rejected, as of March 2023, Chile has begun its second attempt to write a new constitution with a group of experts appointed by Congress. The vote to approve or reject the proposed text is scheduled for December 2023 and the potential passage of the constitution with any anti-corruption provisions the experts may draft will certainly be an area to monitor.[75]

---

71 In Colombia, the Anti-Corruption Act, Law 1474 of 2011, criminalises active and passive bribery, foreign bribery, political corruption and money laundering, among other crimes, and establishes administrative, criminal and fiscal sanctions. In Mexico, the General Law of the National Anti-Corruption System (SNA) coordinates the prevention, detection and prosecution of anti-corruption cases across municipal, state and local jurisdictions. Additionally, the Chilean government has even proposed new anti-corruption provisions to their constitution. Ropes & Gray LLP, Columbia, https://www.ropesgray.com/en/EnforcementExpress/Interactive-Maps/Latin-America/Colombia (last visited 22 March 2023); Anti-Corruption Act, Law 1474 of 2011, http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/Ley%201474%20de%2012%20de%20Julio%20de%202011.pdf (last accessed 22 March 2023).

72 BRAZIL. Decree 11.129 of 11 July 2022. Regulates Law No. 12,846, of 1 August 2013, which provides for administrative and civil liability of legal entities for the practice of acts against the public administration, national or foreign. Diário Oficial da União, Brasília, DF, 12 July 2022, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11129.htm (last accessed 22 March 2023).

73 *id.*

74 Eduardo Engel & Benjamin Garcia, A new constitution for Chile: Let's try again?, Hewlett Found. (21 February 2023), https://hewlett.org/a-new-constitution-for-chile-lets-try-again/.

75 Chile starts second attempt to draft a new constitution, *Reuters* (6 March 2023), https://www.reuters.com/world/americas/chile-starts-second-attempt-draft-new-constitution-2023-03-06/

Taken together, it is clear that multinational organisations will need to ensure that their compliance programmes and global personnel adhere to the mandates that regulators impose. And whether it is the FCPA, the UKBA or local anti-corruption laws, the basic proscription is the same: nothing of value can be given, directly or indirectly, to improperly influence government officials or commercial counterparties.

Tailoring a global compliance policy

A global enterprise faces a wide array of compliance concerns including bribery, corruption, embezzlement, money laundering, employee kickbacks, accounting irregularities and conflicts of interest across geographies. Tailoring compliance programmes to the localities in which multinational companies operate while simultaneously addressing these cross-jurisdictional concerns poses yet another uphill challenge.

A multinational company may, for instance, choose to implement uniform global compliance policies that include requirements that are either more or less restrictive than local regulations, like those discussed above. Other multinational companies may mix and match – applying consistent standards globally while also supplementing them with country-specific guidance. Given the sheer number of individuals within a multinational organisation, it is also advisable that companies create roles for compliance professionals to be available to personnel globally for 'on the ground' guidance and feedback.

Tailoring training to an audience's size, industry, risk profile, geographical footprint, language, sophistication and subject-matter expertise is crucial and underscored in the DOJ's March 2023 ECCP.[76] Above all else, when developing training programmes, multinational companies should tailor presentations and materials to the roles of its workforce, and policies and training should be presented in local languages and in person to the extent possible.[77] Aiding companies that operate in Spanish-speaking jurisdictions and recognizing the significant need for alignment with regional developments, AAG Polite at the ABA Conference announced that the DOJ would reissue the 2020 FCPA Resource Guide in Spanish.[78]

---

76 See US DOJ ECCP, at 1.

77 See Globalizing Your Compliance Program, Ropes & Gray LLP (29 January 2018), https://www.ropesgray.com/en/newsroom/alerts/2018/01/Globalizing-Your-Compliance-Program.

78 ABA Conference Polite Remarks.

Training programmes should also be brimming with real-world examples tailored to any specific localities. Real-world examples that span the globe while also implicating Latin America are not difficult to find. In April 2022, for example, Stericycle Inc. ('Stericycle), an international waste management company headquartered in Illinois, agreed to pay more than US$84 million to resolve parallel investigations by authorities in the United States and Brazil into the bribery of foreign officials in Brazil, Mexico and Argentina.[79] Specifically, between 2011 and 2016, Stericycle caused hundreds of bribe payments that were calculated as a percentage of the underlying contract payments owed to Stericycle from government customers to be made to officials at government agencies and instrumentalities in Brazil, Mexico and Argentina.[80]

The DOJ enforcement action against Stericycle, along with a parallel investigation by the SEC related to conduct in multiple jurisdictions, provides a window for compliance professionals to educate their workforces on how bribery and books-and-records violations can play out in Latin America. Indeed, in all three countries, the co-conspirators tracked the bribe payments through spreadsheets and described the bribes through code words and euphemisms, such as 'CP' or 'commission payment' in Brazil, 'IP' or 'incentive payment' in Mexico, and 'alfajores' (a popular cookie) in Argentina.[81]

In the aviation sector, Linhas Aéreas Inteligentes S.A. (GOL), an airline headquartered in São Paulo, Brazil, paid more than $41 million to resolve parallel bribery investigations by criminal and civil authorities in the United States and Brazil.[82] According to AAG Polite's statement in a September 2022 press release:

79 See US DOJ, press release 22-401, Stericycle Agrees to Pay Over $84 Million in Coordinated Foreign Bribery Resolution (20 April 2022), https://www.justice.gov/opa/pr/stericycle-agrees-pay-over-84-million-coordinated-foreign-bribery-resolution (last accessed 22 March 2023).

80 See *id.*

81 See *id.*

82 US DOJ, press release 22-978, GOL Linhas Aéreas Inteligentes S.A. Will Pay Over $41 Million in Resolution of Foreign Bribery Investigations in the United States and Brazil, (15 September 2022), https://www.justice.gov/opa/pr/gol-linhas-reas-inteligentes-sa-will-pay-over-41-million-resolution-foreign-bribery (last accessed 22 March 2023).

> *GOL paid millions of dollars in bribes to foreign officials in Brazil in exchange for the passage of legislation that was beneficial to the airline . . . The company entered into fraudulent contracts with third-party vendors for the purpose of generating and concealing the funds necessary to perpetrate this criminal conduct, and then falsely recorded the sham payments in their own books.*[83]

As part of the resolution, GOL agreed to continue to enhance its compliance programme and provide reports to the DOJ regarding the remediation and implementation of compliance measures, signalling the importance of compliance professionals enhancing their compliance programmes in the first instance.

Companies that operate in the oil and gas sector will also find lessons learned in the use of intermediaries to facilitate improper payments from Honeywell UOP's December 2022 resolution. There, Honeywell UOP agreed to pay US$160 million to resolve parallel bribery investigations by criminal and civil authorities in the United States and Brazil stemming from funds offered to a high-ranking official at Brazil's state-owned oil company.[84] As part of the arrangement, Honeywell UOP entered into an agency agreement with a sales agent for the purpose of paying US$4 million to the high-ranking Petróleo Brasileiro S.A. (Petrobras) executive.[85]

The increase in individual prosecutions involving Latin America also signals a continued focus on the region as well as a regulatory focus on individual accountability. In 2022 and 2023, for example, both Venezuelan and Brazilian nationals have been charged with violations of the FCPA. More specifically, in February 2023, a senior oil and gas trader and a Brazil-based intermediary were charged with conspiracy, multiple counts of violating the FCPA and money laundering in connection with an alleged scheme to pay bribes to Brazilian officials to win contracts with Brazil's state-owned and state-controlled energy company,

---

83 *id.*

84 US DOJ, press release 22-1383, Honeywell UOP to Pay Over $160 Million to Resolve Foreign Bribery Investigations in U.S. and Brazil, (19 December 2022), https://www.justice.gov/opa/pr/honeywell-uop-pay-over-160-million-resolve-foreign-bribery-investigations-us-and-brazil (last accessed 22 March 2023).

85 See *id.*

Petrobras.[86] Clearly, FCPA enforcement in Latin America is 'forecast to remain hot as US regulators strengthen partnerships with their counterparts' and the 'pace of FCPA enforcement doesn't appear to be slowing in 2023'.[87]

Tailoring global compliance policies in a way that grapples with these real-world realities, whether they draw from corporate resolutions or individual prosecutions, will only provide multinational companies with a competitive advantage and bolster their ability to attract and retain superior talent. It will also ensure that business is done the 'right' way and help employees, wherever they are in the world, take stock in a company that acts with integrity.

Conclusion

Compliance programmes that incorporate the lessons learned from around the globe and marshal the tools outlined above as prophylactics will be well positioned to avoid enforcement actions on the back end. Government regulators are encouraging companies to do precisely that for their own benefit.

Architects who design compliance programmes in this age of anti-corruption 'accretion' must look to the past, present and future in managing multinational workforces and building effective internal communication channels. Compliance programmes should factor into their policies the role of incentives and clawbacks, especially as they relate to executive compensation and rewarding compliance leadership. Training should include lessons learned from past enforcement actions as well as lessons from within a company while making innovative use of measures such as data analytics in diagnosing, mitigating and responding to compliance risks. Training should also take a multidirectional approach to educating the workforce on the current state of anti-corruption accretion and its evolving nature and be tailored to an employee's locality when applicable. In addition, trainings should provide employees a glimpse into what the future could hold as seen in recent enforcement actions if compliance is not prioritised, providing adequate resources, anonymous reporting mechanisms, guidance and even mega-fine figures to ensure that the future is not, in fact, realised.

---

86 US DOJ, press release 23-187, Senior Oil and Gas Trader and Brazil-Based Intermediary Charged in Bribery and Money Laundering Scheme (17 February 2023), https://www.justice.gov/opa/pr/senior-oil-and-gas-trader-and-brazil-based-intermediary-charged-bribery-and-money-laundering (last accessed 22 March 2023).

87 Phillip Bantz, White Collar Attys Brace For More Latin America FCPA Action, Law360 (8 February 2023), https://www.law360.com/articles/1574007/white-collar-attys-brace-for-more-latin-america-fcpa-action.

CHAPTER 9

How to Conduct Internal Investigations of Alleged Wrongdoing

Adrián Magallanes Pérez and Diego Sierra Laris[1]

Introduction

This chapter provides a framework for how to conduct an internal investigation into any situation in which the code of conduct, internal policies of a company, or applicable laws or regulations might have been breached. Although we focus on practice in Mexico, we believe the ideas we develop can be applied more broadly in whichever jurisdiction an investigation is being carried out.

When properly conducted, internal investigations help companies to respond adequately to adverse situations that arise from possible wrongdoing, avoid or mitigate risks and potential administrative or criminal liability, and take appropriate measures to sanction and prevent the repetition of improper conduct.

Additionally, as part of investigations, companies can prevent tampering or destruction of relevant evidence and information that authorities may request in labour, administrative or even criminal procedures, by properly identifying sources of information such as video recordings, witnesses or documents.

Before starting an investigation, the investigator must review the legislation applicable to the conduct being investigated and the scope of permissible investigations. Different legal areas might require review. Criminal, data protection and labour law can be relevant to each step of the investigation.

1 Adrián Magallanes Pérez and Diego Sierra Laris are partners at Von Wobeser y Sierra, SC.

Importance of internal investigations

Internal investigations help companies to identify, prevent, measure, and avoid or mitigate risks of potential liability and determine the validity and seriousness of the concerns that have triggered the need for an investigation.

However, different laws foresee a duty to investigate internally, and regulators consider the implementation and application of internal policies before imposing any sanctions for improper conduct.

In recent years, various countries, including Argentina, Brazil, Chile, Colombia, Costa Rica, Mexico and Peru, have modified their anti-corruption laws to facilitate corporations' prosecution and establish requirements or mitigation credit for companies' anti-corruption compliance programmes.

Pursuant to Article 422 of the Mexican National Code of Criminal Proceedings (NCCP), when determining a corporation's liability, law enforcement authorities must consider, among other aspects of corporate culture, the existence of proper controls within the company, such as adequate investigative methods. Since Mexican laws do not currently provide objective and clear standards for evaluating such controls and procedures, the Public Prosecutor's decision is mostly discretionary. However, in the First Annual Report of Activities and Results of the Specialized Agency for Combating Corruption, the Anti-Corruption Prosecutor María de la Luz Mijangos Borja, committed to propose guidelines to evaluate corporate compliance programmes. It will be interesting to learn about the development of prosecutorial criteria and whether they will work in a similar way to those best practices laid out by the US Department of Justice (US DOJ) and the US Securities and Exchange Commission (US SEC) (e.g., FCPA Resource Guide and the June 2020 DOJ Evaluation of Corporate Compliance Programs).

In addition, Article 11 of the Federal Criminal Code allows for a reduction in criminal liability of up to a quarter of the corporation's liability, as long as the corporation proves that, before the commission of the unlawful conduct, it had a compliance department in charge of preventing that conduct and that it sought to mitigate the potential harm before or after being accused.

Furthermore, the Mexican General Administrative Responsibilities Law provides that law enforcement authorities must consider a company's 'integrity policy' before determining the applicable sanctions. Article 25 of this Law provides that an integrity policy must contain, among other things:

> *a code of conduct duly published and circulated among all members of the organization, with systems and mechanisms of real application, and adequate reporting systems both within the organization and to the competent authorities, as well as disciplinary systems and specific consequences regarding those who act against internal policies or Mexican legislation.*

Moreover, under NCCP Article 222, any person with knowledge of conduct that could constitute a probable crime shall report it to the authorities. Failure to report conduct that could constitute a probable crime could be sanctioned through the crime of concealment. Thus, the rule calls for a probabilistic analysis, measuring the likelihood of an event taking place. Therefore, corporations should decide whether the particular facts hit a certain standard and thereby trigger a reporting obligation. Federal courts have issued non-binding precedents on the elements of that crime, ruling that an individual can be held liable for the crime of concealment, if obtaining knowledge that identifies criminal activity of a specific time and place. Since we believe that the principle of presumption of innocence should be weighed into the required probabilistic analysis, and if persons are to be considered innocent until proven guilty beyond a reasonable doubt, the probabilistic analysis should imply a high scrutiny: not just a more probable than not (preponderance of the evidence), but one that alludes to the severity of the matter at hand (beyond a reasonable doubt). Therefore, the person or corporation considering or deciding whether to self-report should evaluate whether the reported conduct supports a certain probabilistic importance meriting that report. Therefore, a company can only make an informed decision and reduce exposure to the crime of concealment by conducting a thorough and structured investigation of probable wrongdoings.

Article 20, Section B of the Mexican Constitution provides the fundamental right against self-incrimination in criminal matters. However, Mexican courts have not issued binding precedents on how this is related and applies to the complexity of a company's duties to report illegal conducts to prove efficient internal policies and controls to mitigate or even exclude the company's criminal liability for concealment or any other crime applicable (e.g., bribery).

In enforcing the US Foreign Corrupt Practices Act (FCPA), the DOJ and the SEC also consider the investigative steps taken by a company before imposing sanctions. The 'Resource Guide to the US Foreign Corrupt Practices Act' (the FCPA Resource Guide) provides that:

> *once an allegation is made, companies should have in place an efficient, reliable, and properly funded process for investigating the allegation and documenting the Company's response, including any disciplinary or remediation measures taken. Companies will want to consider taking 'lessons learned' from any reported violations and the outcome of any resulting investigation to update their internal controls and compliance program and focus future training on such issues, as appropriate.*[2]

In some cases, external auditors are obliged to investigate and evaluate certain potentially illegal types of conduct when analysing a company's financial statements.

Well done internal investigations not only decrease the risk of potential corporate liability but also foster employees' commitment to internal policies and applicable laws.

Beginning of the investigation

A well-structured compliance programme and internal auditing systems are essential for any company to prevent and manage any potential liability. Data from self-reported cases of foreign bribery show that companies are most likely to become aware of bribery by internal audits (31 per cent), M&A due diligence (28 per cent) and whistleblower complaints (17 per cent).[3] Another report by an international accounting firm found that 25 per cent of the fraud cases discovered in surveyed companies came to light through whistleblower complaints, which was the main source for detection of fraudulent acts.[4]

A well-structured and properly publicised hotline is essential for any compliance programme and for an eventual investigation, given that it allows employees to denounce any potentially improper conduct anonymously and without fear of retaliation. This is also helpful for investigators, given that it provides additional data about allegedly improper conduct, and whistleblowers can function as collaborative parties.

---

2 US Department of Justice, Criminal Division, and US Securities and Exchange Commission, Enforcement Division, *A Resource Guide to the U.S. Foreign Corrupt Practices Act* – Second Edition (2020), p. 66.

3 See OECD Foreign Bribery Report, 'An analysis of the crime of bribery of foreign public officials', OECD (2014), https://read.oecd-ilibrary.org/governance/oecd-foreign-bribery-report_9789264226616-en#page18pp. 16-17.

4 KPMG Forensic, 'Profile of a Fraudster', Survey, 2007, p. 26.

However, companies must be aware of the applicable laws, particularly regarding data protection concerning the extent to which a hotline might be used. For instance, in some countries, labour issues might be excluded from an internal hotline scope.

Besides whistleblower complaints, internal investigations might also be triggered by direct complaints, lawsuits, threatened litigation, government inquiries, suspicion of misconduct within the company, media reports or accidents in the workplace, among others.

On some occasions, internal investigations might be a result of government investigations. In these cases, the nature and certain aspects of an investigation might change, or an investigation and cooperation with authorities might be necessary to obtain reduced sanctions and other benefits.

Once a report is received from any internal or external source, it must be redirected to the proper authorities within the company to (1) make a preliminary assessment of the report, (2) determine the nature of the reported conduct and (3) evaluate whether external counsel is needed.

It is usually advisable for companies to assign the responsibility of receiving, following up, and preparing reports of potential improper conduct to internal legal and compliance authorities, given their knowledge and understanding of the applicable regulations and relevant areas within the company, particularly their sensitivity to topics such as legal privilege or preservation of evidence.

Preliminary assessment

Before starting any internal investigation, a company should make a preliminary assessment of the reported conduct to determine whether an investigation is appropriate. A correct preliminary evaluation of the proper type and extent of investigation will save a company both time and costs.

Frequently, reported conduct, even if assumed to be true, might not constitute a breach of the applicable laws or regulations and can be dismissed at the outset. Furthermore, certain issues might imply an easy and quick solution without needing a full investigation. In these situations, depending on the allegation's nature, the receiving department might solve the problem directly or forward it to the proper area to take any necessary action.

However, when there is reasonable evidence of potential improper conduct, the best course of action will be for the company to trigger an internal investigation.

The situation becomes more complicated when there are indications of potentially improper conduct, but only limited information is available in the first instance. In these cases, investigators should seek other methods of obtaining preliminary information before initiating a full investigation. One effective way

to do this is to seek further assistance from the whistleblower or conduct preliminary interviews of potentially collaborative parties while striving to preserve the investigation's confidentiality. Otherwise, evidence could be hidden or destroyed by the alleged perpetrators.

A good practice when a company has obtained preliminary confirmation of potential wrongdoing is to issue a hold notice to all relevant employees and departments involved in the investigation, instructing that data, documents or records should not be destroyed, removed or altered from that time going forward.

Nature of the reported conduct

Once a company determines that a full internal investigation is necessary, it will need to unravel the nature of the reported conduct, to establish a preliminary scope of the investigation, foresee the potential implications of the conduct and determine which department would be the most suitable to carry out the investigation.

Departments that may handle these types of investigations include compliance (in respect of anti-corruption and anti-money laundering), audit (e.g., fraud and improper use of assets), legal (e.g., public bids, intellectual property and anti-trust), human resources (e.g., labour, health and workplace security) and IT (e.g., cybersecurity), among others.

However, this could greatly vary from one company to another. Some aspects to take into consideration are the resources available, the experience and authority of the investigators within the company, and the perception of independence. In any event, the investigators must be perceived as independent and must avoid any conflict of interests.

For specific types of investigations, different departments should cooperate and interact (e.g., anti-corruption, human rights, fraud and sexual harassment). When suspected misconduct involves senior management or serious misconduct, or there is a potential conflict of interests, the company should take all necessary steps to maintain independence and impartiality. In these cases, it might be advisable to create a special committee of the board or retain external counsel.

Is external counsel needed?

Depending on the nature of the reported conduct, it might be advisable to retain external counsel to perform the investigation or to serve as an aid. External counsel may offer substantive expertise, relevant experience, scale and other benefits not available from internal resources. Additionally, other external experts may be needed to assist with an internal investigation, such as forensic accountants or e-discovery vendors.

When assessing whether to retain external counsel, another consideration is the potential applicability of the attorney–client privilege and work-product doctrines. The work of external counsel is usually protected by legal privilege, whereas that of in-house counsel may not be protected. In the United States, attorney–client privilege typically applies to the work of both external and in-house counsel. Relatedly, the work of accountants and other third parties may qualify as privileged when work is under the direction of external counsel to enable counsel to provide legal advice.[5]

In Mexico, rather than a specific attorney–client privilege, there is a general obligation for all professionals, including attorneys, to maintain professional secrecy. However, attorney–client privilege may be claimed over communications exchanged between counsel and client. This criterion has been developed only recently in Mexican law: in an antitrust investigation, tribunals have held that the privilege covers communications between a client and its external counsel. According to the courts' interpretation, 'communication' is understood to refer to all information exchanged and thus refers to both spoken or written communications (e.g., verbal conversations and emails) or work-product (such as written notes or memoranda). Some of these precedents also suggest that legal privilege in Mexico shall not be applicable to in-house counsel.[6] Under NCCP Article 362, the testimony of any person who has knowledge of the facts under investigation because of their profession is inadmissible, unless the owner of the privileged information issues a formal release (e.g., ministers, lawyers, human rights visitors, doctors, psychologists). Hence, companies should give careful consideration to the question of retaining external counsel at the outset of an investigation. If a company decides not to, the work-product obtained from the investigation and third parties hired by the company might not be protected under privilege. Therefore, regulators and enforcement authorities (and civil litigants) could demand full access to those potentially adverse and incriminating documents.

---

5 Tarun, Robert W, and Tomczak, Peter P, *The Foreign Corrupt Practices Act Handbook: A Practical Guide for Multinational Counsel, Transactional Lawyers and White Collar Criminal Practitioners*, Third Edition, American Bar Association (2013), p. 196, quoting *In re John Doe Corp.*, 675 F.2d 482 (2d Cir. 1983) (investigation by accounting firm as part of its audit is not privileged) and *In re Grand Jury Subpoena*, 599 F. 2d 504, 510 (2d Cir. 1979) (investigation by management is not privileged).

6 See 'Non-binding precedents No I.1o.A.E.193 A (10a.) and I.1o.A.E.194 A (10a.) by the First Collegiate Court on Antitrust, Broadcasting and Telecommunications Matters for the First Circuit (Mexico City)' in Federal Judicial Weekly Report and its Gazette, Volume XXXVIII (January 2017), pp. 2475, 2721.

Investigation plan

Confirming the preliminary assessment regarding the scope and nature of an investigation and drafting an investigation plan will provide a clear road map. As a minimum, such a plan should consider the following aspects:

- nature of the investigation;
- scope of the investigation;
- specific potential improper conduct;
- relevant stakeholders and involved parties;
- time frame;
- evidence needed and available;
- potentially applicable legislation, regulations and internal policies;
- the need for experts to conduct or assist with the investigation (e.g., forensic accountants or economists); and
- confidentiality policies.

Self-reporting or revealing that a company is conducting an investigation is always fact-specific. A company might want to disclose its investigation plan to the authorities early in the process, with the aim of receiving cooperation credit and avoiding more severe sanctions at a later stage.

Depending on the nature and facts of the investigation, it might be advisable to conduct certain interviews and request cooperation from any whistleblower and potentially collaborating parties before moving to the investigation's next steps. At all times, it is critical to protect the confidentiality, integrity and potential evidence related to the investigation.

Furthermore, investigators should consider whether it is convenient to notify the implicated parties or the whole company and to what extent, always considering the measures necessary to preserve evidence and avoid retaliation.

Investigators must always be mindful of the company's best interests and that all documents created, facts uncovered and witness statements in relation to the investigation might be shared with or requested by authorities in the future.

Preservation of evidence

An essential step at the outset of an internal investigation is preserving potentially relevant evidence. Measures to preserve evidence include:

- gathering and securing electronic and physical information (such as hard copy files);
- sending preservation notices to employees, informing them that it is prohibited to delete, alter, or destroy any relevant evidence and information;

- communicating to employees about the existence of an investigation, requesting them to cooperate and maintain the investigations' confidentiality and stop or deter certain conduct, which may also serve to avoid any gossip and speculation within the company;
- restricting access to certain information to preserve its integrity; and
- suspending employees who could compromise the integrity of the investigation.

If the company suspects that the well-being of a potential collaborator or witness might be compromised as a result of the investigation, the company should take note of this sensitive subject and assess if it is possible to issue instructions or measures to protect their integrity and willingness to aid the investigators.

Investigators must always be aware of the applicable data privacy laws when securing, transferring and sharing information, and of guaranteeing appropriate protection of personal data. This is particularly relevant in transnational investigations in which information might be transferred to different countries, or shared between counsel in different jurisdictions, often offering inconsistent regulations.

Before securing information from emails or cellphones owned by the company, it is advisable to have a prior policy or consent regarding the company's authority to access information that belongs to the company or is related to employees' work. The company must properly inform employees that the information created and shared within the company network and systems belongs to the company and shall be subject to scrutiny, without any expectation of privacy.

Depending on the jurisdiction, it may be advisable to have a prior signed consent from employees (e.g., as a condition of employment), given that some jurisdictions require express consent to use and have access to communications from third parties. In Mexico, a prior policy without express consent could be considered insufficient to obtain and process an employee's data.[7]

7 See Non-binding precedent, 'Prueba electrónica o digital en el proceso penal. Las evidencias provenientes de una comunicación privada llevada a cabo en una red social, vía mensajería sincrónica (chat), para que tengan eficacia probatoria deben satisfacer como estándar mínimo, haber sido obtenidas lícitamente y que su recolección conste en una cadena de custodia' [Electronic or digital evidence in a criminal proceeding. Evidence regarding private communications in a social network via chat, to be legal must satisfy a minimum standard by having been legally obtained and properly documented in a chain of custody'], First Collegiate Tribunal in Civil Matters for the First Circuit, 2013524. I.2o.P.49 P (10a.), Federal Judicial Weekly Report and its Gazette, Volume XXXVIII (January 2017), p. 2609 (MEX).

If a company does not have a proper policy or seeks to obtain communications from personal devices, to the extent permissible, it should obtain written and signed consent from the owner of the device. The interception of private communications is usually prohibited and considered a criminal offence in many jurisdictions (e.g., Mexico).

Ownership of the documents and the chain of custody will also be relevant if the documents have to be produced in litigation, administrative or criminal proceedings, or to regulators. If the documents belong to the company, in principle, the company will be able to directly produce them before any authority. However, if the documents belong to an individual, the company will usually need that person's consent or to request judicial assistance to obtain them lawfully.

The chain of custody is relevant in criminal and some administrative and civil proceedings to assure that the documents have not been tampered with or contaminated. Each measure and step related to gathering, handling, storing, securing, transferring, and managing evidence must be properly documented to guarantee that evidence is authentic and legal. A chain of custody is a *sine qua non*-requirement for the validity of evidence in many criminal and some civil proceedings.[8] Intervention of forensic experts with verified training and expertise in implementing and following a proper chain of custody is recommended, as both physical and digital integrity of information must be guaranteed to enforcers and litigators.

Measures to avoid retaliation

Investigators must promptly take all necessary measures to avoid any retaliation against whistleblowers, cooperating parties, stakeholders or even the implicated parties. This helps preserve the integrity of an investigation and anyone involved.

Examples of appropriate measures to avoid retaliation are:

- maintaining the confidentiality of the whistleblower and cooperating parties;
- restricting access to certain information;
- the temporary reallocation of certain employees; and
- the suspension or removal of potentially implicated parties.

8 See Non-binding precedent 'Cadena de custodia. Debe respetarse para que los indicios recabados en la escena del crimen generen convicción en el juzgador' [Chain of custody. It must be guaranteed in the crime scene for indicia to generate conviction in the judge], First Chamber of the Supreme Court of Justice, 2004653, 1a. CCXCV/2013 (10a.), Federal Judicial Weekly Report and its Gazette, Volume XXV (October 2013), p. 1043 (MEX).

Not being able to take appropriate measures to avoid retaliation will be viewed negatively by regulators and authorities. Furthermore, these measures strengthen a culture of compliance within the company, guaranteeing that employees will not be punished in any way for denouncing, in good faith, any improper conduct or cooperating with an investigation. By failing to take these measures, a company might give a contradictory message to its employees.

Document review

A key step in any investigation is obtaining the proper evidence regarding the potentially improper conduct. Thorough e-documents searches are standard for virtually any significant internal investigation and have proven to be revealing in improper conduct investigations. Additionally, cellphone searches are becoming increasingly relevant, given that alternative channels of communications such as WhatsApp, Microsoft Teams or Telegram are being used more often as working tools, especially in the aftermath of the covid-19 remote working conditions, in which companies encouraged and explicitly authorised that virtually all information and communications related to work activities are created, stored and shared via email or these new communication channels. Improper conduct is now documented in emails less often, and people are more wary about what they write in emails. Other relevant evidentiary sources include working documents held in computers or databases, such as Word or Excel documents, as well as physical documents and material.

Documents and information should be collected and reviewed in light of the scope of the investigation, the implicated parties and any other evidence that suggests that the documents might be relevant for the investigation.

Numerous e-discovery platforms enable counsel or other investigators to apply search criteria to reduce the amount of information that needs to be analysed. Artificial intelligence that uses predictive coding is also a powerful tool that can reduce time and costs.

The people in charge of reviewing documents must have sufficient knowledge of the nature and scope of the investigation, the relevant facts and the information that they should be seeking, so as to properly identify relevant documents. This is often one of the most labour-intensive parts of an investigation and is essential for proper fact-finding.

Adequate document review therefore should include a protocol or methodology to properly tag electronic documents by issue and identify potentially confidential or privileged information.

Once documents have been reviewed, it is useful to have a chronology of all relevant documents and information to track and analyse key events, conduct, stakeholders and documentation. Again, investigators must be mindful of the company's best interests and that all documents created, facts uncovered and witness statements in relation to the investigation might be shared with or requested by authorities in the future.

As well as a document review, it is sometimes advisable to seek additional sources of information and, depending on the case, to engage an accounting firm to conduct forensic transaction testing. Often, the sources of concern lie in how a company keeps its books and records. Forensic and accounting experts will analyse whether a company's books accurately, reasonably and timely reflect the transactions represented therein. They also might look into revenue recognition in books and reality and search for discrepancies with a company's policies. Moreover, they will frequently analyse third-party vendor accounts and whether their services and bills are well supported and conform to market standards.

Additionally, some investigations may benefit from the engagement of a vendor to conduct open-source investigation regarding possible relevant parties in public records and online information. Some conflict of interest or corruption allegations might not be clarified until shareholders, managers or legal representative of certain companies are properly identified and their relationships with a company's employees understood.

Online public information may also provide document reviewers with additional context or clues to properly discriminate between relevant and non-relevant information. For example, a vendor might not seem to be related in any way with a public official, but the media or social networks might provide some valuable indications not known or revealed by witnesses or internal documents.

Interviews

Interviews are also essential to any corporate internal investigation, ideally once a thorough document review has been performed, and the key issues have been outlined in a working chronology. Interviews should be conducted with relevant stakeholders, witnesses and implicated individuals. In general, all those materially involved in the underlying facts should be interviewed.

For this, investigators must (1) determine which parties to interview according to the evidence previously obtained, (2) draft an interview protocol regarding the relevant evidence and facts, and (3) conduct interviews in accordance with the foregoing.

The interview protocol should serve as a guideline for the interviews, by making express reference to the relevant documents by topic or chronological order and the proposed questions for interviewees. Other relevant topics that might be useful are the factual background, knowledge of the regulation applicable to the conduct and proposals for how to remediate certain types of conduct.

Depending on the case, it might be advisable first to interview witnesses and then the implicated parties, starting with lower-level employees and working up to the most senior employees. Investigators must also pay close attention to who will perform and be present during the interviews. In all cases, investigators must make sure to be perceived as independent and to try to avoid creating an overly formal environment that could affect the outcome of the interviews. Interviewers must be mindful of the language used during the interview, as well as of the setting and number of people present during an interview, which might favour or restrict the flow of information. Therefore, interviews of low-level employees will not always be performed in the same manner as those related to higher-ranking officials in the company.

Depending on the jurisdiction, investigators typically inform interviewees (1) that they only represent the company (or whoever they represent) and do not represent the interviewees or their interests and that they may wish to seek separate counsel, (2) of the purpose of the interview, (3) that the interview is privileged and confidential and shall not be shared or disclosed by the employee with third parties, and (4) that the privilege and confidentiality of the interview belong to the company, and that only the company controls such privilege and might decide to waive and disclose it to third parties, including authorities. This is known as the *Upjohn* warning, which originates from the case *Upjohn Co. v. United States*.[9]

Interviews should seek to establish the facts by presenting relevant documentation and allowing interviewees to accurately recollect the facts and express their opinion with the aim of obtaining information that is as accurate and reliable as possible. Interviewees might request before or during the interview to have their own counsel present or to have an opportunity to be advised by their own counsel. One issue that may arise is whether the company should pay for an employee's personal counsel.

In general, interviewers should avoid recording or transcribing interviews verbatim; note taking is the standard. Among other considerations, recordings and transcripts are also usually not protected by legal privilege and they add an

9 *Upjohn Co. v. United States*, 449 U.S. 383 (1981).

air of unnecessary formality to an interview, which can be counterproductive in some cases and can affect the quality and content of the interviewee's responses. Consistent with legal privilege, it is usually advisable to take notes on personal perspectives and opinions about the interview, and to address legal theories.

Third parties are in no way obliged to agree to these interviews and careful consideration must be given before interviewing third parties or former employees over which the company has no authority. Anti-corruption contractual clauses can in some cases be useful for the purpose of compelling a third party to cooperate. In these cases, investigators must weigh the potential benefits and costs, and act in the best interests of the company.

After the interview, employees should be reminded of the confidentiality of the information and that the information must not be shared with other employees or any third party and provide contact details in case the interviewee wishes to share documents or additional information. The interviewer should also remind the interviewee of anti-retaliation policies and protective measures in case they are approached by implicated parties or pressured to disclose information related to the investigation or their interviews. Once the information has been analysed, investigators must determine whether additional fact-finding in the form of document review or interviews is necessary or if they should proceed with the final report and suggested remediation measures.

Interviewers and employers should be mindful of not restricting an interviewee's freedom to leave the premises where the interview is being conducted, and should avoid conduct that could be interpreted as intimidating as laws often provide criminal liability for illegal restrictions to personal freedom and threats.

Final report and remediation measures

Once an investigation has been concluded, investigators should analyse all the information gathered in the investigation and report the findings and suggested remediation measures to the appropriate officers and directors within the company (and, potentially, outside the company). The final report should address the factual issues and conclusions and provide a legal analysis of the subject matter and the potential remediation measures that the company might adopt. However, this sequence of events needs to be flexible. Investigations frequently offer insights into other aspects of the business that require greater scrutiny. Thus, one line of analysis often sets the stage for a new or deeper investigation.

Depending on the case, careful consideration must be given to whether the report will be in written form or oral.

Companies should always take appropriate remediation measures to ensure that the risk of repetition of improper conduct is mitigated and properly sanction those who may have acted improperly. This is essential to mitigate any risk for the company and, in fact, without this step, an investigation ultimately may become meaningless.

Some typical remediation measures include:

- disciplining the implicated parties (for which it is advisable to have already established a policy);
- implementation or enhancement of internal controls;
- appropriate training;
- measures to avoid repetition of the improper conduct;
- amendment of certain contractual provisions, such as inclusion of anti-corruption representations and warranties and audit clauses;
- termination of contracts or relationships with third parties;
- disclosure within the company of certain information about the investigation and remediation measures;
- oversight of certain areas or transactions;
- periodical testing and assessment of internal controls; and
- reporting to the proper authorities, if deemed appropriate and advisable under the particular circumstances.

When taking remedial action, parties should seek to be consistent in imposing and applying measures and should always seek to reduce the risk of repetition and implement measures to identify future risks. In particular, companies must heed the lessons learned and incorporate them into their policies and procedures to avoid or mitigate recurrence risk.

Local applicable labour laws must be analysed before taking any action against employees. For instance, Mexican legislation does not allow a salary reduction[10] and grounds for dismissal follow strict scrutiny and will always be interpreted in favour of the employee.

Finally, the appropriate department within the company must decide whether the investigation and its findings should be notified or voluntarily disclosed to regulators or other authorities, to the extent not already self-reported or otherwise known. This is a decision that should not be taken lightly and requires consultation with external counsel with proper knowledge of the jurisdiction and applicable laws, as such a report may trigger a broad investigation by authorities.

10 Mexico's Federal Labour Law, Articles 51(IV), 82 and 84.

Companies may engage in a dialogue with the authorities and opt to cooperate in their investigation to try to seek a reduction of sanctions. Some of the criteria taken into account by authorities when considering whether to reduce sanctions are whether the cooperating party:

- is the first to cooperate;
- discloses the conduct within a reasonable time frame;
- provides new and meaningful evidence to the authorities;
- cooperates continuously;
- stops participating in the improper conduct; and
- remediates the conduct appropriately and in a timely manner.

Once an authority brings charges against a company, as a general rule, the company may enter into a dialogue to address the authority's concerns.

Some of the factors that should be considered before deciding whether voluntary disclosure is appropriate are:

- potential legal consequences faced by a company after self-reporting and resulting from the settlement (regarding civil, commercial, criminal and administrative matters);
- willingness to cooperate with law enforcement authorities;
- potential penalty reductions and the extent to which a potential settlement agreement could mitigate risks and consequences for the company;
- potential legal and reputational consequences faced by the company's directors, officers and employees; and
- the likelihood that the authorities may otherwise learn of the relevant facts or seek to conduct an investigation.

Conclusion

As has been discussed, internal investigations are an invaluable tool for companies to mitigate risks of potential liability regarding misconduct within the company and are essential for any well-structured compliance programme. In some cases, internal investigations are also necessary or helpful in obtaining a reduction in criminal, civil or administrative penalties. Having a working compliance programme within the company, properly investigating improper conduct and sometimes self-disclosing improper conduct, has proven to be helpful when dealing with authorities.

While all investigations and companies are different, a well-conducted, successful and effective investigation must be performed under a general framework and a basic set of rules. A well-structured investigation will help to prevent

any undesirable surprises and to maintain proper control of relevant conduct and facts being investigated. In contrast, an improper investigation could have disastrous outcomes for a company, even increasing significantly its risk of liability.

From the outset of an investigation, the people in charge must clearly outline the nature and scope of the conduct under review, the potential implications and who should investigate. It is also essential to consider other issues that could have serious implications, which range from the need to retain external counsel, to preserve attorney–client privilege over the investigation, and to determine which specific measures to take to preserve evidence and avoid retaliation.

While this chapter is not an exhaustive analysis of every issue and situation to take into consideration when performing an internal investigation, it should serve as a useful guide for any internal investigation a company carries out to review potential improper conduct.

Lastly, the remediation measures a company adopts after finishing an investigation are essential to mitigate the risk of repetition, including the recurrence of potential liability. This step helps companies to remediate any improper conduct and to learn from its mistakes. An investigation is incomplete without taking this critical step.

For these reasons, and many others, a proper policy addressing improper conduct and ensuring well-conducted investigations is imperative for mitigating potential liability. It is also vital to take appropriate measures to sanction individuals who engage in improper conduct and to enhance relevant controls to prevent improper conduct in the future.

CHAPTER 10

Assessing and Mitigating Compliance Risks in the Transactional Context

Andrew M Levine and Erich O Grosz[1]

Even with the proliferation of anti-corruption laws and enforcement in Latin America, corruption risk need not be a deal-killer. In fact, under the right circumstances, a company tainted by corruption might be a highly attractive investment target. On the other hand, undiagnosed corruption risk can prove catastrophic, quickly undermining financial assumptions that motivated a transaction and exposing an acquiring company to unwanted regulatory and reputational risks.

As discussed in this chapter, anti-corruption and other compliance risks can greatly affect the value and appropriateness of a given transaction. An acquirer may be subject to successor liability for a target's pre-closing wrongdoing, even if unknown to the acquiring company before closing. Likewise, an acquiring company may face regulatory exposure for ongoing and future violations, including for misconduct that may have begun before but continues after closing. Failure to detect a corruption problem before signing also limits an acquirer's strategic options and may result in overpaying for a target. In addition to potential penalties, the true value of an acquired business – once operated in compliance with applicable laws – may prove less than it appeared historically, when corrupt activities artificially inflated its perceived value.

For these reasons, compliance due diligence is a crucial component of transaction planning. Any company engaging in a merger, acquisition or other investment at least should consider the risk that a target has past or current corruption or other compliance issues that may affect the transaction. The level of potential risk and the findings of related due diligence can have a cascading effect. This

1 Andrew M Levine is a partner and Erich O Grosz is a counsel at Debevoise & Plimpton LLP.

includes consideration of the appropriate level of due diligence and the inclusion of relevant contractual provisions. When potential misconduct is identified before signing, an acquirer can attempt to shift some or all of the associated financial responsibility to the seller by adjusting the price or negotiating an indemnity. The acquirer also may pursue other strategies to limit future risk, including coordinated outreach to relevant government authorities.

This chapter addresses compliance-related risks in mergers and acquisitions, focusing in particular on anti-corruption matters given the risk landscape in Latin America. The discussion considers in turn potential liability for pre-transaction misconduct, continuing misconduct and misconduct in a given transaction. The chapter then describes practical steps to mitigate these risks, including pre-transaction due diligence (which has involved some heightened challenges during the global pandemic), inclusion of contractual protections and post-transaction compliance measures.

Compliance risks associated with M&A transactions

In the transactional context, compliance risk falls into three principal categories: (1) pre-acquisition conduct by the target that may result in successor liability for the acquirer (distinct from the predecessor's liability); (2) conduct by the target that continues or recurs post-closing; and (3) conduct related to the transaction itself.

Pre-acquisition conduct

Successor liability arises when an acquirer inherits direct liability for an acquired entity's pre-acquisition conduct. Many countries, including the United States and various countries in Latin America (such as Argentina, Brazil, Colombia and Mexico), recognise the doctrine of successor liability in one form or another.

United States

When a company acquires or merges with another company, the successor generally assumes all liabilities of the predecessor (in contrast to an asset sale, in which liabilities generally do not transfer). Nevertheless, in the Resource Guide to the US Foreign Corrupt Practices Act (the Resource Guide) – first issued in 2012 and then updated in 2020 – the US Department of Justice (US DOJ) and the US Securities and Exchange Commission (US SEC) stated that they often have decided not to take enforcement action against companies that voluntarily disclosed and remediated wrongdoing uncovered in transactional due diligence and cooperated with the US authorities.

In particular, the US DOJ and the US SEC explained that they 'have taken action against successor companies only in limited circumstances, generally in cases involving egregious and sustained violations or where the successor company directly participated in the violations or failed to stop the misconduct from continuing after the acquisition'.[2] Additionally, the US authorities noted, '[s]uccessor liability does not . . . create liability where none existed before', such as 'if an issuer were to acquire a foreign company that was not previously subject to the FCPA's jurisdiction'.[3]

The US DOJ and the US SEC have recognised 'the potential benefits of corporate mergers and acquisitions, particularly when the acquiring entity has a robust compliance program in place', and have encouraged companies to 'conduct pre-acquisition due diligence and improve compliance programs and internal controls after acquisition'. The US DOJ reinforced this message in its 'Evaluation of Corporate Compliance Programs' guidance, revised most recently in March 2023, stating that a 'well-designed compliance program should include comprehensive due diligence of any acquisition targets, as well as a process for timely and orderly integration of the acquired entity into existing compliance program structures and internal controls'.[4]

The Resource Guide added that 'a successor company's voluntary disclosure, appropriate due diligence, and implementation of an effective compliance program may also decrease the likelihood of an enforcement action regarding an acquired company's post-acquisition conduct when pre-acquisition due diligence is not possible'.[5] The result of this prior guidance had been at least a perception of something close to a 'safe harbour' for acquirers that follow it.

The US DOJ also has confirmed that its Corporate Enforcement Policy (the Policy) applies in the transactional context, further underscoring the value of anti-corruption due diligence.[6] Specifically, under the Policy – absent aggravating circumstances such as senior management's involvement in wrongdoing, pervasiveness of misconduct throughout the company or criminal recidivism – there is a presumption that the US DOJ declines prosecution if an acquiring company (1) discovers and then voluntarily and fully self-discloses in a timely

2 US Dep't of Justice [US DOJ] and US Sec. & Exch. Comm'n [US SEC], *A Resource Guide to the U.S. Foreign Corrupt Practices Act* (2020) [Resource Guide], at 30.

3 *id.*, at 29.

4 US DOJ, 'Evaluation of Corporate Compliance Programs' (2023), at 8.

5 Resource Guide, at 31–32.

6 US DOJ, Justice Manual 9-47.120, 'FCPA Corporate Enforcement Policy', https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977.

manner misconduct uncovered at a target, such as through pre-acquisition due diligence or post-acquisition audits and compliance integration efforts, (2) fully cooperates with the US DOJ and (3) works to remediate appropriately, including by implementing in a timely manner an effective compliance programme at the merged or acquired entity.

Because an acquiring company may have limited access to a target's data before closing, the Policy's presumption also applies if the successor uncovers wrongdoing post-acquisition. Additionally, revisions to the Policy in January 2023 make clear that 'even if aggravating circumstances existed as to the acquired entity', the acquiring company nevertheless may be eligible for a declination of prosecution – if the company voluntarily self-discloses 'immediately' upon discovering the misconduct and engages in 'extraordinary' cooperation and remediation.[7]

Argentina

Like the United States, Argentina recognises the doctrine of successor liability. Under Argentine law, in a merger or acquisition, the criminal responsibility or other liability of an acquired legal entity transfers to the resulting legal entity. The law states that criminal liability of the legal entity will 'survive' as long as it continues its business and its employees, customers and suppliers remain substantially the same.[8]

Brazil

Brazilian law defines a 'merger' as an operation whereby one or more companies are absorbed by another, which in turns succeeds to all rights and obligations of the predecessors.[9] 'Consolidation' is defined as an operation whereby two or more corporations unite to form a new corporation, which also succeeds them in their rights and obligations.[10]

With respect to successor liability, the responsibility for current and previous liabilities, both known and unknown, therefore generally follows the legal entity. Under Brazil's Anti-Corruption Law, in the event of a merger or consolidation, the successor company is liable for the payment of fines and for fully remediating the

---

7 *id.*

8 Law No. 27401 (on criminal liability of legal entities), Article 3, http://servicios.infoleg.gob.ar/infolegInternet/anexos/295000-299999/296846/norma.htm.

9 Law No. 6404 of 1976, Article 227, www.cvm.gov.br/export/sites/cvm/subportal_ingles/menu/investors/anexos/Law-6.404-ing.pdf (in English).

10 *id.*, at Article 228.

harm up to the total value of the transferred assets.[11] The Brazilian Administrative Improbity Law of 25 October 2021 (Law No. 14,230/2021), which modifies the existing Administrative Improbity Law (Law No. 8,429/1992), limits the scope of successor liability for acts of improbity in the event of a merger or consolidation to only restitution for damages up to the total value of the transferred assets.[12]

Brazil's Office of the Federal Comptroller General, taking note of this type of risk, has recommended that any company engaging in a merger or acquisition take appropriate pre-transaction measures, including examining company records, conducting research in public records and potentially engaging in a more extensive investigation, to determine whether the target company has engaged in any improper conduct.[13]

With corruption-tainted companies facing the prospect of judicial reorganisation, such as following *Operation Car Wash*, one means of potentially protecting against the risk of successor liability is to acquire assets in the context of a reorganisation. Under Brazilian law, the sale of assets of a company under judicial reorganisation ordinarily will occur free of any burden and without a buyer succeeding to a seller's obligations.[14] Through an amendment effective by congressional override of a presidential veto on 17 March 2021, that protection now expressly covers prior violations of anti-corruption laws.[15] Although Brazilian law before that amendment did not expressly protect a buyer in judicial reorganisation against violations of anti-corruption laws by its predecessors, there was a doctrinal understanding that the spirit of the law was to afford such protection.[16]

---

11 Law No. 12846 of 2013, Article 4, Paragraph 1, www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12846.htm.

12 Law No. 14230 of 2021, Article 8, 8-A, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14230.htm.

13 See Office of the Federal Comptroller General, Integrity Programme: Guidelines for Legal Entities (October 2015).

14 Law No. 11101 of 2005, Article 60, sole paragraph and Article 141(II), www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/lei/l11101.htm.

15 Bill of Law No. 4458 of 2020, enacted as Law No. 14112 of 2020 (modifying Law No. 11101 of 2005, among others), https://www25.senado.leg.br/web/atividade/materias/-/materia/144510

16 See, e.g., Council of Federal Justice, Enunciation No. 104 of 7 June 2019, https://www.cjf.jus.br/cjf/noticias/2019/06-junho/iii-jornada-de-direito-comercial-e-encerrada-no-cjf-com-aprovacao-de-enunciados/copy_of_EnunciadosaprovadosIIIJDCREVISADOS004.pdf.

Colombia

Under Colombian law, a 'merger' is defined as an operation whereby one or more companies dissolve, without liquidation, to be absorbed by another or to create a new one. The absorbing or new company acquires the rights and obligations of the company or companies dissolved when the merger agreement is formalised.[17]

Mexico

Mergers may not take effect in Mexico until three months after the filing of merger documents with the competent registry. During this period, any creditor of the merging companies may legally oppose the merger, which will be suspended until final resolution of the opposition. If the three-month period elapses without opposition, the merger may take place, and the company that subsists or results from a merger will be responsible for the rights and obligations of the merged or absorbed companies.[18]

Conduct that continues post-acquisition

The most significant category of compliance risk in M&A transactions is arguably pre-existing conduct that continues post-acquisition. When this type of conduct occurs, the acquirer is more clearly responsible and less able to protect itself against liability by means of due diligence, contractual protections and post-closing remediation.

For example, Zimmer Biomet agreed in January 2017 to pay more than US$30 million to resolve parallel US DOJ and US SEC investigations involving charges that, after Zimmer Holdings acquired Biomet in 2015, the acquired business continued to 'interact and improperly record transactions with a known prohibited distributor' in Brazil and 'used a third-party customs broker to pay bribes to Mexican customs officials' on behalf of Biomet.[19] Zimmer Biomet's 2017 settlement arose from the US DOJ's determination that Biomet had breached its obligations under its 2012 deferred prosecution agreement (DPA) and that Zimmer, as the acquirer, had inherited these obligations.[20]

---

17 Decree No. 410 of 1971 (Commercial Code of Colombia), Articles 172 and 178, www.secretariasenado.gov.co/senado/basedoc/codigo_comercio.html.

18 Mexico's General Law of Commercial Companies of 1934, Article 224, www.diputados.gob.mx/LeyesBiblio/pdf/144_140618.pdf.

19 Press release, US SEC, 'Biomet Charged With Repeating FCPA Violations' (12 January 2017), https://www.sec.gov/news/pressrelease/2017-8.html.

20 Status Report ¶ 3, *US v. Biomet, Inc.*, No. 12-cr-00080-RBW (D.D.C., 6 June 2016).

According to the US DOJ, despite being aware of prior corruption-related misconduct in Brazil and Mexico, Biomet 'knowingly failed to implement and maintain an adequate system of internal accounting controls designed to detect and prevent bribery by its agents and business partners'.[21] The US DOJ also stated that Biomet failed to conduct appropriate due diligence on its Brazilian distributor and third-party associates in Mexico.

Conduct in connection with the transaction

The final category of risk relates to an acquirer's own conduct in connection with finding, sourcing and completing a particular transaction. For example, hedge fund manager Och-Ziff's DPA with the US DOJ in 2016 related to its payments to an African intermediary in sourcing various investment deals in sub-Saharan Africa.[22]

More broadly, completing a cross-border transaction almost always involves obtaining regulatory approvals, including with respect to competition law, foreign investment law or otherwise. This requires contact with government officials and thereby the risk of corrupt activity.

Addressing compliance risks in M&A transactions

Tailoring the approach to the circumstances of a transaction

Compliance-related risks may be addressed in two phases of an M&A transaction: (1) pre-acquisition, by focusing on risk assessment, due diligence, contractual protections and, in some circumstances, pre-closing remediation; and (2) post-acquisition, by focusing on supplementary due diligence and post-closing remediation and integration. Of course, each transaction is different, and the nature and scope of these steps in each phase will differ based on business realities, resources and other factors.

For example, in the wake of Brazil's *Operation Car Wash*, the need of companies adversely affected by investigations to generate cash – in part to pay penalties imposed as a result of wrongdoing – created the potential for asset and share deals at attractive prices and conditions. These opportunities also highlighted the uncertainty that a target's past (or continued) involvement in a highly publicised corruption scandal brings to a transaction, especially with respect to successor

21 *US v. Zimmer Biomet Holdings, Inc.*, Superseding Information, Cr. No. 12-CR-00080 (D.D.C., 12 January 2017), https://www.justice.gov/opa/press-release/file/925171/download.

22 *US v. Och-Ziff Capital Management Group LLC*, Deferred Prosecution Agreement, Cr. No. 16-516 (E.D.N.Y., 29 September 2016), https://www.justice.gov/opa/file/899306/download.

liability. Given the risk of being held responsible for corruption-related liabilities, interested buyers have increased legal scrutiny of potentially tainted assets, including by means of expansive due diligence, and sometimes have conditioned concluding a deal on final approval of a leniency or plea agreement.[23]

How and when to deal with this type of compliance risk is largely dependent on the size, timing and purpose of a transaction, as well as the parties' respective risk tolerance and leverage. The value of a transaction and its inherent risk profile typically influence the resources an acquirer devotes to pre-acquisition and post-acquisition procedures addressing anti-corruption and other compliance risks.

Similarly, when an investment results in a non-controlling stake, an acquirer may be more limited in what compliance steps can be taken post-acquisition, which highlights the importance in these situations of conducting pre-investment due diligence and obtaining relevant contractual protections. While a minority investment may result in less legal risk to the investor under applicable laws, the risk that an enforcement action will impair the value of the investment remains acute. An accurate assessment of compliance risk is important for determining the extent to which those potential liabilities undercut the attractiveness of a contemplated transaction.

The precise timing of a transaction is often influenced by business realities beyond the sole control of a potential acquirer. Likewise, the scope of due diligence may be limited by applicable law, including securities laws when the target is listed on a public exchange, and practical limits to the availability of certain information, including in a work-from-home environment. While friendly strategic transactions, including mergers, often involve significant pre-acquisition due diligence (and potentially remediation), other types of transactions may move too quickly or be subject to other limits on the ability to assess and protect against corruption or other compliance risks.

Where multiple potential acquirers seek to bid for a target, negotiations may centre on price and result in a 'race to the bottom', in which the bidder least interested in due diligence effectively sets the schedule and access for every other bidder. Alternatively, but somewhat less commonly, a target's desire to attract or keep additional bidders to maintain competitive negotiations on price sometimes can increase the scope of permitted due diligence.

---

23 'Lava Jato levou empresas a vender mais de R$ 100 bilhões em ativos desde 2015', *G1 Globo* (13 October 2017), https://g1.globo.com/economia/negocios/noticia/lava-jato-levou-empresas-a-vender-mais-de-r-100-bilhoes-em-ativos-desde-2015.ghtml.

Finally, companies understandably have different purposes in pursuing M&A transactions or similar investments, such as:

- entering a new market;
- expanding existing market share;
- expanding into different but related product markets (or exploiting existing synergies);
- acquiring technologies or intellectual property with the potential for current or future synergies; and
- seeking investment returns.

Transactions undertaken for the first two purposes lend themselves more easily to integration, expanding what can be done in the post-acquisition phase. Transactions undertaken for the latter two purposes may involve sound business reasons for continuing to operate the target as a separate company, often retaining local management and resulting in a different post-acquisition calculus. The third purpose – expanding into different but related product markets – may land somewhere in between. As a result, the purpose of the transaction and the envisioned post-completion relationship between the acquirer and target should be taken into account throughout the transaction.

Pre-acquisition phase

Risk assessment

In preparing for and planning appropriate due diligence, the potential acquirer should conduct an initial compliance risk assessment of the target, while recognising the limits of what can be known at this early stage. The initial assessment will help to determine the scope of due diligence and the negotiating position with respect to compliance-related provisions in the transaction documentation.

An initial anti-corruption risk assessment should take into account, among other factors, the jurisdictions in which the target operates. A basic tool for measuring the corruption risk associated with relevant jurisdictions is Transparency International's Corruption Perceptions Index (CPI).[24] Although useful, the CPI is based on perceptions and is therefore susceptible to overstating or misunderstanding actual corruption risks. The nature of the rankings also can suggest that some jurisdictions are materially safer than others when, in fact, the differences in their scores are relatively minor. Given that the CPI ranks corruption perception

24 Transparency International, Corruption Perceptions Index, https://www.transparency.org/research/cpi/overview.

by country, it also can miss significant regional differences within a country (for example, in many countries, more remote areas tend to be associated with greater corruption, while the opposite might be true in others).

It is therefore necessary to supplement the CPI with an overview of basic knowledge about the target, including its size, ownership structure, industry, locations of operations (and the types of corrupt practices prevalent in those locations) and government touchpoints. For example, in many jurisdictions, a publicly traded company is likely to have better corporate governance than a private entity. Conversely, companies in certain industries are likely to have more elaborate contacts with government officials and generally face greater anti-corruption risk.

Due diligence

Compliance due diligence is a key component of the process in mergers and acquisitions. Issues uncovered during due diligence not only affect the transaction's price but also reveal areas that the acquirer must consider and remediate to reduce the future risk of liability.

The scope of due diligence may need to be negotiated with the target and may depend on the particulars of the transaction, including its purpose, the risks presented and the ability to conduct additional due diligence in subsequent phases or post-closing. For example, anti-corruption due diligence may include the following:

- a background check on the target and potentially its owners, key members of management and select third parties;
- a review and evaluation of the target's existing compliance programme (if any), both on paper and, to the extent possible, in practice;
- an assessment of touchpoints with government officials, defined broadly to encompass not only elected officials and representatives of government agencies and ministries but also anyone acting on behalf of government-owned or government-controlled entities;
- a review of any payments or other benefits of any kind offered or provided to government officials;
- an analysis of third-party relationships – such as sales agents, distributors and consultants – especially those involved in interactions with government officials; and
- a review of any known, suspected or alleged corruption-related or other compliance issues.

The thoroughness of diligence typically will depend on the target's risk profile, time available for diligence and size of the investment, among other factors. Diligence procedures can include written requests, review of compliance policies and other documents, management discussions (of varying number and depth), on-the-ground interviews (especially challenging during the global pandemic) and possibly testing by a forensic accounting firm of a sample of potentially relevant transactions to assess their legitimacy and support and, more broadly, to understand the control environment.

Even if there is little time for, or availability of, due diligence, basic diligence ideally should provide enough information to determine the importance and scope of contractual representations, warranties and other terms; identify areas for pre-closing and post-closing remediation, if possible; define the basic scope of post-acquisition diligence; and inform negotiations related to price and indemnities.

Regarding anti-corruption risk, it is also important to determine which laws already apply to the target. A target subject to the US Foreign Corrupt Practices Act (FCPA) or other actively enforced anti-corruption laws will be more likely to have a compliance programme and may be more receptive to broader diligence (the absence of either, without a good explanation, may be a red flag). If the target is subject to the FCPA, that circumstance also may inform any decision to self-report potential violations uncovered in due diligence. In transactions potentially subject to US jurisdiction, there also should be consideration of whether to communicate with US regulators about the allocation of responsibility for past matters to the sellers, possibly even before the signing or closing of a transaction.

If the target operates in a high-risk jurisdiction from a corruption perspective and is not subject to the FCPA or other rigorously enforced anti-corruption laws, then the acquirer should be more prepared to encounter corruption-related issues – or at least allegations of such misconduct – during diligence. Indeed, the absence of any such indication or suggestion of improper conduct, while operating in a high-risk area, could be a red flag in itself. Moreover, even if a target is not subject to these laws, a lender financing a given transaction may impose these types of anti-corruption compliance obligations, complicating the due diligence and related analysis.

The failure to conduct thorough due diligence, in addition to exposing the acquirer to legal risk, may prove enormously costly. For example, in 2007, eLandia acquired Latin Node Inc. and discovered only post-acquisition that Latin Node had been making improper payments to government officials in Honduras and

Yemen. Although eLandia disclosed the wrongdoing to the US DOJ and cooperated, Latin Node ultimately pleaded guilty to FCPA violations. eLandia shut down Latin Node and wrote off its investment.[25]

By contrast, in January 2020, Landec Corporation stated publicly that it had made a voluntary disclosure to the US enforcement agencies that a recently acquired business, Yucatan Foods, may have engaged in improper conduct in Mexico beginning prior to the acquisition.[26] Landec's disclosure made clear that it had hired external counsel already to conduct an internal investigation of potential FCPA violations, and that, under the indemnification provisions of its agreement to acquire Yucatan Foods, Landec may be able to recover any related losses from the sellers.

Another example that underscores the importance of pre-acquisition diligence involves Amec Foster Wheeler, relating to conduct by Amec plc before its 2014 acquisition by Foster Wheeler AG and then a 2017 acquisition by John Wood Group PLC (Wood). In 2021, Wood announced coordinated resolutions with authorities from the United States, Brazil and the United Kingdom. These settlements involved payments of approximately US$177 million to resolve charges involving a scheme to bribe Brazilian officials to obtain business in the oil and gas industry.[27] Wood acquired the relevant business several years after the alleged bribery, though also after the commencement of investigations, and ultimately incurred penalties paid by its subsidiaries and continuing obligations under various resolutions.

More encouraging, from the standpoint of acquiring companies, are two recent declinations by US DOJ under the Policy, with both resolutions involving misconduct that took place under prior ownership of an acquired entity. First, in

25 US DOJ, 'Latin Node Inc. Pleads Guilty to Foreign Corrupt Practices Act Violation and Agrees to Pay $2 Million Criminal Fine' (7 April 2009), https://www.justice.gov/opa/pr/latin-node-inc-pleads-guilty-foreign-corrupt-practices-act-violation-and-agrees-pay-2-million.

26 See Landec Corporation, Form 10-Q, dated 2 January 2020, http://ir.landec.com/node/14721/htm.

27 John Wood Group PLC, 'Wood reaches resolution on legacy investigations' (25 June 2021), https://www.woodplc.com/news/latest-press-releases/2021/wood-reaches-resolution-on-legacy-investigations. With respect to the US resolutions, for example, see US DOJ, 'Amec Foster Wheeler Energy Limited Agrees to Pay Over $18 Million to Resolve Charges Related to Bribery Scheme in Brazil' (25 June 2021), https://www.justice.gov/opa/pr/amec-foster-wheeler-energy-limited-agrees-pay-over-18-million-resolve-charges-related-bribery; US SEC, 'SEC Charges Amec Foster Wheeler Limited With FCPA Violations Related to Brazilian Bribery Scheme' (25 June 2021), https://www.sec.gov/news/press-release/2021-112.

March 2022, US DOJ declined prosecution of Jardine Lloyd Thompson (JLT) for a bribery scheme intended to win contracts with a state-owned Ecuadorian surety company.[28] US DOJ credited the voluntary self-disclosure, full cooperation and remediation by JLT, which Marsh & McLennan had acquired after the improper conduct ended. US DOJ also credited the US$29 million that JLT agreed to disgorge to the UK Serious Fraud Office in a parallel resolution related to the same underlying conduct. Similarly, in December 2022, US DOJ declined prosecution of Safran after the company voluntarily disclosed a bribery scheme that it discovered through post-acquisition diligence of a subsidiary and agreed to disgorge US$17.9 million in profits.[29]

Contracting

Transaction documentation often is heavily negotiated. While a purchaser may not have sufficient bargaining power to obtain all the provisions listed below, potential compliance provisions to consider seeking include:

- anti-corruption and other compliance representations and warranties on behalf of the sellers and the target, addressing (for example) compliance with all applicable anti-corruption laws and regulations, expressly referencing those most likely to apply, such as the FCPA and relevant laws of the countries where the transaction is taking place. The less thorough the compliance due diligence, the more thorough these clauses arguably should be, though they are not a replacement for reliable diligence;
- for non-control deals, compliance covenants as to future behaviour and maintenance of an effective compliance programme, as well as rights to undertake a post-completion compliance audit and ongoing information and audit rights. Additional safeguards to consider for non-control deals include veto rights over key decisions and the right to appoint executives in charge of certain core functions (e.g., the general counsel or chief financial officer);
- provisions relating to pre-closing rights, should any corrupt or other problematic activity be found, such as deal termination rights;
- exceptions from confidentiality clauses permitting self-reporting to government authorities (if possible);
- indemnity or escrow provisions (if possible and relevant); and

28 Declination Letter from US DOJ, 'Re: Jardine Lloyd Thompson Group Holdings Ltd.' (18 March 2022), https://www.justice.gov/criminal-fraud/file/1486266/download.

29 Declination Letter from US DOJ, 'Re: Safran S.A.' (21 December 2022), https://www.justice.gov/criminal-fraud/file/1559236/download.

- exit or put rights in the event of post-closing discovery of serious corruption or other compliance issues (if possible).

The case of Abbott Laboratories and Alere illustrates the importance of both robust due diligence and well-defined contractual protections, including termination rights. In February 2016, Abbott announced a US$5.8 billion acquisition of Alere. The following month, Alere disclosed that it had received subpoenas from the US DOJ and the US SEC relating to potential FCPA violations. Abbott expressed concerns about the FCPA inquiry and delays in Alere's public filings and sought to terminate its acquisition agreement. Alere refused, leading to contentious litigation before the parties ultimately agreed to proceed with the transaction for US$500 million less than the originally agreed purchase price.[30]

Similarly, in the wake of *Operation Car Wash* and other anti-corruption enforcement operations, a number of companies have sought to purchase at attractive valuations assets known or believed to be tainted by corruption. In addition to reinforcing the need for thorough due diligence to identify and assess the scope and magnitude of any corruption-related issues, those opportunities illustrate the importance of well-crafted contractual protections. Such provisions include, for example, potentially segregating a portion of the purchase price to cover possible liabilities and expressly allocating responsibility among the parties for known or anticipated liabilities.

Pre-closing remediation

Occasionally, issues are discovered during due diligence, and it is possible to remediate these issues prior to closing or even to carve out parts of the acquisition tainted by corruption.

Pre-closing remediation also can decrease dramatically the likelihood that known misconduct recurs after a transaction closes, leaving the buyer even more clearly exposed.

30 Rhodes, Adam, 'Abbott, Alere Settle Watchdogs' Issues With $5.3B Deal', Law360 (28 September 2017), https://www.law360.com/articles/969249/abbott-alere-settle-watchdogs-issues-with-5-3b-deal.

Post-transaction steps

Deal dynamics often limit the time and ability of acquirers to address fully all relevant compliance risks pre-closing. It is sometimes easier for acquirers in control deals to complete these procedures post-closing, though attention should be paid in contracting to whether the seller will have any trailing obligations.

To the extent not already in place, implementation of a risk-based compliance programme at a target is an important step post-closing. In Opinion Procedure Release 14-02 – formal guidance issued in November 2014 regarding an actual (but anonymised) acquisition – the US DOJ encouraged companies engaging in mergers and acquisitions to 'implement the acquiring company's code of conduct and anti-corruption policies as quickly as practicable' to 'conduct FCPA and other relevant training for the acquired entity's directors and employees, as well as third-party agents and partners' and to 'conduct an FCPA-specific audit of the acquired entity as quickly as practicable'.[31]

A recent US enforcement action reflects the potential consequences of failing to implement appropriate compliance policies and procedures post-closing. In September 2021, international advertising agency WPP plc entered into a US$19 million settlement with the US SEC. WPP was charged with FCPA violations involving failures to ensure that acquired entities in higher-risk markets (including Brazil and Peru) implemented WPP's internal accounting controls and anti-corruption compliance policies, as well as associated failures to address red flags of ongoing misconduct.[32]

In non-control deals, the acquirer may have less leverage with respect to compliance matters, but nevertheless should attempt to obtain undertakings from the target to engage in certain compliance-related steps. Similarly, if the acquirer is buying only part of a company rather than the entire business, the acquisition might not include legal and compliance personnel and resources. In these circumstances, the acquirer should be prepared to hire new personnel and invest in compliance resources promptly post-closing. Without adequate personnel and resources, the acquirer will be unable to take any of the other important steps described above.

---

31 US DOJ, Opinion Procedure Release 14-02 (7 November 2014), https://www.justice.gov/criminal/fraud/fcpa/opinion/2014/14-02.pdf.

32 Press release, US SEC, 'SEC Charges World's Largest Advertising Group with FCPA Violations' (24 September 2021), https://www.sec.gov/news/press-release/2021-191.

Depending on the extent of pre-acquisition due diligence, acquirers also should consider undertaking a post-acquisition compliance review as soon as practicable. Notably, the situation described in Opinion Release 14-02 included particularly thorough due diligence and not an undertaking for any post-acquisition audit.[33] This suggests that there is some discretion – at least from the perspective of the US DOJ – as to whether such a review must be conducted and how extensive it should be. In determining the extent of a review, acquirers should consider whether the target previously was subject to audits under Generally Accepted Accounting Principles, International Financial Reporting Standards or similar standards, and how soon the target will be integrated into the acquirer's own audit programme. Acquirers should document their decision-making as to the timing of any such review or audit.

Perhaps most importantly, an acquirer should rapidly take steps to remediate any wrongdoing uncovered in pre-closing or post-closing diligence. In doing so, an acquirer must consider whether to self-report any issues to relevant enforcement agencies, which is always a fact-based determination warranting careful consideration and consultation with counsel.

Conclusion

We live in an era of aggressive anti-corruption enforcement, including by authorities across Latin America. It has become essential, therefore, in any potential merger, acquisition or similar investment, for acquirers to identify, evaluate and mitigate compliance-related risks at a target company.

In addition to acquiring a target's unknown and undesirable liabilities, a company that does not conduct appropriate compliance due diligence and address any related issues may overpay for an asset. It also can be challenging to extinguish wrongful practices post-transaction, and the cost of implementing or upgrading a compliance programme may be substantial. The strategies summarised in this chapter offer both legal and commercial benefits to companies engaging in mergers, acquisitions or other investments. Although corporate transactions in high-risk markets can present attractive opportunities, investments in assets built on corruption or other improper conduct frequently find themselves on weak foundations, unless the issues are identified and appropriately remedied.

33 *id.*

CHAPTER 11

Why Fresh Perspectives on Tech Solutions are Key to Evolving Data-Driven Compliance Monitoring

Gabriela Paredes, Dheeraj Thimmaiah, Jaime Muñoz and John Sardar[1]

Technology is here to stay. With business and information flowing at a rapid pace, decision-makers must merge their knowledge and experiences with data-driven insights to navigate the vast amount of information within an organisation. Legal and compliance functions are no exception: a data-driven approach is essential to create effective compliance programmes. This is especially relevant as companies face increasing regulatory scrutiny and pressure to comply with a growing list of laws and regulations, making compliance programmes an essential component of modern business operations.

One of the key challenges facing compliance programmes is the sheer volume of data that must be collected, analysed and reported on a regular basis. Traditionally, this has been a time-consuming and labour-intensive process, requiring significant resources and personnel to manage. However, with the rise of new technologies and digital tools, companies are increasingly able to streamline and automate many aspects of their compliance programmes, making them more effective.

---

1 Gabriela Paredes is the compliance manager responsible for Ecuador, Dheeraj Thimmaiah is the global head of compliance analytics, Jaime Muñoz is the global director of ethics and compliance for Latin America and John Sardar is the global head of compliance at Anheuser-Busch InBev.

Anheuser-Busch InBev (AB InBev) is the world's largest brewing company and has a history of over 600 years of beer brewing. The company operates in more than 50 countries and is known for its diverse portfolio of brands, including Budweiser, Corona, Modelo and Stella Artois. As the company continues to expand, the need for effective compliance management has become increasingly important. AB InBev has embraced the use of data-driven compliance monitoring to ensure that the company operates within the legal and ethical framework of each country in which it operates.

Technology is undoubtedly important in the task of staying one step ahead in terms of compliance processes and, at the same time, helps to position the company as a benchmark for regulators in the different countries where it operates. The added value is such that some practices are ahead of what governments are trying to do regarding corruption and money laundering issues. AB InBev is an example of what can be done to help the business be more efficient in controlling expenses and reviewing employees' (and even vendors and suppliers) conduct.

Despite our practices and platforms, such as the many features of BrewRIGHT,[2] the biggest surprise is always how the compliance group makes proper use of something that perhaps should not be part of the day-to-day of lawyers and investigators. In fact, the great step that has been taken with BrewRIGHT's integration into the compliance programme, is that the compliance group is now not only for lawyers, but also technologists (including data privacy experts), auditors, and business administrators. We are privileged to be able to be part of this paradigm change.

This chapter will explore the role of data-driven compliance monitoring in AB InBev's business operations and the impact it has on the company's overall reputation and success.

2 'BrewRIGHT' is a compliance analytics platform developed by Anheuser-Busch InBev. BrewRIGHT is designed to enhance compliance management and proactively monitor for potential risks. With its analytics capabilities, BrewRIGHT allows users to visualise data trends, prioritise potential risks, generate reports, and gain a holistic view of compliance programme elements across different locations. By leveraging machine learning algorithms and data driven insights, the platform aims to enhance efficiency, minimise risks, and maintain high-quality standards for the company. Overall, BrewRIGHT serves as a comprehensive compliance management platform that enables global and regional (zones) compliance teams to maintain consistency, proactively identify and prioritise potential risks and manage limited elements of the compliance programe effectively.

Data-driven compliance monitoring

A definition for data-driven compliance monitoring is as follows: the use of data and technology to monitor and manage the compliance activities of a company. It involves the collection, analysis, and reporting of data to identify and mitigate compliance risks. Compliance analytics can be used in a variety of areas, including but not limited to, anti-bribery and corruption, anti-money laundering, data privacy, and environmental regulations.

Less than 10 years ago, the compliance programmes, both in Latin America and the rest of the world, were 'paper based' programmes focused on ensuring regulatory compliance, training and investigations. This approach, although not mistaken, was limited in scope, since due to its reactive nature, it didn't provide Compliance professionals with the opportunity to predict and subsequently advise the business on the correct course of action. Furthermore, leveraging data to drive insights made it impossible for the compliance function to be perceived as a strategic ally to the business, to reduce overhead costs, collaborate creatively, avoid unnecessary and additional costs to the company.

In the earlier days of compliance programmes, the last point would have been hard to believe, given the former viewpoint of compliance as a 'cost centre' department, which usually needs resources to perform its activities and solve issues that have already happened. These days, with the new data-driven approach that compliance monitoring programmes provide, that scenario is far from reality. Within AB InBev, the ethics and compliance team is launching a Quarterly Ethics & Compliance Assurance report (QECAR) as a product of the BrewRIGHT platform to monitor and assess the effectiveness of compliance programmes across areas of ethics and compliance in countries where it maintains operations. The outcome from the QECAR will be to compare areas of ethics and compliance between geographies to learn and understand areas for improvement and areas of strength. This will also yield cross-learning between geographies and transparency across the board.

This entirely data-driven information can, for instance, make a difference on the final decision between two countries that were being considered as possible choices to conduct a pilot project of a new app that requires users to provide large amounts of personal information. If Country 1 has consistently showed poor results in attendance at training courses regarding the company's data protection policy on all QECAR of the last year, then it's clear that the more suitable option to conduct the pilot will be Country 2. In addition, in the future, this will yield cross-pollinated information within ethics and compliance to provide a holistic view. For example, if there was a harassment case on an employee, and when reviewing the case within the BrewRIGHT investigation dashboard,

additional information on the employee is shown within the investigation dashboard. The additional information is focused on the types of training taken by the employee, any compliance disclosures present for the employee, total number of travel expenses associated to the employee, etc. Leveraging data by cross-pollinate information on different topics will enable optimise decision-making.

Integrating technology

Compliance conferences witness a veritable bazaar of solutions aimed at simplifying generally accepted compliance workflows with greater or lesser benefit to companies themselves. Although not intended to be exhaustive, the following are some opportunities that compliance professionals can evaluate for possible use in integrating technology into their compliance programmes.

Third-party due diligence

One of the most significant benefits of technology for compliance programmes is the ability to conduct more thorough due diligence on third-party vendors and suppliers. In recent years, many countries in Europe have enacted legislation aimed at improving supply chain transparency and reducing the risk of corruption and other unethical practices by extending companies monitoring obligations to all members of their supply chain. For instance, the 2023 Supply Chain Due Diligence Act in Germany requires that large companies (with over 3,000 employees) perform and conduct detailed due diligences on their third-party vendors and contractors to ensure that they comply with social and environmental standards and are not engaging in unethical or illegal behaviour, such as human rights violations.[3] This increases the responsibility on German companies on not only monitoring their own activities, but also the activities of their direct suppliers worldwide and to report any violation found.

While regulations such as this are well-intentioned, they also pose significant challenges for companies that must comply with them. Conducting due diligence on multiple suppliers across various locations and industries can be a daunting and time-consuming task. Fortunately, technology can provide a solution to these challenges. For example, at AB InBev we have developed a machine learning algorithm leveraging a combination of categorical and continuous variables (e.g., GL Accounts, Cost Center, Vendor services, Invoice descriptions), to

3 Business & Human Rights Resource Centre, 'German mandatory human rights due diligence law enters into force', 27 January 2023, https://www.business-humanrights.org/en/latest-news/german-due-diligence-law.

prioritise vendors through risk score for potential touch point vendors (TPV). This data-driven monitoring creates a well-rounded risk-based due diligence process for further validation or review, versus others that pose a significant less risk due to the nature of their operations This action facilitates the general volume of work and the subsequent monitoring of vendors over time, focusing on those with a greater risk profile.

Risk management

In addition to enhancing due diligence processes, technology can also help companies to develop more effective compliance programmes. In 2022, there was a significant increase in enforcement actions by regulatory agencies in both the US and Europe, and this trend is expected to continue in 2023. Companies that can demonstrate strong compliance programmes and effective risk management have a significant advantage in faring better in these investigations. Data-driven compliance programmes, powered by advanced analytics, artificial intelligence (AI) engines and natural language processing (NLP) can be used to automate compliance-related tasks, such as reviewing and analysing legal documents, while also providing companies with insights that enable them to identify and address potential compliance issues before they become major problems, along with providing recommendations for improvement.

An example of ways in which technology can assist with testing and proving the effectiveness of a company's current risk management state is the use of a Quarterly Ethics & Compliance Assurance Reports (QECAR) system.

This soon to be reporting capability, through its standardised format, enables AB InBev companies to measure the progress on the implementation of their ethics and compliance programmes. The QECAR system provides a framework for collecting and reporting data on key compliance metrics, such as training completion rates, compliance disclosures, proactive monitoring, investigation metrics (e.g., substantiation rates) and hotline usage. The data is collected on a frequent basis, aggregated over time and through key performance indicator (KPI) tracks and measures the threshold on acceptance. This enables AB InBev companies to identify trends, areas of strengths, and improvements. Also, by using a standardised reporting system, AB InBev companies can benchmark their performance against other geographies to demonstrate to stakeholders that they are committed to promoting a culture of ethical behaviour and proactively manage its compliance risks.

Automation and process optimisation

Compliance inevitably involves a high degree of process. For example, with a compliance training programme, it's not always easy for an organisation to certify which executives have been trained, which whistleblower reports have been investigated and which vendors have been vetted without tracking and monitoring. Compliance programmes often employ professionals who spend inordinate amounts of time tracking spreadsheets and following up with emails to ensure completion. Approaching this solution tends to be labor-intensive and does not capitalise on the insights that the data generated from such processes offer. In terms of reducing workflow, there is a growing number of platforms that provide basic functionality for following up on tasks to be automated. These platforms not only remove a lot of repetitive email and spreadsheet updating but can generate a lot of insight into risk. Ask yourself whether it is more helpful to send 100 emails asking someone to attend a training event or to identify (and perhaps publicise) which vice presidents lead teams that are consistently ahead of or behind compliance training? Would it not give better insight to establish whether a certain business unit has requested diligence on a meaningfully higher (or lower) number of high-risk vendors? In AB InBev, this year we are removing the mundane workflow in compliance training programme and allowing the compliance team to focus on analyses of trends and patterns that drive meaningful decision-making through digitisation and reporting.

Another example relates to outgoing payments and sanctions. In recent months, there have been various sanctions policies in place in many different countries where AB InBev operates and have different ERP (SAP/SYSPRO) systems in place. Within the BrewRIGHT platform, a new methodology was created called 'alert-based monitoring'. Alert-based monitoring triggers an alert when an event has occurred and, in this case, the event is when an invoice was generated to a payable vendor in Russia or Belarus. The process will alert certain audiences in the company through email, to scrutinise and if need be, stop the invoice from being processed. This methodology (framework) can be leveraged to help compliance officers create alerts based on potential risks to manage and be notified when alerts are triggered.

Content delivery

According to the research site Statista, the number of smartphone subscriptions worldwide in 2023 surpasses 6 billion people. That number is forecast to further grow by several hundred million in the next few years.[4] This increase in

4 Taylor, Petroc, 'Number of smartphone mobile network subscriptions worldwide from 2016 to 2022, with forecasts from 2023 to 2028', 30 March 2023, https://www.statista.com/

connectivity offers new ways for compliance officers to interact with their workforce. The key to managing this change is to ensure that the content generated by a compliance team is fit for mobile, in a timely and relevant fashion. We are not saying that compliance will ever truly compete with a trending YouTube or Tik Tok video, celebrity exploits or the highlights of a top-level sporting event. However, the competition for attention on a smart screen means that compliance officers need to give more thought to how their information is being consumed. Does it make sense for a company policy to be converted to PDF and placed on a mobile-accessible website for employees to comb through the minuscule type? Or should the delivery of these types of documents be tailored and formatted to mobile, where questions can be asked, and relevant answers provided in an easy-to-use, easy-to-read interface?

For instance, companies like global brewer Anheuser-Busch InBev (AB InBev) have invested in chatbots, not just as customer service tools, but also as compliance 'allies' to identify what topics people are searching the most. These chatbots, that can be accessed through computers or smartphones alike, do not only provide insights on what are the topics most searched, to better tailor future trainings, but are also used to provide accessible, anonymous and fast delivered answers to common questions, such as how to access the compliance hotline, without human interference.

For tools such as chatbots and similar platforms, it can be greatly beneficial to rely on the insights provided by Net Promoter Score (NPS) results from user interaction with such platforms. These metrics will generate an understanding of topics such as user rates and satisfaction levels with the platform, that can be crucial to determine in what direction the platform will need to focus on the future to remain relevant and continue to add value to the organisation.

Managing data

A 2022 survey performed by KPMG showed that despite the challenging years that have taken place after the pandemic, US CEOs consider advancing digitisation and connectivity across their businesses as the top operational priority for achieving growth as immediately as the next three years. Furthermore, 74 per cent of them believe they need to act more quickly when shifting investment to digital opportunities and divesting in areas that face digital obsolescence.[5] Even

statistics/330695/number-of-smartphone-users-worldwide.

5 KPMG International, 'KPMG 2022 CEO Outlook', October 2022, https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2022/10/ceo-outlook-report.pdf.

if compliance officers were not traditionally leading this charge, it does not mean that the transformation being undertaken by organisations is generating data sets that can provide operational insights that are invaluable to compliance.

For instance, one of the functionalities of AB InBev's Digital Risk Management platform 'Lighthouse' is to determine the appropriate data management procedures that need to be followed for data collected by the different assets of several business units across the globe. This platform provides several relevant insights, such as a breakdown of digital or data risks identified on a particular asset, intrusion management and potential biases in artificial intelligence (AI), to name a few. These insights prove valuable when later executed and analysed by the digital ethics teams across AB InBev, to better assist the business on a better course of action.

Structured data versus unstructured data

A key question for any data strategy is whether the work product generated by compliance will lend itself to useful data analysis. Implicit in this decision point is whether the company should invest the time and resources necessary to organise data in a structured way.

For those unfamiliar with these terms, unstructured data is data that is not organised in a predefined model. Text in an email, presentation or document is often considered unstructured in nature. In contrast, structured data is data arranged either at creation or shortly thereafter organised into defined buckets and categories. Numbers organised in a spreadsheet or database, with rows and columns, are typically looked at as structured data. Attorneys tend to operate within an unstructured data milieu and prefer to create precise written narratives as part of their work-product that are inherently unstructured. Imagine a narrative compliance entry in a diligence file: 'The vendor is being paid $26,501 to advise on customs clearances in Mozambique.' Structured data inputs tend to require selection of predetermined fields, such as a series of dropdowns or multiple-choice answers. The same information, therefore, could be reduced to four fields to the effect of (1) vendor [being paid] (2) < $30,000> for (3) services with a subcategory of (4) customs. Currently, structured data fields lend themselves to analysis far better – particularly if there is good hygiene around the data – meaning that controls are in place to ensure consistency of input. Unstructured data inputs can express information in a myriad of ways, which can make it difficult to organise them and make meaningful decisions.

Once data is structured, organisations must guarantee that the information also complies with the following requirements:

- Standardisation: meaning there should be consistency in all fields of data input to facilitate analysis and drive consistency and objectivity in the monitoring process.
- Harmonisation and reconciliation: to achieve this, from our own experience, the performance of a particular set of compliance analytics can be radically improved by combining human resources data inputs with the feed from the system in question.
- Accuracy: data accuracy is critical, given that its inaccuracy could lead to flawed conclusions and decisions. Compliance professionals need to take steps to ensure the security and privacy of the data they collect, as well as comply with applicable data protection regulations, such as keeping the data in a secure auditable manner and implement robust data governance policies and procedures in place to prevent tampering or other forms of data manipulation.

Blockchain

Blockchain technology has the potential to revolutionise compliance processes by providing a secure, transparent, and tamper-proof platform for recording and verifying transactions. The decentralised nature of blockchain makes it difficult for people or entities to manipulate or alter the data, providing greater transparency and accountability. This advantage can be used to create an immutable and auditable record of all transactions, making it easier to monitor and enforce regulatory compliance.

It is precisely these transparency and traceability features that lead AB-InBev, in 2020, to launch a project in Europe that used blockchain technology to give consumers clear and direct information regarding each part of the brewing process from barley farmer to brewer. The end-to-end initiative meant that consumers were able to scan a QR code that was displayed on the packages that in turn showed information regarding the farm where such barley was grown. This innovation provided a secure method of ensuring the quality of ingredients and compliance with stipulated processes and standards, and at the same time, enhance consumer's trust on the products and utilising data to improve the farmer's use of natural resources.

It is also worth mentioning that one of the key advantages of blockchain is its potential to automate and streamline many compliance processes. For instance, smart contracts, which are self-executing programmes that run on a blockchain, can be programmed to enforce compliance rules automatically. This could be used, for example, to ensure that a supplier complies with a specific set of environmental or labour standards. If the supplier fails to meet the standards, the smart contract

could automatically impose penalties or terminate the contract. This automation helps organisations to reduce the risk of human error and increase efficiency while maintaining a high level of transparency and accountability.

The advent of unsupervised learning

Many companies are looking at digital transformation and technology initiatives to reduce costs and seek competitive advantages. The continued buzz around AI, particularly the subset focused on machine learning (ML), is therefore an important element to understand and apply when seeking to enhance your compliance monitoring functions. Specifically, the advent of unsupervised machine learning in compliance is particularly relevant given the conspicuous and hidden nature of fraud and corruption schemes. But first, it is important to understand the differences between supervised and unsupervised learning.

In supervised learning, an individual trains a machine using data that is tagged. This means that some records (e.g., transactions) are tagged with the correct answer, such as 'relevant', 'potential bribe' or 'potential fake invoice'. The data can be compared to learning with the supervision of a person who can fine tune and revise the model to find more statistically similar transactions. Unsupervised learning does not need a human to supervise, or train, the model by feeding it known outcomes. Instead, the machine seeks to teach itself to improve the predictive model and work on its own to discover patterns and information that are statistically relevant. Model outputs include the key variables or transactions driving certain outcomes, such as what are the outlier or unusual transactions, which patterns and trends look suspicious and who are the most anomalous vendors or customers, and why. As a result, unsupervised learning algorithms enable more complex processing tasks, across more disparate data sets, as compared to supervised learning.

Both supervised and unsupervised learning are helpful tools for compliance investigations and risk management processes for organisations. In AB InBev's case, the BrewRIGHT platform we leverage both supervised and unsupervised learning to be able to track unusual patterns or trends on invoices and payments, touchpoint vendors and travel expenses, among others. For instance, in the case of travel and expenses, certain transactions can be tagged to determine if such expenses are outside the policy, if they are in violation of legality or cost sensitive (unnecessary expenses). Through continuous tagging and training, the platform searches for similar scenarios that will be considered as potential irregularities. Unsupervised learning is also used on BrewRIGHT, especially for transactions, such as payments, where there are multiple different data sets in areas like commercial and compliance, that need to be analysed to reach a conclusion. For

instance, to measure the risk level of certain payments, unsupervised learning can be helpful to assist in scoring transaction across multiple metrics, such as higher value transaction than usual for that specific vendor or type of service provided, and to compare it with compliance categories, such as if the vendor is a TPV, to get a more accurate risk score.

It is up to each organisation to determine which technique is better suited for different scenarios, however, in our experience, the human factor still brings a real benefit in making sure the models and systems in place to collect data are not flawed and will be conducive to accurate and relevant information being collected. Relying on our own experience with AB InBev's compliance platform 'BrewRIGHT', it is highly recommended that compliance professionals are involved in the implementation of improvements and updates for the AI tools. Despite its elevated potential to learn and analyse different scenarios, often, there are specific country or event period nuances that will require a human to provide feedback for the tool to decrease their error margin, especially at its earlier stages.

Compliance vision of the future

It is undeniable that, despite the challenges that could present turning a former 'paper based' compliance programme into a digital one, the benefits significantly pay off. By leveraging advanced technologies and digital tools, companies can streamline their compliance efforts, reduce costs and improve the overall effectiveness of their programmes, a major competitive advantage in an era of ever-increasing regulatory scrutiny.

Companies, like AB InBev believe that the future of compliance resides in leveraging data-driven compliance monitoring to manage its compliance risks and to ensure that it operates within the legal and ethical framework of each country in which it operates. The use of data-driven compliance monitoring has allowed the company to improve its compliance management, enhance data privacy and make more informed decisions about its compliance efforts. As the company continues to be more organic, data-driven compliance monitoring will play an increasingly important role in ensuring the company's reputation and success.

CHAPTER 12

It Takes Two to Tango: How Forensic Accountants Can Complement Attorneys

Nelson Luis, Raúl Saccani and Fernando Peyretti[1]

Introduction

According to the American Institute of Certified Public Accountants (AICPA), the field of forensic accounting is a branch of accounting that 'generally involve[s] the application of specialised knowledge and investigative skills by a member to collect, analyse and evaluate certain evidential matter and to interpret and communicate findings (forensic services).'[2] Forensic accountants combine accounting, auditing and investigation techniques to assist organisations mitigate its financial and compliance risks, as well as detect and prevent fraud, financial crimes, and other financial misrepresentations.

Broadly speaking, they focus on analysing financial records (such as balance sheets, income statements, tax returns and other accounting and financial records) using a variety of techniques and tools, including data analytic procedures, forensic accounting and behavioral interviewing. They are trained to analyse financial records to detect errors, discrepancies and anomalies that may indicate acts of noncompliance, fraud or other financial misrepresentations. From an education perspective, forensic accountants usually have a degree in accounting, finance, information technology or a related field, and many also hold certifications such as certified public accountant (CPA) or certified fraud examiner (CFE).

---

1 Nelson Luis is a partner and serves as Deloitte's forensic services practice leader for the Spanish Latin America region, and Raúl Saccani and Fernando Peyretti are partners at Deloitte.

2 American Institute of Certified Public Accountants. Forensic & Valuation Services Executive Committee, 'AICPA: Statement on Standards for Forensic Services No. 1' (2019).

One of the key responsibilities of forensic accountants is to detect and investigate instances of financial irregularities. This may be manifested through the analysis of structured data (spreadsheets, databases) and unstructured data (emails, PDFs) to identify suspicious activities and patterns of behaviour that may indicate corruption. For example, they may look for transactions that are not in line with the normal business operations of the organisation, or that are out of line with the normal spending patterns of employees. Generally, forensic accountants combine accounting, auditing and investigative skills to:

- identify internal control weaknesses, implement controls and provide expertise in financial data analysis to assist organisations maintain an effective compliance programme;
- assist in internal investigations through the examination of financial transactions and data to uncover evidence of fraud, embezzlement or other financial crimes; and
- provide valuable insights, expertise and evidence that can assist in solving complex financial disputes and provide expert testimony.

A representative example of how a forensic accountant could provide value is in a fraud investigation involving allegations of embezzlement of funds, which is a common fraud scheme throughout Latin America. Based on a recent study by the Association of Certified Fraud Examiners (ACFE), Latin America has the second highest average fraud loss of any region in the world, after the Eastern Europe and Western/Central Asia region. Moreover, victim organisations based in Latin America had the lowest rate of recovering fraud losses (67 per cent versus the global average of 52 per cent).[3]

Forensic accountants can assist organisations recoup fraud losses during embezzlement matters by investigating where suspect employees may have stolen funds from their employer. The forensic accountant can analyse the company's financial records to identify any suspicious transactions, such as unauthorised transfers of funds or falsified invoices. They can also review bank statements and other financial documents to determine the extent of the fraud and the amount of money that has been stolen. Based on their findings, the forensic accountant can provide a report to the company, its external counsel or law enforcement agency that can be used as evidence in court.

3 Occupational Fraud 2022: A Report to the Nations. Copyright 2022 by the Association of Certified Fraud Examiners, Inc.

Complementing one another

The legal and financial worlds are intertwined and, in many cases, they require collaboration to resolve complex legal disputes, regulatory issues and investigations. Attorneys and forensic accountants are two professions that often work together in these situations. For instance, one way to ensure the effectiveness of a compliance programme is to involve attorneys and forensic accountants. Attorneys are experts in navigating regulatory frameworks, while forensic accountants are financial professionals who specialise in analysing financial data.

While attorneys and forensic accountants have different areas of expertise and focus, both parties complement one another by providing guidance and assistance to their clients that is tailored to the specific needs of an organisation. Involving legal counsel and forensic accountants can provide valuable support and expertise in legal and financial matters, helping to protect an organisation's interests and mitigate risk.

The following table lists examples of where the two disciplines complement one another.

Criteria	Attorney	Forensic accountants
Expertise	Legal experts	Financial experts
Focus areas	Representing clients in trial proceedings and settlement negotiations	Adroit at analysing financial records
Legal advice	Provide legal representation and guidance	Do not provide legal advice
Court appearance	Represent clients in court	Provide expert testimony in legal cases involving financial disputes, fraud or noncompliance matters
Specialisation	Specialise in providing legal guidance	Specialise in accounting and financial matters
Regulatory requirements	Identify and make recommendations on how to comply with regulatory requirements	Assist organisations implement internal controls and perform financial testing to assess compliance with regulatory requirements
Education and training	Typically have law degrees and pass the bar exam	Typically have accounting or finance degrees and hold a certified public accountant or other certifications

Key responsibilities for a forensic accountant

Forensic accountants can play a critical role in assisting organisations and counsels in a variety of ways. While they can support in reactive investigations to identify financial wrongdoing and provide expert testimony, they can also support

in myriad ways to mitigate an organisation's risks. Forensic accountants can assist with due diligence, regulatory compliance, fraud prevention, computer forensic analysis and identifying financial red flags. Within the following section, we provide a brief synopsis into each of these matters, and later in this chapter we will cover three of these areas in more depth.

Proactive matters

Conducting due diligence

It is imperative to conduct due diligence reviews during mergers and acquisitions or other business transactions so management can make sound decisions. Forensic accountants can analyse financial data to identify potential financial risks, assess the accuracy of financial statements and identify potential undisclosed or hidden liabilities. Forensic accountants can provide insight into the financial aspects of the transaction, enabling external counsel to make informed decisions.

Background checks

Forensic accountants ascertain through open-source record searches the credibility of a company and its upper management to safeguard from fraud and future liability (see the 'Third-party risk management' section for expanded details). This is a fraud mitigation and compliance exercise that safeguards organisations from being defrauded due to lack of proper background checks on various stakeholders.

Regulatory compliance

Forensic accountants analyse financial data to identify potential violations of laws and regulations and suggest corrective actions. They can also assist in developing compliance programmes and policies that prevent violations of laws and regulations.

Fraud prevention

Forensic accountants identify potential vulnerabilities in financial systems and internal controls. Implement effective internal controls to prevent financial fraud and other financial crimes. Forensic accountants can also assist in developing policies and procedures that prevent financial fraud, such as internal controls, accounting systems, and employee training programmes. They may provide training to corporate employees on how to detect and report suspicious activity, as well as advise on the implementation of internal controls and other safeguards.

Reactive matters

Investigations

Forensic accountants can assist in gathering and analysing financial data, identifying potential financial irregularities or fraud, and providing insight into the financial aspects of the case. They can also help develop investigative strategies, conduct interviews and assist with evidence collection (see the 'Dealing with electronic evidence in Latin America' section for expanded details). One of the ways that forensic accountants provide support in investigations and compliance matters is the analysis of large data sets to identify patterns and anomalies that may indicate fraudulent activity. Forensic accounting firms have been in the forefront of leveraging different technologies to analyse data efficiently. They can also use data analytics to identify trends and potential areas of non-compliance (see the 'Transaction testing and monitoring' section for expanded details).

Expert testimony and settlement negotiations

Forensic accountants can provide expert testimony in legal proceedings related to financial crimes. They can explain complex financial data and transactions to the judge and jury in a clear and concise manner, making it easier for non-financial experts to understand. They can provide expert opinions on the financial aspects of the case, such as the credibility of financial documents or the extent of financial damages. Additionally, they can assist counsel develop different financial sensitivity analyses that may resourceful during negotiations related to settlements.

Forensic accountants also support organisations in recovering fraud losses in the development of a fidelity fraud claim. Moreover, many organisations possess insurance coverage that may reimburse them for the professional fees that they incur to quantify the loss and prepare reports for use in civil or criminal proceedings. The organisation's insurance carriers may assign an adjuster who will involve forensic accountants as part of their team. Forensic accountants could be valuable members of the team in assisting in claim strategy and development, especially if the organisation does not possess the technical expertise and experience in these claims processes.

Third-party risk management

According to Transparency International's Corruption Perception Index 2022, nearly every country in Latin America ranked below the global average in connection with the perceived level of public sector corruption.[4] A lack of bold, decisive action to fight corruption and strengthen public institutions throughout Latin America is fueling organised criminal activities and other sources of violence. It is also undermining democracy, human rights and development. Furthermore, according to the Global Corruption Barometer for Latin America and the Caribbean 2019, corruption contributes to the erosion of confidence of citizens in the government.[5] Results show that confidence in governments, the courts and police is very low in Latin America and the Caribbean.

Latin America poses a challenging working environment due to its linkage to numerous financial crime risks. Some of these financial crime risks, to name a few, include mineral smuggling, drug trafficking, human trafficking (which also includes migrant smuggling).[6] The development of these financial crime risks is generating illegal cash flows involving money laundering, trade-based money laundering, terrorist financing, corruption and corporate fraud. All of these risks typically involve the use of third parties to perpetrate these crimes.

Third parties can pose risks to organisations, such as bribery and corruption, legal and reputational risks. For instance, analysing the number of US Foreign Corrupt Practices Act (FCPA) matters initiated per year alleging bribery schemes, 89 per cent involved third-party intermediaries, of which 72 per cent of the identified third parties were agents, consultants and brokers.[7] Resultingly, organisations must have a thorough grasp of its third-party population to implement efficient processes to combat these risks. An organisation may have hundreds to thousands of third parties, and the sorts of third parties may be uniform or vary greatly depending on the size and type of business it performs. Year after year, organisations are faced with increased regulations with the consequences of potential sanctions and reputational damage, resulting from the potential improper acts by

4 Corruption Perception Index 2022, January 2023, available at: https://www.transparency.org/en/publications/corruption-perceptions-index-2022.

5 Global Corruption Barometer for Latin America and the Caribbean 2019, September 2019, available at: https://www.transparency.org/en/gcb/latin-america/latin-america-and-the-caribbean-x-edition-2019.

6 Financial Crime in Latin America and the Caribbean: Understanding Country Challenges and Designing Effective Technical Responses, October 2021, available at: https://gfintegrity.org/report/financial-crime-in-latin-america-and-the-caribbean/.

7 Stanford Law School, available at: https://fcpa.stanford.edu/statistics-analytics.html?tab=4.

its third parties. Therefore, it becomes fundamental for organisations to understand its risks associated with third parties and how background checks can protect its business.

Third-party due diligence: key elements to act as regulators are expecting[8]

Conducting due diligence on third parties is considered a leading practice. Laws such as the FCPA, UK Bribery Act, the most recent anti-corruption regulations promulgated in Latin America, and guidance from multinational organisations all advise companies to 'know' their foreign counterparts. While the need is clear, there is no regulatory guidance specifying a minimum level of due diligence to be conducted. This ambiguity can make it tempting for companies to take a cursory swipe at due diligence, review one database, check the 'all-clear' box and enter into a business agreement.

As evidenced by the US Securities and Exchange Commission (SEC) and US Department of Justice (DOJ) judgments in which US companies have been faulted for not performing sufficient due diligence, a cursory approach will no longer suffice. Increasingly, companies are expected to conduct a deeper, more systematic assessment of potential international business agents and partners that involves collecting information from the business partner, verifying the data and following up on identified 'red flags'.

Guidance on due diligence from the US DOJ and other Latin American regulators

The DOJ's Criminal Division published updated guidance in April 2019, June 2020 and March 2023[9] discussing the factors prosecutors should use to determine whether a company under investigation will be considered to have an effective compliance programme. In it, the DOJ reiterates its expectation that an effective compliance programme should apply 'risk-based due diligence to its third-party relationships.' For instance, the DOJ condemned an organisation[10] for employing a Taiwanese consultant and recognising two years later that the consultant lacked any relevant experience in his description. The corporation 'did not conduct

8 International third-party due diligence, Jessica Raskin, 2019, available at: https://www2.deloitte.com/us/en/pages/advisory/articles/international-third-party-due-diligence.html.

9 US Department of Justice Criminal Division Evaluation of Corporate Compliance Programs, available at: https://www.justice.gov/criminal-fraud/compliance.

10 *US v. Alcatel-Lucent Trade Int'l*, A.G.

any formal due diligence regarding the agent's background, qualifications, other employment, or relationships with foreign government officials before or after engaging him,' according to court documents in another case.[11]

Generally, organisations should consider performing the following:

- require the third party to disclose information on a questionnaire;
- use a risk-based approach to verify the information provided and independently identify adverse information; and
- take action on any identified 'red flags' uncovered in the process.

Following the completion of the aforementioned steps, the organisation should strive to divide its third-party population into three categories: high, medium and low risk. High-risk third parties could include those located in a country with a considerable risk of corruption, those having significant interaction with government officials, or those for which red flags have been identified in the due diligence process. Medium-risk third parties could include those that may have less contact with government officials, such as lawyers or accountants, yet are located in a high-risk jurisdiction. And low-risk third parties might include vendors of goods and services that are not acting in an official capacity for the organisation.

The following sections address the steps an organisation could take to categorise its third-party population using a risk-based due diligence approach.

Information disclosure[12]

Organisations should design an effective and thorough questionnaire that asks reasonable questions and puts the third party 'on the record' regarding certain specific issues, containing, at a minimum, the following elements:

- company background, including identifying and registration information;
- ownership and management, including beneficial owners and others able to exercise influence over the entity and any relationships with government officials, as well as identifying information on these individuals;
- disclosure of any civil, criminal, and regulatory matters, to identify a history of issues that may present risk factors;
- compliance with regulatory matters (such as anti-corruption regulations), including questions about knowledge of laws and the company's compliance regime and training efforts;

11 *US v. Titan Corp.*

12 International third-party due diligence, Jessica Raskin, 2019.

- references for individuals knowledgeable about the third party who can provide verification of business relationships and experience; and
- signature of a responsible party who attests to the veracity of the information and agrees to abide by all applicable laws and policies of the company in carrying out its activities.

Background research methodology

Organisations should conduct their background searches considering:

- the type of relationship;
- service criticality;
- the corruption risk associated with the jurisdiction;
- the corruption risk associated with the industry sector;
- interaction with government officials;
- delegation of authority to represent the company;
- a compliance regime;
- unusual payment methods required by the third party;
- known adverse information about the third party; and
- whether the details concerning third parties are important:[13]
    - whether an entity is a 'real' business partner with a business profile and is it experienced in the relevant industry;
    - whether said business partner is owned by company employees, or if other potential conflicts of interest exist;
    - whether the business partner, or its principals, have a track record of bankruptcy or solvency issues that might threaten the supply chain;
    - whether the business partner, or its principals, have a history of serial litigation, criminal problems, counterfeiting, child labour or product safety issues;
    - whether the business partner is associated with organised crime, terrorist groups, money laundering, bribery or corruption; and
    - whether the business partner is located in a country restricted by US law from receiving payment, or whether the vendor appears on sanction and embargo lists such as that of the US Department of the Treasury's Office of Foreign Assets Control (OFAC).

13 International third-party due diligence, Jessica Raskin, 2019.

After executing the due diligence analysis, different types of red flags can be detected, such as in cases where:[14]

- there are links to public officials:
  - a public official recommends, pressures for or demands use of a third party;
  - the third party has connections with a public official or a member of the ruling family, including family, close friendship or current or past joint business interests;
  - the third party is closely linked to a political party, as evidenced by political contributions, public statements, attendance at or hosting of political events;
  - a director or manager of the third party is a former public official;
  - the third party relies heavily on keeping good and close contacts with public officials for its other business interests;
  - the third-party refuses to disclose ownership and beneficial ownership information;
  - there is evidence of a genuine entity;
  - the basic attributes of a functional business are found to be lacking;
  - no pertinent experience or qualifications are evident;
  - excessive fees are charged, usually expressed as a percentage of the contract value, or overcharges for the work performed;
  - there is no evidence of a service or work product;
  - credible office and facilities are found to be lacking;
  - website, internet and social media presence are not commensurate with the nature and size of the third party;
  - the entity is unlisted in business journals, directories or chamber of commerce membership;
  - there is inadequate evidence that the entity has the expertise or technical facilities to deliver; or
  - circumstances of the third-party entity's creation are vague;
- questions arise over the entity's relationship attitude:
  - the third party resists requests for information, reveals as little as it can, is not forthcoming about aspects of its business or claims grounds of market confidentiality;

14 Managing third party risk, Transparency International, June 2016, available at: https://www.transparency.org.uk/publications/managing-third-party-risk-only-as-strong-as-your-weakest-link.

    - the third party resists receiving visits to or tours of its premises and facilities.
    - the third party provides what it expects is required but the information is window-dressing, does not live up to close inspection or has no depth in its application across the activities of the third party, such as an 'off-the-shelf' anti-bribery programme designed to satisfy and deceive the potential client;
    - the third party refuses to commit to implementing an anti-bribery programme equivalent to that of the company;
    - company officials exhibit unusual behaviour, such as not being acquiescent to all requests, being uneasy, nervous, deflecting questions or being unavailable for meetings;
    - the information provided is vague, lacking in detail or irrelevant; or
    - the third party is unclear about the subcontractors it will use, payment arrangements with subcontractors or the role of subcontractors; or
- there are questions about the entity's reputation:
    - there are suggestions that the third party or its officers have links to corrupt activity – this can be references in the media and social media or comments by opinion formers, contractors or contacts of the third party;
    - the third party or its officers have been subject to criticism in media and social media for poor ethical standards or alleged wrongdoing;
    - the third party has been the subject of investigations or sanctions in any field, not just bribery and corruption;
    - there is evidence of unsatisfactory relations or unexplained contract terminations between the third party and its customers and suppliers;
    - there are financial and operational concerns;
    - statutory accounts are late in posting;
    - books and records show inaccurate recording of expenditures;
    - proposed fees and commissions are excessive;
    - contract records show manipulation of the contract terms and specifications once having been awarded; or
    - there is evidence of financial pressures.

Dealing with electronic evidence in Latin America

One of the tools in a forensic accountant's toolkit is the ability to collect and analyse large data sets to search for evidence of wrongdoing. E-discovery is the industry term for forensic practices to collect, preserve and identify data required

for the discovery process or potential use as evidence in legal proceedings. Typically, E-discovery is triggered in reaction to an event or an information governance, compliance, legal or some other strategic initiative, as further described below:

- An event can include an investigation, litigation or response to a regulatory scrutiny.
- A strategic initiative can include migrating to a cloud environment to facilitate remote working, process or a policy realignment to cope with changing data privacy regulations.

During an event such as a bribery and corruption case, the longer it takes to identify and stop any wrongdoing, the more time the perpetrator has to remit improper payments that may expose the organisation to sanctions, penalties and other legal risks. E-discovery encompasses the identification, collection, processing and review of electronic and hard copy data. It facilitates forensic accountants to review different forms of data, regardless of its source, and maintain the proper context and chronology of the issue in question. Organisations may often view the use of e-discovery advanced technologies as using a sledgehammer to crack a nut. However, in Latin America, there are many flexible, agile and reduced-cost approaches that can be taken to derive significant value from the e-discovery process. A consolidated end-to-end managed document review approach is the key to reducing costs while maximising results and alleviating the pressure on the team.

There are two key digital solutions to consider for continuous monitoring to proactively spot corruption related risks:

- Human-created information such as emails, personnel files and financial information. E-discovery technologies have been built to proactively monitor human-created information in real-time. This can include insider trading, collusion and other non-compliant behaviour by plugging into conversations (including, but not limited to, Microsoft Exchange, Office 365, Google Suite, MS Teams, Skype and social media messaging services), and automatically alerting of potential risks.
- Human behaviour, such as employees leaking confidential information. E-discovery technologies also can generate alerts for risky behaviour on the organisation's network or employee's laptop in real-time. This could be the copying of confidential information resulting in an alert and the employee's laptop being automatically blocked pending investigation to mitigate or prevent the leakage of sensitive and confidential information to its competitor.

The global framework for e-discovery

Since 2005, the Electronic Disclosure Reference Model (EDRM)[15] has helped guide organisations through information governance and the discovery process for electronically stored documentation. The EDRM is created and maintained by a community of e-discovery and legal professionals. It helps organisations select e-discovery software tools, determine the skillsets needed to operate those tools, and design documentation that maps the process from end-to-end for legal purposes.

One of the key aspects for Latin American (and other global) law firms to consider is an organisation's need to defensibly delete data under the various data protection laws that vary from one Latin American country to other, including the increase in data sources leaving organisations oblivious to where its data resides.[16]

Challenges of preserving and collecting evidence

Forensic accountants work with attorneys to set expectations regarding deliverables, information to be available and regulations that would affect the procedures. During investigations, the task of collecting relevant evidence, determining whether it meets the requirements to produce documents or provide information – or whether it should otherwise be produced to demonstrate a cooperative stance – is time and resource intensive. It often requires specialised technical knowledge and experience. Information should not be treated as an easily portable product, and personal data protection requirements and other confidentiality restrictions should be carefully considered before information is transferred between jurisdictions or produced to the authorities.

In the first instance, it is good practice to understand the complete picture of information, considering data, documents and human sources (e.g., witnesses). This will better position the team to determine how best to obtain the different types of data, factor in any legal constraints, cross-border and resource planning and capacity, and timing (how, when and where). The chain of custody serves the purpose of demonstrating that the evidence has been duly preserved from any alteration or damage and will therefore retain its value intact. At the time

15 Available at https://edrm.net/edrm-model/current/ Last access April 4th 2023.

16 Linda Sheehan, Navin Sing, Greg Rammego and Clayton Thomopoulos, Key areas for collaboration between lawyers and e-discovery professionals in South Africa, February 2021.

documents or devices enter the forensic accountant's chain of custody, a record should be maintained of the items received or returned. The level of detail required to secure the chain of custody could be agreed with the attorneys.

Types of electronic information usually include, but are not limited to, emails, text messages, instant correspondence and other electronic chats (WhatsApp, Telegram, WeChat, etc.), financial records, internet history, deleted files and temporary files. There are two central debates in Latin America around the use of electronic evidence in the context of an internal investigation. The first relates to the organisation's legal right to review information that could be protected by the employee's constitutional right to privacy. The second relates to the procedures followed to produce that evidence, which ensures its integrity and proper preservation.

It is good practice to define the scope and objectives for the e-discovery procedures, as well as identifying and resolving non-technical issues that may impede the successful completion of the electronic evidence collection process. This generally includes an understanding of the matter being investigated (including the purpose of the investigation, individuals involved), nature and size of the business, legal or regulatory aspects of evidence preservation (in case of intervention by an enforcement authority), and timelines. Additional considerations may include:

- the nature of the IT environment (e.g., operating systems, communications topology, platforms used);
- data privacy considerations that may affect what data can be examined or obtained;
- legal privilege that may affect the evidence collection process;
- the authorisation matrix under which evidence must be acquired (e.g., approval of the system owner, custodian's consent, by court order);
- the intervention of a public notary who certifies and records the procedures performed and the forensic tools that were used should be evaluated to reinforce the process; and
- the nature and location of the evidence, as digital information is likely to reside on various types of media (e.g., hard drives, personal computers, servers, backup tapes and other removable media) or electronic devices (e.g., mobile phones, tablets). Relevant date ranges and other parameters will help define the required dataset.

Preservation of documentation

The basic premise of document preservation is it seeks to collect the data in such a manner that it can later be used as a valid form of evidence. For this purpose, minimal manipulation of the original device is good practice, given that electronic evidence is volatile and may be inadvertently altered or destroyed, therefore the investigator should perform his or her work on a forensic copy of the original dataset. Dates and times arising from both the system and the forensic process, which may be relevant to validating information or testifying in court, should also be recorded.

Simplifying to the extreme the protocol of evidence acquisition (data preservation), we could summarise it as the 'forensic image' of a device that contains information in a way that replicates a bit-by-bit image, or the structure and contents of a storage device such as a hard disk. This operation is essential to analyse the metadata (and the attributes of the files) contained in the devices. The information contained in the second disk (forensic image) is validated with respect to the information contained in the first by applying an algorithm that generates a unique representation of the dataset. Technically, this process is known as 'hashing' and generates a long string of characters that comes to identify that evidence and validate data integrity, ensuring that the information has not been altered.

Incorporating mobile devices in investigations

Data extracted from mobile devices can provide crucial evidence during the execution of an investigation. However, organisations are urged to have proper controls and mechanisms in place to be able to reap the benefits of this critical information. The development of mobile forensics is a subset of digital forensics focused on the recovery of mobile digital evidence in a manner that is acceptable by law.

With the current smartphone penetration in Latin America, as well as the significant dependence on mobile devices in people's daily lives, it is likely that relevant corporate data will be found on both corporate and personal mobile devices. The rising trend of remote and flexible work and bring-your-own-device (BYOD) contributes to blurring the lines between corporate and personal information. These factors make mobile devices an essential data source during investigations, helping piece together the puzzle or identifying the 'smoking gun'.

The use of messaging applications and other off-system communications channels for business purposes is under scrutiny from regulators since the information running through those ephemeral messaging platforms are not captured by

companies' record-keeping systems.[17] On 2 and 3 March 2023, during speeches by Deputy Attorney General (DAG) Lisa Monaco[18] and Assistant Attorney General (AAG) Kenneth A Polite Jr,[19] at the ABA's annual White Collar National Institute in Miami, the US Department of Justice's (DOJ) Criminal Division announced several policy updates consistent with the initiatives announced in the September 2022 Monaco Memorandum. Among others, the DOJ released an updated guidance on the 'Evaluation of Corporate Compliance Programs' (Compliance Evaluation Guidance).[20] Overall, the guidance indicates that company policies on these issues 'should be tailored to the corporation's risk profile and specific business needs and ensure that, as appropriate and to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company.' In his 3 March 2023 speech, AAG Polite Jr tied these issues back to cooperation noting that in an investigation:

> *if a company has not produced communications from . . . third-party messaging applications, our prosecutors will not accept that at face value. They'll ask about the company's ability to access such communications, whether they are stored on corporate devices or servers, as well as applicable privacy and local laws, among other things [and a] company's answers – or lack of answers – may very well affect the offer it receives to resolve criminal liability.*

Corporate policies should include both personal and corporate devices and attention should be on how best to segregate personal and corporate data. For example, with mobile devices, the use of two SIMs or the use of WhatsApp Business for corporate matters could help in segregating business and personal communications. In the same way, storage of personal data on corporate devices should be limited and managed appropriately, such as through restricting access or using access logs. Depending on the jurisdiction and policies in place, the organisation may have the right to obtain all corporate data, including any business

17 Andrew M Levine and Chana Zuckier, The messaging dilemma: grappling with employees' off-system communications, February 3rd 2023, available at: https://www.reuters.com/legal/legalindustry/messaging-dilemma-grappling-with-employees-off-system-communications-2023-02-03/ Last access April 4th 2023.

18 Available at https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-monaco-delivers-remarks-american-bar-association-national Last access 4 April 2023.

19 Available at https://www.justice.gov/opa/speech/assistant-attorney-general-kenneth-polite-jr-delivers-keynote-aba-s-38th-annual-national Last access 4 April 2023.

20 Available at https://www.justice.gov/opa/speech/file/1571911/download Last access April 4th 2023.

communication on personal devices. However, appropriate legal advice should be sought in all cases. This also includes how data may be transferred, based on the applicable laws and regulations.[21]

The stage of data preservation would not imply a violation of the right to privacy, since there is no access to protected content. The processing stage is also low risk, since it consists of a series of procedures on the evidence (de-duplication, indexing, filtering, among others) where there is no access to the contents by the operator. It is in the review stage where the forensic accountants could read the documents and evaluate whether they are relevant. In this instance, a reviewer may eventually access protected content. Keyword searches usually help reviewers focus on those documents that would be potentially relevant and related to a business matter.

How is electronic evidence reviewed?

Once the evidence processing stage is completed (in which deleted documents are restored, duplicates are eliminated, documents are indexed and filtered, among others), the data is uploaded to a review platform, whose function is the review and labelling of evidence. All collected and processed data can be uploaded to the review platform, including paper documents that can be digitised using an OCR technology that allows text to be searched in the same way as electronic data. A review platform should encompass the following.

- Remote access: authorised users access a secure central repository hosting all data sources and case files from any location 24/7 using an internet connection. Highly customisable security rights are desirable. For example, authorised users can control the type of access (e.g., none, read or write) each user has on a document and project level basis.
- Ability to host all data relating to a matter in one secure place: advanced processing technologies are built to create structure across unstructured data to allow investigators to run searches across a variety of data sources in one go. This could include handwritten notes, work diaries, hard copy files, email, enterprise tools, text messages, voicemail, IMs, file sharing, financial platforms, social platforms, lifestyle audit results, background checks and due diligence reports, and other electronic content that may be stored on desktops, laptops, file servers, mainframes, smartphones, employees' home computers or on a variety of other platforms.

21 Cezar Serhal, Natalie Forester and Faiz Ali Khan, 'Blurred lines: Incorporating mobile devices in corporate investigations', Spring 2022, Deloitte Middle East.

- Record all work product in one secure place: advanced review tools provide an automated and detailed document history mechanism that tracks changes made to a document, the person who made them and when the changes were made. Authorised users can be provided with an easy upload document function to integrate all information relating to the matter into the same environment from their desktop.
- Traditional lexicon-based processes, such as, text extraction/OCR, search index and keyword application.
- Advanced searching and keyword refinement using natural language processing, latent semantic indexing and machine learning to expedite the identification of key information within the dataset.
- Ability to visualise email activities to track the flow of information by exploring what emails have been sent to who and determine what email domains have been most accessed.
- Visual timeline builder for the events, issues and key role players linked directly to the reliable evidence.
- Automated translation, transcription and redaction tools to enable the searchability of foreign documents and media as well as protecting sensitive information through user-defined terms.
- Transferable data and insights between multiple cases.

The dataset is filtered by a list of search terms (keywords). Traditionally, this process consisted of listing relevant search terms, such as names, specific keywords, phone numbers, or any other word or phrase that could help identify relevant documents. Those keywords should be tailored based on local jargon. In Latin America, we use corruption related terms in Spanish such as '*cometa*' (Argentinean slang for bribe), '*mordida*' (Mexican), '*corbata*' (Colombian), '*matraca*' (Venezuelan), among others. While this remains a useful method for identifying relevant documents, many vendors now offer other sophisticated document search and review technologies leveraging artificial intelligence and sentiment algorithms, which could detect and relate unique phrases between unstructured data sets, to refine them to the most relevant information.

These review technologies are broadly classified under the name of 'predictive analytics' and provide the building of an intuitive machine learning process and case-specific algorithms on the platform itself. Simply put, once the review is initiated, the platform can learn what the reviewers are searching for and move the most relevant documents to the top of the review batch. This can expedite the identification of the most relevant documents. Other tools include conceptual searches, context searches, metadata searches, relevance classification, clustering,

and early case evaluation. To varying degrees, all these processes allow review teams to quickly focus on relevant documents and potentially identify relevant witnesses.

Transaction testing and monitoring

Regulators in the US and across various jurisdictions around the globe have expressed their expectations that organisation's corporate compliance programmes include a data analytics component. In addition to being able to meet regulatory expectations, organisations are finding that distilling large data sets – such as vendor payments, internal and external communications, social media usage, network activity, customer interactions, cross-border transactions and accounting records – is useful to identify potential anomalies and risky patterns that would be challenging to detect otherwise. Based on a recent global study by the ACFE derived from more than 2,000 real cases of fraud affecting organisations in 133 countries and 23 industries, it underscored the importance of organisations using proactive data analytic techniques. According to the study, when controls were in place using data analytics the average duration of fraud incidents were eight months. However, in cases where no controls were in place, it took 18 months. This represents a 56 per cent faster fraud detection rate when data analytics were in place, ranking it as the number one control to help mitigate fraud.[22]

During the planning stage of an investigation, forensic accountants should discuss with attorneys the types of transactions and analyses that will be completed on the different datasets. The procedures to be carried out (e.g., testing of transactions related to corruption risks) should be discussed and agreed. Based on the forensic accountant's experience, they could develop specific fraud queries based on the nature of the matter and attributes of the records that are analysed from a selection of transactions ('targeted sample'). There are several ways to identify the transaction population that should be analysed as part of an investigation. In general, forensic accountants may consider the allegations first, which may detail some particular transactions of interest or may include larger subsets of data.

In the following section, we explore how forensic accountants leverage data analytics to assist organisations in mitigating one of the highest risk areas – that is, payment remitted to its vendors. Following legal counsel's instructions

22 Occupational Fraud 2022: A Report to the Nations. Copyright 2022 by the Association of Certified Fraud Examiners, Inc.

(so privilege is protected), forensic accountants could conduct an assessment of payments remitted to vendors, which is usually focused on a relevant review period. The procedures to be performed could include:

- aggregate accounts payable and payments data provided by the organisation from the ERP systems covering, as needed, different subsidiaries and business units.
- perform analytical procedures on the accounts payable and payments data and public records searches on select vendors to identify higher-risk transactions and vendors;
- select a risk-based and targeted sample of transactions for further analysis; and
- request and review vouchers and supporting documentation for sampled transactions.

Risk-ranking methodology using analytical and public records searches

The following table lists examples of risk indicators that could be considered when running analytics on an organisation's vendor population.

Priority	Description
Very high	Vendors reported by the Tax Authority as issuers of fake invoices (tax credit blacklist)
Very high	Vendors that are also current or former employees of public entities; this only applies to vendors that are individuals
Very high	Vendors directly linked with public officials (e.g., a public official is a director or shareholder of a vendor)
Very high	Vendors that participated as donors of political campaigns (it only applies to individuals that are vendors and participated as donors of presidential or mid-term elections)
High	Vendors directly related to those reported by the Tax Authority as issuers of fake invoices (for sharing officers, addresses, employees, assets, among others)
High	Vendors that provided services to political campaigns (for advertising, ballot printing, among others)
Medium	Vendors that also have active employment with other entity (it only applies to vendors that are individuals)
Medium	Vendors that, according to tax authorities, are not registered as employers or have fewer than five employees
Medium	Vendors that are (or were) national state contractors or suppliers
Medium	Vendors that are current or former client employees; only applies to vendors that are individuals
Medium	Vendors directly related to client employees (for sharing officers, addresses, employees, assets, among others)

Priority	Description
Low	Vendors with activities reported to tax authorities that are considered as high risk of corruption or money laundering activities
Low	Vendors that have been identified by tax authorities due to potential issues related to tax evasion
Low	Vendors created in the last six months (from their registration in different taxes).
Low	Vendors directly linked to other vendors (for sharing officers, addresses, employees, assets, among others)

Once the vendor population has been defined, based on the risks under investigastion, a selection may be made from various transaction-level risk indicators to run analytics based on the ERP data. The following provides a sample list of potential fraud queries:

- invoices that failed Benford's law of digit frequency distribution;[23]
- invoices over the weekend or a holiday;
- a vendor who submitted multiple invoices with the same date, same amount and different invoice numbers;
- duplicate invoices (same vendor, invoice number, amount, different date);
- one-time vendor by year (one invoice a year);
- payment date before or on invoice date;
- accounts payable processed faster than average (rush payments);
- vendor invoice total increases by 100 per cent per period (one year);
- multiple payments to the same vendor within a specific time period;
- invoices that have vendors with same address but different names;
- invoice amount reduced by 80 per cent from one invoice to next invoice;
- invoice within two days of quarter-end close;
- invoice splitting (same vendor number, date, invoice number, but different amount);
- sequentially numbered invoices;
- invoices with descriptions that contain an FCPA keyword;
- large invoice value;
- payment date before or on invoice date;
- supplier names containing the word 'cash';
- high percentage of round dollar invoices for a vendor;
- payments over the weekend or a holiday;

23 First digit of invoice local currency amounts is identified using Benford's law of uniform distribution to identify outliers for specific digit anomalies.

- invoices with uncommon transaction groupings; and
- invoices with round amounts.

Sampling methodology

A risk-based and targeted sample of high-risk transactions is selected from the ERP data for further analysis, based on the results of the analytical procedures described above. A typical sample selection criteria are listed and categorised as follows:

Category A: transactions hit on transaction risk indicators for 'very high-risk vendors'

Selected high-risk transactions for each of the vendors directly connected to previous corruption cases (per local news articles and other open sources) and vendors that hit on the very high vendor risk indicators as defined above. High-risk transactions refer to the transactions that had high risk scores based on the tests ran against the transaction risk indicators as defined above.

Category B: transactions hit on transaction risk indicators for high-risk vendors

Selected high-risk transactions for each of the vendors that hit on the high vendor risk indicators as defined above.

Category C: transactions hit on transaction risk indicators for medium-risk vendors

Selected high-risk transactions for each of the vendors that hit on the medium vendor risk indicators as defined above.

Category D: transactions hit on transaction risk indicators for low-risk vendors

- Selected high-risk transactions for each of the vendors that hit on the Low vendor risk indicators as defined above.

Category E: top 1 per cent of transactions based on transaction risk indicators for very low-risk vendors

- Selected a targeted sample of transactions that did not hit on a vendor risk indicator but were risk-ranked to be in the top 1 per cent based on transaction risk indicators as defined above.

Category F: other transactions considered for testing purposes

- Selected high-risk transactions from each of the following populations:
  - ERP transactions that hit on transaction risk indicators for vendors NOT included in Categories A-D; and
  - ERP transactions that did not hit on transaction risk indicators for vendors included in Categories A-D.

Usual outcomes of the transaction testing in Latin America, based on the review of sample supporting documentation

Based on the procedures described above, when managing the risk of corruption in Latin America, the following red flags are normally found:

- Payments made to potentially higher risk vendors, including entities alleged to be associated with previous corruption cases and vendors that are included in the tax authorities' blacklists.
- Payments made to vendors that may be linked to government officials or agencies, including 'politically exposed persons' or vendors engaging in political contributions.
- Vendors that appeared to have circumvented the organisation's procurement controls.
- Record retention may appear inconsistent as the nature and quality of support for some transactions is better than others, including:
  - Nature of support: For some transactions, the nature of goods or services provided by the vendors may appear to be inconsistent with their business profile. Although the file may maintain the purchase order, invoice and payment order, there may be limited proof of services as support for these transactions. In other cases, the nature of goods or services provided appeared to be consistent with the vendors' business profile. However, the supporting documentation may be generally limited, and the information provided may not allow the forensic accountants to further evaluate the costs in the context of the broader tender to which the invoices were related.
  - Inconsistent procurement process and determination of price reasonableness: the procurement processes may be inconsistent, and, in many instances, the supporting evidence may not include documentation related to the process for selecting vendors or procedures to obtain competitive bids. Based on the information contained in the supporting documentation packages, some cases will present challenges to determine if the invoiced amounts are reasonable and commensurate with the fair value

for the goods or services provided. Also, transactions sampled may relate to advance payments associated with goods or services, which fair value cannot be determined.

- Insufficient proof of services: same transactions may include copies of work certificates (services) or delivery orders (goods). For some transactions (e.g., marketing-related vendors), the organisation may provide examples of reports evidencing the services rendered; however, there may be instanced where the forensic accountant is unable to tie these reports to individual invoices.
- Method of payment: when the organisation pays most of its vendor's pending invoices by issuing checks, it is quite common that the transaction support may not include documentation (e.g., copies of cancelled checks) that would allow the forensic accountants to confirm the beneficiary or recipient.

Conclusion

The SEC and DOJ's decisions have shown that severe negative effects on an organisation's ability to operate can occur if they do not follow their expectations related to third-party risk management, proper evidence collection methods and leveraging data analytics to efficiently cull through large data sets. While executing these procedures, the legal and financial worlds are intertwined, and in many cases, they require collaboration to resolve complex legal disputes, regulatory issues and investigations. Attorneys and forensic accountants are two professions that can complement one another to achieve optimal results for clients.

Forensic accountants can provide valuable assistance to law firms in a variety of ways, such as by analysing financial data to detect and prevent fraudulent activities, identifying financial red flags and ensuring regulatory compliance. Leveraging their expertise in accounting and investigation techniques, forensic accountants can assist attorneys with due diligence, regulatory compliance, fraud prevention, computer forensic analysis, transaction testing for identifying financial red flags, among others.

The organisations that implement solid integrity programmes, especially in regions that pose high-risk, will be best positioned to mitigate its risks and protect themselves against potential sanctions and fines.

Part III

Legislative and Regulatory Pressure Points

CHAPTER 13

Navigating Competition Rules Throughout the Region

Lorena Pavic, José Pardo, Benjamín Torres and Raimundo Gálvez[1]

How compliance with competition law shapes business activity

In many Latin America jurisdictions, competition regulation has become one of the most relevant legal issues to be considered when doing business, as countries throughout the region have responded to the new challenges that this discipline represents by strengthening their competition policies and institutions.

Therefore, the implementation of an effective competition compliance programme that meets the raising standards that jurisdictions throughout the region have established on this matter has proven to be of the utmost importance when doing business in Latin America.

This chapter aims to provide a general framework of the different aspects that should be considered when designing a competition compliance programme, giving an overview of the legal reforms in this area in recent years, relevant case law in Latin America, and sanctions that companies may face if antitrust infringements are detected, as well as possible connections with other compliance risks.

Legal reforms on competition

In the past decade, the evolution of the different Latin American legal frameworks on competition has involved major reforms, which have significantly raised the standards and requirements for companies regarding a wide range of

1 Lorena Pavic and José Pardo are partners, and Benjamín Torres and Raimundo Gálvez are associates, at Carey.

competition topics. These include exclusionary and exploitative conduct, vertical restraints, commercial policies, membership of trade associations, merger control, interlocking regulation and cartel enforcement, among others.

Chile

In the case of Chile, the most relevant recent reform to Chilean competition law, Decree-Law No. 211 (DL 211), was introduced by Law No. 20945 in 2016. This amendment strengthened the competition authorities' powers to align local regulation with international standards, especially following recommendations by the Organisation for Economic Co-operation and Development regarding Chilean competition policy.[2] The following are the main amendments that have had a significant effect on the competitive performance of undertakings active in the Chilean market:

- the introduction of a per se rule with respect to hardcore cartels, independently of the parties' market power, the intent of the infringer or the anticompetitive effects of the conduct;[3]
- the recriminalisation of cartels, by the establishment of a penal sanction of up to 10 years' imprisonment;[4]
- an increase in the amounts of fines, introducing a flexible maximum up to double the illegal gains obtained (the economic benefit) or up to 30 per cent of the offender's sales during the corresponding period in which the infringement was executed;[5]
- the establishment of additional penalties for cartels, such as absolute temporal disqualification to act as a director or manager in certain types of corporations and companies, and a ban for up to five years on entering into any type of agreement with state bodies (e.g., to be a supplier to the state), or being awarded any public concession;

2 'Chile – Accession Report on Competition Law and Policy'; OECD, 'Assessment of Merger Control in Chile', Report by the OECD Secretariat (2014), http://www.oecd.org/daf/competition/chile-merger-control-2014-en.pdf.

3 This follows the European regulation regarding restrictions by object, Article 101(1) of the Treaty on the Functioning of the European Union.

4 Criminal sanctions to cartels were in force until Law No. 19911 was enacted in 2003; however, they were never actually applied.

5 This replaced the former fixed maximum amount, up to 30,000 tax units (approximately 19.5 billion Chilean pesos) for collusion and 20,000 tax units (approximately 13 billion Chilean pesos) for all other infringements.

- strengthening the leniency programme by the introduction of a criminal liability exemption for the crime of collusion;[6]
- the establishment of a mandatory ex ante control for concentrations whose parties equal or surpass certain turnover thresholds;[7]
- the establishment of the interlocking directorate (i.e., the simultaneous participation of persons in relevant executive positions or as board members in two or more competing companies) as anticompetitive conduct under certain circumstances, and the obligation to report to the National Economic Prosecutor's Office (FNE) the acquisition of a minority stake in a competing company that fulfils certain requirements;[8] and
- the introduction of new powers for the FNE, such as the exclusive initiative of the National Economic Prosecutor for filing criminal lawsuits for collusion crimes, the setting of the turnover thresholds for mandatory merger control and the power to perform market studies, among others.

Peru

In the case of Peru, in 2018, a new Legislative Decree was introduced that incorporated rewards for useful information to detect, investigate and sanction cartels.[9] In addition, Peru's Competition Authority, Indecopi, issued guidelines for public officials in 2018 for combating collusion in public procurement.[10] In June 2020, Indecopi published its Guidelines on Antitrust Compliance Programmes, which seeks to prevent the risks of engaging in anticompetitive conducts. These Guidelines establish the possibility for offending agents to access a reduction benefit of between 5 per cent and 10 per cent of the value of the fine, if the offender has implemented a compliance programme prior to the offence, and

6 Decree-Law No. 211 (DL 211), Article 63.

7 So far, the National Economic Prosecutor's Office (FNE) has analysed approximately 214 concentrations under the mandatory merger control.

8 The FNE submitted its first two claims for alleged interlocking conduct in December 2021. See Case C 436-2021 of the TDLC, FNE's claim against Hernán Büchi Buc and others; and Case C 437-2021 of the TDLC, FNE's claim against Juan Hurtado Vicuña and others. The TDLC has not ruled yet on any of these cases. However, in November 2022 the FNE settled the first of the referred cases with Hernán Büchi Buc and Falabella, including the payment of approximately 1.4 billion Chilean pesos.

9 Supreme-Decree No. 030-2019, Article 26.

10 'Guide to Combating Collusion in Public Procurement' (2018), https://www.indecopi.gob.pe/documents/51771/2961200/Gu%C3%ADa+de+Libre+Competencia+en+Compras+P%C3%BAblicas.

complies with certain requirements, such as the fact that senior management has not participated in the commission of the offence, and the offence is promptly reported to Indecopi, among others.[11]

In December 2020, the Peruvian Congress published Law No. 31112, establishing merger control in Peru, and replacing the prior Emergency Decree No. 013-2019. Later, in March 2021, the Merger Control Law Regulations were officially published and entered into force in June 2021. Previously, the law established mandatory pre-notification and clearance requirements only for vertical or horizontal concentrations occurring in the fields of electricity generation, transmission, or distribution. The new merger control regime applies now to concentrations occurring in all fields of economic activities.

In January 2023, Indecopi published the first version of its Guidelines for the qualification and analysis of concentration operations, which seeks to improve the predictability of the merger control regime. The first section of the Guidelines is dedicated to defining a concentration from a substantive perspective, while the second section describes the procedure under which the Antitrust Commission of Indecopi will determine whether to clear, approve with conditions, or forbid an operation. According to the local agency, the document has been prepared following the technical advice of the World Bank's Global Markets, Competition and Technology Unit, as well as the International Finance Corporation (IFC).

Regarding the implementation of the merger control procedure, the Indecopi recently informed the Peruvian Congress that, to this date, they have received 27 notifications, of which 22 were cleared, one was withdrawn by the applicant, one was conditionally approved due to the risks identified, and three are still under review. Regarding timing, the local agency noted that approved notifications were resolved in an average of 26 working days.

Argentina

In Argentina, a new Competition Law was enacted in 2018, which created a National Competition Authority to replace the Comisión Nacional de Defensa de la Competencia (CNDC). This Law also instituted a new ex ante merger control regime, a leniency programme and increased fines for anticompetitive conduct, among other measures.[12]

---

11 https://www.indecopi.gob.pe/documents/51771/2962929/Gu%C3%ADa+de+Programa+de+Cumplimiento.

12 Greco, Esteban M; Quesada, Lucía; Volujewicz, Federico A, 'Argentina: Competition Authority', The Antitrust Review of the Americas 2019, https://globalcompetitionreview.com/insight/the-antitrust-review-of-the-americas-2019/1173674/argentina-competition-authority.

Mexico

Peru and Argentina are not the only jurisdictions that have made radical institutional changes. In 2013, Mexico also introduced a new competition authority, the Federal Economic Competition Commission (Cofece).[13]

Furthermore, Mexico introduced a Federal Telecommunications Institute, which is exclusively responsible for the broadcasting and telecommunications markets,[14] and a Directorate General of Digital Markets to analyse the development of digital markets and their impact on competition.[15]

Brazil

Regarding Brazil, its competition agency (CADE) issued in 2016 its Guidelines on Competition Compliance Programmes,[16] which address specific measures enterprises must adopt to avoid breaching competition rules and also what CADE expects from an effective antitrust compliance programme. In March 2020, the Brazilian authority also updated its guidelines regarding CADE's antitrust leniency programme.[17]

Ecuador

More recently, in September 2022, the Ecuadorian president signed Executive Decree No. 570, which introduced substantial changes to the Competition Act's Regulation, the most important ones being: (1) the definition of anti-competitive effect is provided, and now the Ecuadorian agency must prove that this effect materialises in an actual or potential harm to the consumer in order to sanction it; (2) when the agency wants to argue that a conduct is by its object anticompetitive, it will have to demonstrate that there is doctrinal consensus on that qualification in addition to several precedents that point this out; and (3) regarding merger control, turnovers will now only consider revenues in the relevant market, which will impact the turnover threshold used to determine whether a merger is mandatorily notifiable.

---

13 Comisión Federal de Competencia Económica. Legal and Regulatory Framework (in Spanish), https://www.cofece.mx/publicaciones/marco-juridico-y-normativo.

14 Instituto Federal de Telecomunicaciones, http://www.ift.org.mx/sites/default/files/contenidogeneral/conocenos/Modificacion_EOIFT_130718.pdf.

15 https://www.eleconomista.com.mx/empresas/Cofece-crea-direccion-para-supervisar-a-los-mercados-digitales-20200707-0041.html.

16 https://cdn.cade.gov.br/portal-ingles/topics/publications/guidelines/compliance-guidelines-final-version.pdf.

17 https://cdn.cade.gov.br/portal-ingles/topics/publications/guidelines/GuidelinesCADEsAntitrustLeniencyProgram.pdf.

Growing competition standards for doing business

All these major reforms in Latin America demonstrate how standards for competition are rising significantly. They pose a challenge for companies, as decisions from Latin American authorities can sometimes be more difficult to predict. Penalties have increased, demands on firms have grown progressively stricter and authorities have become more active and have greater enforcement powers. In Chile, the FNE's growth in terms of experience and consolidation has been manifested in a greater level of success in its actions against cartels, both before the Competition Tribunal (TDLC) and the Supreme Court. In fact, the last rejected FNE claim regarding a cartel case was filed in 2009.[18] The FNE has obtained convictions in the 19 claims filed since then.

This evolution occurs in a regulatory environment in which the legal and institutional frameworks are rather young. This means that the criteria to be applied by the authorities are often still uncertain.[19] Authorities may be overzealous in their investigations, applying conservative standards and in some cases requesting excessive information from the involved parties (e.g., during the process of notification of concentrations). For example, in Chile there are not many rulings on unilateral conduct, the merger control regime is still young, and the first and only case of concerted practices as a hub-and-spoke cartel was sentenced by the Supreme Court in April 2020.[20] This case is especially relevant from the compliance standpoint. One of the most relevant aspects of the TDLC ruling was the recognition of the role of compliance programmes as potential tools for mitigating and even exempting liability. However, the Supreme Court disagreed with the TDLC, establishing that compliance programmes do not constitute exemptions of responsibility, even though the court agreed with the TDLC regarding the possibility that a complete, real and serious programme can be considered when determining the amount of the fine.

In the case of Mexico, there is no jurisprudential practice or regulatory recognition that allows reducing a sanction resulting from the implementation of a compliance programme. However, authorities may consider the cooperation of the offender and its good faith for purposes of grading the sanction.[21]

---

18 Case C 197-2009 of the TDLC, FNE's claim against Abercrombie & Kent SA and others.

19 For example, there are only a few rulings of the TDLC on the standards and requirements for unilateral conduct. Indeed, currently the standards for many forms of unilateral conduct are only established by the FNE in the context of the closing of its investigations.

20 Case C 304-2016 of the TDLC, FNE's claim against Cencosud SA and others.

21 https://centrocompetencia.com/compliance-en-latinoamerica-de-dulce-y-agraz.

In Colombia, although there is no legal framework that regulates compliance programmes, their requirements and their effects, there is an instrument of the Energy and Gas Regulatory Commission, Resolution No. 80 of 2019. This regulation established a mandatory compliance system for regulated parties in the energy and gas sector, which includes compliance with competition regulations.[22] On the other hand, the Colombian Institute of Technical Standards and Certification (INCOTEC), the body in charge of issuing technical standards and certifying quality standards for companies, published in January 2020 a document that defines certain guidelines for the establishment of good practices in the protection of competition. Nonetheless, none of the above-mentioned documents refers to the effects that the adoption of a compliance programme may have when determining the fine to be applied to an agent that has violated competition rules.

The result of all the foregoing is that companies are having difficulties in adapting to changes and new standards. Doing business in Latin America can be complex from a regulatory point of view, so it is vital that undertakings, especially those agents with a relevant market power that participate in risky or complex markets, understand current legislation and compliance standards, and stay up to date with changes as they happen.[23]

Undertakings without full knowledge of competition regulation are at risk of illicit anticompetitive conduct, with the consequent risk of severe sanctions or, on the other hand, inhibit conduct that is actually licit, constraining the competitiveness and success of that conduct.[24] Because of this, competition law compliance and a functioning compliance programme are essential. Executives and employees, especially those in executive and commercial positions, must be properly trained, as this type of measure can help to avoid competition risks and to conduct business legally, with the intent of ensuring that the commercial success of the company is accompanied by a low exposure to competition risks.[25]

Considering the above, issues such as use of the right sources for business intelligence, the risks of accessing commercially sensitive information from competitors, the potential exclusionary or exploitative effects of certain designs of

22 idem.

23 In this regard, and for the effectiveness of a competition compliance programme, the FNE requires companies to always keep an updated analysis of the current and potential competition risks applied to the specific entity and its different business areas or divisions.

24 This happens especially regarding more complex forms of anticompetitive conduct and in those cases where there are unclear standards, such as some cases of abuse of dominance.

25 The training on competition compliance for executives and employees is one of the important requirements requested by both the FNE's Guidelines and the TDLC.

commercial policies, the necessary safeguards when participating in trade associations, the ex ante assessment of concentrations, among other things, are now some of the main priorities in day-to-day business.

Anticompetition risks and requirements in Latin America

The different jurisdictions in Latin America present some differences in the conducts qualified as anticompetitive, particularly in relation to those that are exposed to criminal sanctions.

For example, in Chile, Article 3 of DL 211 provides, generically, that whoever carries out or enters into, individually or collectively, any conduct, act or agreement that 'impedes, restricts or hinders free competition or that tends to produce such effects', will be sanctioned with the measures contemplated therein. This includes, among other things, vertical and horizontal anticompetitive agreements (both unilateral and coordinated), different forms of abuse of dominance and some conduct related to concentrations.

Risks of being involved in anticompetitive conduct in Chile are related to a wide range of severe sanctions that can be imposed by the TDLC both on undertakings – either public or private – and on individuals. The sanctions of general application include:

- the modification or termination of agreements, contracts or arrangements against competition;
- the modification or dissolution of the company, corporation or other legal entity involved in anticompetitive infringements;[26] and
- fines of up to 30 per cent of the offender's sales of the respective product or service line of business during the period in which the infringement was executed, or up to twice the economic benefit received as a result of the infringement. If is not possible to determine either the sales or the economic benefit, the TDLC may impose fines up to a maximum amount equivalent to 60,000 tax units (approximately 39 billion Chilean pesos).[27]

---

26 Regarding the dissolution of companies, corporations or other legal entities, this measure has only been implemented in cartel cases with regards to trade associations, where the latter was used as a vehicle to organise and implement the collusive agreement. As an example, see: (1) Antitrust Court, Case No. 236-2011 of the TDLC, FNE's claim against Agrosuper SA and others, ruling from 25 September 2014 (confirmed by the Supreme Court on its ruling from 29 October 2015); and (2) Supreme Court, Case No. 5609-2015, FNE's claim against the Gynaecologists Trade Association (ruling from 7 January 2016).

27 DL 211, Article 26, Paragraphs (a), (b) and (c).

In Chile, regarding criminal penalties, Article 62 of DL 211 punishes from three years and one day up to 10 years anyone who enters into, organises or executes anticompetitive agreements that fix prices, limit production, allocate market zones or quotas or affect the outcome of public bids, namely hardcore cartels.

In Colombia, criminal sanctions apply only to bid rigging.[28] The Colombian Criminal Code establishes in these cases fines of up to 1,000 legal minimum wages (approximately 1.16 billion Colombian pesos) and between six and 12 years' imprisonment.

In contrast, and similarly to Chile, in Brazil only cartels are considered federal crimes, for which individuals may be prosecuted and sanctioned not only with fines, but also with imprisonment of between two and five years. Brazil's antitrust authority (the Administrative Council for Economic Defence (CADE))[29] has signed a series of cooperation agreements with criminal prosecutors' offices from a number of states, to make criminal prosecutions more effective, and to facilitate the notification of foreign individuals and entities investigated by the agency, the collection of relevant evidence and information, and the possibility of learning new techniques from other agencies.

Beyond Brazil and Chile, individuals in Mexico may also be prosecuted for entering, ordering or executing any contract or arrangement between competitors with certain anticompetitive purposes, facing between five and 10 years' imprisonment.

In the case of Peru, the Criminal Code establishes the crime of 'abuse of economic power' punishing (1) the abuse of dominant position and (2) the participation in practices and agreements restricting competition with the purpose of preventing, restricting or distorting competition. The person who engages in such conduct may be punished with two to six years of imprisonment.

Beyond the legal context, the reality is that the number of detected cartels has increased significantly over time in Latin America. According to a study carried out by the World Bank, in recent decades, out of a total of around 400 cartels discovered in the region, around 250 were detected in Brazil, Chile, Colombia, Mexico and Peru.[30] Another of the study's findings was that most of the sectors affected by cartels are of importance to countries' competitiveness and productivity, such as manufacturing, warehousing and transportation.

---

28 Law No. 1474, Article 410A.

29 Conselho Administrativo de Defesa Econômica.

30 https://documentos.bancomundial.org/es/publication/documents-reports/documentdetail/148021625810668365/fixing-markets-not-prices-policy-options-to-tackle-economic-cartels-in-latin-america-and-the-caribbean.

Safeguards to mitigate competition risks

Regarding recommendations in the context of competition law breaches, first and foremost – as the most serious competition infringement – companies should implement safeguards and measures to avoid any kind of collusive behaviour, certainly including hardcore cartels and any type of concerted practices, including those related to the sharing of commercially sensitive information between competitors, either directly or through third parties (e.g., customers or suppliers).

The previous safeguards are especially important in the context of markets subject to additional factors that could facilitate collusion, such as those characterised by high levels of market concentration, symmetric market shares, product homogeneity, low innovation, price and costs transparency, stability of demand and low levels of entry or exit of competitors, among others.[31]

Regarding collusive behaviour, undertakings should have internal mechanisms to identify and prevent anticompetitive behaviour, for deterring illegal conduct, first, and if applicable, making it possible to apply for leniency. This is the purpose of the existence of leniency programmes. In this respect, in Chile a reliable and effective compliance commitment demands full disclosure of background information to the authorities in the event of identifying a cartel.[32]

Collusive conduct is the most serious competition infringement. In Chile, the Supreme Court imposed fines in cartel cases of more than US$45 million in total in January 2020,[33] and in December 2019, the FNE filed an antitrust claim for collusion against companies active in the market of feed and nutrition for salmon, requesting fines totalling US$70 million.[34] More recently, in October 2021, the FNE filed a claim against Brink's, Prosegur and Loomis, companies active in the securities transportation market, and six of their executives, for, according to the

31 See Ivaldi, Marc; Bruno, Jullien; Rey, Patrick; Seabright, Paul; Tirole, Jean (2003), 'The Economics of Tacit Collusion', Final Report for DG Competition, European Commission, https://ec.europa.eu/competition/mergers/studies_reports/the_economics_of_tacit_collusion_en.pdf.

32 DL 211, Article 39 bis.

33 'Corte Suprema condena a laboratorios Sanderson y Fresenius por colusión en licitaciones públicas de medicamentos con multa total de US$15 millones', FNE (January 2020), https://www.fne.gob.cl/corte-suprema-condena-a-laboratorios-sanderson-y-fresenius-por-colusion-en-licitaciones-publicas-de-medicamentos-con-multa-total-de-us-15-millones; see also https://www.fne.gob.cl/corte-suprema-condena-a-cmpc-y-sca-por-colusion-en-el-mercado-del-papel-tissue.

34 'FNE acusa colusión de empresas productoras de alimentos para salmón y pide multas de US$ 70 millones al TDLC', FNE (December 2019), https://www.fne.gob.cl/fne-acusa-colusion-de-empresas-productoras-de-alimentos-para-salmon-y-pide-multas-de-us-70-millones-al-tdlc.

FNE, having colluded to fix prices for the transportation of securities and related services. In this case, the FNE requested fines up to US$63 million in total. This case is particularly interesting, since it is the first case of collusion charged under the current legal text, that is, after the legal reform to DL 211 of 2016. Thus, if the TDLC and the Supreme Court issue a final conviction, the cartel may be criminally prosecuted in application of the criminal sanctions contemplated for the crime of collusion.[35]

In Brazil, in 2018, CADE initiated 35 new cartel investigations and issued final rulings on 20 cartel cases, imposing approximately US$180 million in fines.[36]

In turn, in Colombia in 2017, the antitrust authority imposed fines of approximately US$68 million on Argos, Cemex and Holcim, and on senior managers of these companies, for participation in a cement price-fixing cartel.

In May 2017, Cofece imposed its highest cartel fine to date (approximately 1.1 billion Mexican pesos) on providers of pension-fund administration services for collusion to set limits on the transfer of savings accounts from one fund to another.[37]

In the case of Costa Rica, the competition agency recently successfully investigated and sanctioned nine companies which colluded in the rice market, agreeing not to buy rice from the national producer until a decree is published establishing a consumer price.[38] In this case, penalties of over 5 billion colones (equivalent to more than US$8 million) in total were established.

Leniency programmes have been established in Latin American countries such as Argentina, Brazil, Chile, Mexico and Peru. These five countries, which form the Latin American Strategic Alliance on Competition, signed a joint

35 See Case C-430-2021 of the TDLC, FNE claim against Brink's, Prosegur and Loomis.

36 'CADE's General Superintendence recommends condemnation of companies for cartel in the national sea salt market', Administration Council for Economic Defence (CADE) (March 2017), http://en.cade.gov.br/press-releases/cade2019s-general-superintendence-recommends-condemnation-of-companies-for-cartel-in-the-national-sea-salt-market.

37 https://www.cofece.mx/wp-content/uploads/2018/02/COFECE-025-2017.pdf.

38 https://centrocompetencia.com/casos-exito-en-mexico-costa-rica-colombia-segun-autoridades.

statement – the Paris Letter[39] – in late 2018 on shared principles that would guide the implementation of their respective leniency regimes, with the objective of tightening the relationship between their competition authorities.[40]

Further, there have been recent jurisdictional changes that have added leniency programmes to competition regimes. For example, in Argentina, a set of amendments were introduced by Law No. 27442 in the context of a new presumption of illegality of hardcore cartels, including the creation of a leniency programme for cartel cases, which offers full immunity to the first firm that confesses to having participated in a cartel, a fine reduction of between 20 per cent and 50 per cent for the second agent, and an extra benefit for those who, not having obtained full immunity in a leniency procedure, disclose or recognise a cartel in a different market. For instance, in November of 2022, the CNDC declared that Alliance, Grisú and Powerlink were guilty of a collusive agreement to fix prices and share the market for discotheque services for student tourism in the city of San Carlos de Bariloche. The CNDC considered that any concerted practice harms competition and fined Alliance and Grisú 150 million Argentinian pesos and 90 million Argentinian pesos, respectively. However, regarding Powerlink, considering that this company was the one that filed the complaint and provided key information for the investigation, and considering the objective of the legislator with the introduction of the leniency programme in Law No. 27422, the CNDC exempted this firm from a fine.

In the case of Peru, Indecopi issued in 2019 its Leniency Programmes Guidelines.[41] In Chile, the FNE published its Internal Guidelines on Leniency in Cartel Cases in 2017,[42] providing more legal certainty to whoever wishes to obtain leniency benefits and limiting the scope of discretion conferred by the law to this agency.

---

39 Alianza Estratégica Latinoamericana en Materia de Libre Competencia, Carta de Paris, www.cade.gov.br/noticias/cade-e-agencias-antitruste-do-chile-argentina-mexico-e-peru-assinam-declaracao-conjunta-com-melhores-praticas-sobre-leniencia/20181130-carta-de-paris-suscrita.pdf.

40 'Competition Agencies from Brazil, Chile, Mexico and Peru Strengthen the Latin American Strategic Alliance for Competition', Cofece (2018), https://www.cofece.mx/wp-content/uploads/2018/09/COFECE-037-2018-English.pdf.

41 https://www.indecopi.gob.pe/documents/51771/4402954/ESP+Lineamientos+del+Programa+de+Recompensas.

42 https://www.fne.gob.cl/wp-content/uploads/2017/10/Guidelines_Leniency_Cartel_Cases.pdf.

In the case of Costa Rica, the Comisión para la Promoción de la Competencia (COPROCOM) published in May 2022 a leniency programme and guide, which seeks to promote transparency and legal certainty in the agency's proceedings. This programme offers the first participant a total exoneration in exchange for its collaboration, and a partial reduction for three other participants. The programme also exempts the first participant in the programme from disqualification from participating in public bids and, if necessary, establishes subsidiary civil liability for the first participant with respect to the other infringers.

Second, with respect to unilateral conduct, dominant undertakings have a special duty of care in what relates to not restricting competition by deteriorating market conditions, exploiting customers or suppliers or by generating foreclosure effects. To determine the appropriate safeguards, it is necessary to analyse not only the market share of the respective company but also to attend to other features of the market, such as the presence of potential natural or regulatory barriers to entry.

In this sense, dominant undertakings should constantly review their commercial policy and their in-force agreements with suppliers and customers, with consideration of the specific market conditions. The aim is to avoid being involved in anticompetitive conduct through vertical restraints such as exclusivity agreements, tying, resale price restrictions, discounts and rebates, among other things.[43]

Third, the mandatory merger control regime requires companies to notify concentrations that equal or exceed the set turnover thresholds. In Chile, this happens under an administrative procedure before the FNE.[44] This proceeding involves a standstill obligation to the parties of the transaction, which prohibits the implementation of the operation before it is cleared by the FNE.[45] This translates into the following requirements:

Companies must notify to the FNE all transactions that meet the substantive requirements to be considered as a concentration operation and equal or surpass the jurisdictional turnover thresholds, before their closing, subject to the risk of incurring an infringement of failure to notify.[46]

---

43 In November 2021, the TDLC convicted Correos de Chile for abusive exclusionary practices (through the application of targeted retroactive rebates). The TDLC sentenced the Chilean state-owned company to pay a fine of 6,000 UTA (approximately US$4.6 million), without imposing additional measures. See Ruling No. 178/2021.

44 DL 211, Title IV.

45 *id.*, at Article 49.

46 *id.*, at Article 48. There have been no FNE claims regarding failure to notify conduct thus far.

The notifying parties cannot implement the transaction before the FNE's clearance, which may consider a variety of actions that constitute early implementation of the concentration (gun jumping).[47]

Notifying parties must comply with the remedies in the case of conditional approvals.

Companies are not allowed to implement the transaction in the case of a prohibition ruling.

In May 2021, the FNE released a new version of the Guidelines for the Analysis of Horizontal Mergers and Acquisitions, which reflect the FNE's experience in years of operation of the mandatory merger control. The main innovations compared to the previous 2012 version include:

- a direct reference to counterfactual assessment as a basic predictive method of merger control;
- a description of the quantitative methodologies used to estimate unilateral risks;
- a section dedicated to the evaluation of mergers in dynamic markets and digital platforms;
- greater detail in coordinated risk hypotheses; and
- an explanation of the criteria used to evaluate the failing firm defence, among other topics.

Also, the FNE published an Instruction on Pre-notifications, which establishes a formal stage available to companies and economic agents to resolve substantive and procedural doubts for future notifications in the context of the merger control.[48]

In November 2021, the FNE filed a claim before the TDLC against a company active in the maritime transport service, for the acquisition of a competing vessel (Navimag Carga S.A.). This transaction did not exceed the mandatory notification thresholds at the time it was completed, so it was not subject to mandatory control. However, the FNE considered that such acquisition implied the monopolisation by the acquirer of the bidirectional route Puerto Montt–Chacabuco, which could constitute an infringement of Article 3, Paragraph 1 of DL 211 (i.e., a general anticompetitive offence). The FNE requested the imposition of fines and

47 *id.*, at Article 49. There has been only one gun-jumping case brought to the TDLC, regarding early implementation of a transaction. The concentration was approved by the FNE after its closure, and it was finally settled before the TDLC between the FNE and the notifying parties. Case C 346-18 of the TDLC, FNE's claim against Minerva SA and others.

48 https://www.fne.gob.cl/en/fne-actualiza-y-fortalece-regimen-de-control-de-operaciones-de-concentracion-con-nueva-guia-e-instructivo/.

a number of additional measures against the acquiring company.[49] The FNE and Navimag Carga S.A. settled the case before the TDLC, as the company agreed to pay UTA 500 (approximately US$460,000) and adopt several other measures.

Concerning merger control legislation, Argentina, Brazil, Chile, Colombia, Costa Rica, Ecuador, Mexico, Paraguay, Uruguay and [50] Peru, among others, have merger control regimes.

In April 2021, Ecuador established a 'fast-track' merger control procedure as a result of the covid-19 crisis.[51] Comprising a 25-day analysis of the concentration, it allowed the competition authority to reduce their procedure timing by 20 per cent compared with the previous year.

Most of these merger control jurisdictions are modelled on a mandatory filing if the operation surpasses certain jurisdictional thresholds, usually based on individual or combined turnovers, though some of them, such as Argentina, Colombia, Costa Rica and Mexico, also include a de minimis asset threshold.

In this context, in the past few years, Latin American authorities have issued different documents and guidelines, making advances in areas of competition law not previously explored by other authorities in the region. A good example is the Guidelines for the Analysis of Previous Consummation of Merger Transactions published in Brazil by CADE, which details concepts, procedures and penalties for gun jumping, serving as a reference for the rest of the region.[52]

An interesting case in this regard is Costa Rica, the jurisdiction in which the COPROCOM, the local competition agency, imposed a fine of $130 million colones (equivalent to more than US$219,000) in August 2022 on a large pharmaceutical company for failing to report the purchase of six pharmacies over the years, a relevant precedent in gun-jumping matters for local companies.

Another example is Mexico. Cofece published in April 2021 an update of its Merger Notification Guidelines, which seeks to provide greater certainty to economic agents regarding the Commission's treatment of merger analysis. Specifically, the Guide establishes those elements that Cofece will consider in its merger analysis in order to clarify: (1) its treatment of collaboration agreements between economic agents; (2) issues relating to the calculation of notification

49 See Case C 433-2021 of the TDLC, FNE's claim against Navimag Carga S.A.

50 Supreme-Decree No. 030-2019 (Peru), Article 26.

51 SCPM, Resolution No. SCPM-DS-2020-019, https://res.cloudinary.com/gcr-usa/image/upload/v1587675683/RESOLUCI%C3%93N-SCPM-DS-2020-19_1_xr5ntg.pdf.

52 Guidelines for the Analysis of Previous Consummation of Merger Transactions, CADE (2016), www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/guias_do_Cade/guideline-gun-jumping-september.pdf.

thresholds; (3) who is required to notify a concentration involving multiple purchasers; and (4) what information must be submitted to raise the failing firm defence.

Possible connections between anticompetition and other compliance risks

Several types of anticompetitive conduct relate closely to other compliance risks. In many cases, other types of responsibilities may be the consequence of the same facts, such as corporate responsibility, or harm to other groups of individuals may also give rise to penalties, such as consumers or employees. Competition law may also include different types of penalties other than those of an economic nature.

Competition compliance and criminal responsibility

One of the main risks associated with anticompetitive conduct is that derived from criminal responsibility established in the law. In Chile, collusion was punished with imprisonment until 2003, when Law No. 19911 came into force and removed this type of penalty; however, in 2016, it was reincorporated into DL 211 by the amendment introduced by Law No. 20945.[53]

Currently, Article 62 of DL 211 establishes imprisonment sanctions, ranging from three years and one day up to 10 years for those who participate in crimes of collusion. The Law also establishes that, in the event that alternative sanctions may apply, they can only be requested after the convicted person has been imprisoned for at least a year. So far, this sanction has not been applied because there have been no cases regarding events that occurred after the amendment came into force.

Several Latin American countries have imposed criminal sanctions against price fixing cartels. In this regard, Colombia's Criminal Code establishes as a criminal breach bid-rigging in public procurement procedures,[54] and sanctions it with six to 12 years of imprisonment. In a similar sense, Peru's Criminal Code also considers collusive agreements as a crime in the context of public tender procedures.[55] Individuals in Mexico may also be prosecuted for entering, ordering or executing any contract or arrangement between competitors with certain anticompetitive purposes, facing between five and 10 years' imprisonment.

53 *id.*, at Article 62.

54 Article 410-A.

55 Article 384.

Finally, the Economic Crimes Act of Brazil considers collusive behaviours as a crime and sanctions such conduct with two to five years of imprisonment.[56]

Competition compliance and consumer protection

As well as criminal responsibility, anticompetitive conduct may affect consumers, who may be entitled to compensation. In Chile, Article 30 of DL 211 establishes that, once the TDLC has issued a final and binding judgment, later actions may be prosecuted either through a compensation action before the TDLC, or through the procedure for collective actions before a civil court.

This type of civil responsibility is widely contemplated across the region. For example, in the case of Mexico, Article 134 of the Federal Law of Economic Competition establishes that those who have suffered damages as a result of a monopolistic practices or an unlawful concentration may file legal actions in defence of their rights before the courts specialised in antitrust matters. As in the case of Chile, the obligation to pay for this type of damages has its direct antecedent in the declaration of the unlawfulness of such conduct by the competent court, regardless of the fact that the plaintiff has to prove the damage and causation between the damage and the anticompetitive conduct.

Likewise, in Peru, Article 52 of the Peruvian Law for the Repression of Anticompetitive Conduct enables any person who has suffered damages as a consequence of an anticompetitive conduct declared by administrative resolution to file a civil claim for damages before the Judicial Power. The article also empowers the Indecopi to initiate class actions in defense of affected consumers. On 17 May 2021, Indecopi published a guide on compensation for damages to consumers for anticompetitive behaviour,[57] which seeks to complement and delineate the criteria for the application of such rule.

Competition compliance and personal responsibility of board members

Another of the main risks alongside those of competition relates to the responsibility of board members within a company. In Chile, Law No. 18046 of Corporations (LSA) sets forth the right of board members to be provided with sufficient, true and timely information about the essential data of the company, as well as the legal obligation of executing their charge with the due diligence that the duty of being properly informed implies. In fact, in Article 78 of the LSA, it is established that for board members to execute an adequate

56 Article 4, Law 8137/1990.

57 https://cdn.www.gob.pe/uploads/document/file/1898027/Lineamientos%20CLC%20sobre%20demandas%20resarcitorias%20VF%20%281%29%20%281%29.pdf.pdf

administration, it is their duty to acquire sufficient information. Regarding this, the Superintendency of Securities and Insurance (SVS)[58] has sanctioned board members for not executing their right to be informed, owing to the fiduciary nature of their position.

There have been cases in which this standard has resulted in civil responsibilities for board members and other senior executives. In the FASA cartel case, the SVS penalised the president, executives and board members of Farmacias Ahumada during the investigated time period with a fine of 300 Unidad de Fomento (6.2 million Chilean pesos at the time) to each one, for not having duly exercised their legal right to be informed, and in a timely manner, as they should have done by virtue of the background information they had, both public and internal, in relation to a cartel case in which the company was involved.[59]

Competition compliance and anti-corruption regulation

Additionally, the same facts constituting anticompetitive infringements could also imply infringements of the anti-corruption regulation, especially any conduct relating to collusive behaviour (bid-rigging) related to public procurement markets. This relationship between the regulations can produce the risk that legal provisions against corruption undermine the effectiveness of leniency programmes against bid rigging in public procurement.[60]

Competition compliance and labour law

Labour laws can both aid and be in dispute with competition rules. These two areas of corporate compliance go hand in hand, and through fostering a holistic approach to corporate governance, companies can assist in better compliance to competition rules through their employees.

For example, by creating bonuses and other incentives for employee performance regarding compliance programmes within the company, employers incentivise a culture of compliance. Similarly, through the existence of expedited channels for reporting anticompetitive conduct supported by a bounty system (i.e., the creation of rewards for whistleblowers), companies may be able to increase the rate of detection of anticompetitive conduct.

---

58 Superintendencia de Valores y Seguros.

59 Case C 184-2008 of the TDLC, FNE's claim against Farmacias Ahumada SA and others.

60 Luz, Reinaldo; Spagnolo, Giancarlo (2016), 'Leniency, Collusion, Corruption, and Whistleblowing', Working paper to Stockholm Institute of Transition Economics.

In other types of measures, companies may adopt 'negative' incentives for employees to respect compliance programmes, such as certain internal consequences, which might include the recalling of bonuses, civil damage claims by the employer and the loss of reputation.

All these measures must be stated within a company's internal rules; it is also recommended that they are included in employees' contracts.

On the other hand, as mentioned, labour laws can be in direct conflict with competition rules and proceedings. One of the clearest cases is when the need to investigate possible anticompetitive conduct by one or more employees clashes with the employees' right to privacy. While different legislation can have different thresholds regarding what is considered private within the workplace, there is a general consensus that emails, computers and work phones may be monitored; however, it must be explicitly and clearly stated prior to any such monitoring being carried out, and be non-discriminatory (i.e., all employees must be subject to this a priori monitoring).

In Chile, both the FNE and the TDLC recommend that the review of email inboxes is the preferred method of monitoring the effectiveness of compliance programmes. Meanwhile, labour case law states that this kind of screening must be stated in a company's internal rules and be applied as a general, preventive and aleatory measure. The specific monitoring of an employee's email inbox, especially with investigative intent, in most cases is considered strictly prohibited except for when an employee consents to such an examination.

Problems arise when possible anticompetition behaviour by an employee is reported, as a company complying strictly with labour laws might not be able to investigate a possible infringement of competition rules.

There is also a growing interest among competition authorities in three types of conduct in which the affected good is the labour market: no-poach agreements, namely, agreements not to hire employees of competitors; wage-fixing agreements, which are agreements on salaries; and the exchange of information on prices and profits and other relevant variables.

Elements of an effective competition compliance programme

In general, legislation in Latin American jurisdictions does not provide specific requirements regarding competition compliance programmes, being a subject that has had to be developed by case law and by the guidelines of the different competition agencies in the region on this matter.

In the case of Chile, case law under both the FNE and the TDLC has established certain standards that work as indicators, or minimum requirements, for a programme to be effective, notwithstanding that its effectiveness will ultimately depend on how commercial policies are implemented and the particularities of each case.

Another issue relates to the effects of compliance programmes in the field of corporate liability. The TDLC has reduced fines based on the conscientious implementation of a compliance programme, and even raised the possibility of exemptions from liability, which radically differs from practice in the European Union.[61] However, the Supreme Court disagreed with the TDLC on that case, holding that compliance programmes do not constitute exemptions of responsibility, even though the court agreed with the TDLC regarding the possibility that a complete, real and serious programme can be considered when determining the amount of the fine.

Below are the requirements of an effective anticompetition compliance programme, according to FNE's and TDLC's standards. These criteria are not new to the region, and other countries have applied similar requirements for compliance programmes, including Peru,[62] Mexico,[63] Colombia[64] and Brazil.[65]

61 Case C 304-2016 of the TDLC, FNE's claim against Cencosud SA and others.

62 Guía de Programas de Cumplimiento de las Normas de Libre Competencia (Proyecto), Indecopi (September 2019), https://www.indecopi.gob.pe/documents/51771/2962929/Guía+de+Programa+de+Cumplimiento.

63 Recomendaciones para el cumplimiento de la Ley Federal de Competencia Económica dirigidas al sector privado, Cofece (August 2015), https://www.cofece.mx/cofece/images/Documentos_Micrositios/RecomendacionesCumplimentosLFCE_021215.pd>.

64 'Icontec Pretende Establecer Buenas Prácticas de Protección para la Libre Competencia', Fenalco, www.fenalco.com.co/gesti%C3%B3n-jur%C3%ADdica/icontec-pretende-establecer-buenas-pr%C3%A1cticas-de-protecci%C3%B3n-para-la-libre.

65 'Guia para Programas de Compliance', CADE (January 2016), www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/guias_do_Cade/guia-compliance-versao-oficial.pdf.

A good example: FNE's Guidelines on Competition Compliance Programmes

In 2012, the FNE published its Guidelines on Competition Compliance Programmes with the aim of encouraging economic agents to develop internal mechanisms that seek to prevent and detect anticompetitive conduct, by providing some of the markers that the FNE considers a competition compliance programme should contain.[66]

These Guidelines can be seen as the FNE's response to the then increasing trend by competition authorities, on an international level, of aiding the prevention and deterrence of anticompetitive conduct by encouraging the implementation of competition compliance programmes. The FNE's Guidelines have clearly been influenced by earlier guides and documents issued by other competition authorities. For example, the European Commission's Compliance Matters includes many of the same compliance measures: identification of risks, involving senior executives in the compliance policy, the establishment of reporting channels, permanently updating the compliance policy, monitoring and auditing. In September 2022, the FNE launched a public consultation procedure to update their Guidelines on Competition Compliance Programmes. An updated version of these Guidelines has not been published by the FNE yet.

Moreover, the FNE's Internal Guidelines for the Request of Fines from 2019 recognise the possibility of considering the existence of a robust compliance programme to reduce the amount of the fine to be requested to the TDLC, as long as several copulative requirements are met.

Furthermore, Chilean authorities have explicitly recognised the influence of the OECD's Policy Roundtable on Promoting Compliance with Competition Law Policy of 2011. In the summary document of that roundtable, the Chilean representative is quoted as saying: 'The FNE is currently in the process of evaluating what approach to take regarding these programmes, so this Roundtable is very timely for supporting our decision-making.' We can now see some clear correlation between the OECD's document and the FNE's guide (e.g., the evaluation of risks, commitment of the company, monitoring, audits, secure reporting channels, permanent assessment of compliance and use of incentives to promote compliance, among other things).

66 'Programas de Cumplimiento de la Normativa de Libre Competencia', FNE (June 2012), https://www.fne.gob.cl/wp-content/uploads/2012/06/Programas-de-Cumplimiento.pdf.

Other documents appearing around the same time, such as the US Department of Justice's FCPA Resource Guide, and later documents set out many of the same measures already mentioned multiple times.[67] This shows that most competition authorities agree about the minimum measures and characteristics of a competition compliance programme, with certain minimal differences between them depending on the specific characteristics of each jurisdiction.

For instance, in November of 2022, the Colombian antitrust authority, the Superintendencia de Industria y Comercio (SIC), issued the Guidelines for the Implementation of Compliance Programmes in Competition Law, through which it intends to express its intention to foster a national compliance culture. Through said Guidelines, the SIC established the importance of creating a competition law compliance programme, the minimum elements it should have, and the most important guidelines for its implementation.

For the FNE, a competition compliance programme must meet at least the following four conjunctive essential requirements:

A real commitment to comply with competition law, which must be transmitted through the actions of each agent, requiring that both internal and external policies are consistent with competition law.

The identification of current and potential competition risks applied to the specific entity and its different business areas or divisions, especially by recognising weak areas where those risks will probably occur. This requirement is especially important, since it will determine the characteristics of the company's compliance programme in accordance with the corresponding level and areas of risk and the characteristics of the market in which the firm operates. For these purposes, the FNE recommends a detailed study by experts in competition, which should be reviewed at regular intervals or in the event of any relevant change of circumstances.

The existence of internal structures and procedures in accordance with competition law and consistent with it, which relates closely to the first requirement. Some manifestations of a proper commitment would be, for instance, (1) incentives, compensation, bonuses and other benefits to workers who comply with competition law, (2) the establishment of appropriate communication channels for reporting possible anticompetitive conduct, (3) the establishment of a separate

67 For example, 'Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations', US Department of Justice, Antitrust Division (July 2019), https://www.justice.gov/atr/page/file/1182001/download.

and independent pricing area that is distinct from the commercial area, and (4) the designation of a person in charge of the company's competition compliance programme (compliance officer).

The active participation of senior executives and board members of the company in the implementation and development of a compliance programme. All the previous requirements can only be achieved if all individuals within the company, especially those in senior positions, show the importance of compliance with competition law. Finally, the compliance officer should have full autonomy and independence within the company (e.g., responding directly to the board of directors and exhibiting precisely defined grounds for removal).

Additionally, the FNE mentions specific elements that compliance programmes can include to achieve a greater degree of effectiveness. The FNE describes them as having a 'pyramidal' structure: as the measures are progressively more intense and the cost is greater, their effectiveness also increases. The Guidelines establish five distinct elements, in increasing order: (1) manual; (2) training; (3) monitoring; (4) audits; and (5) disciplinary measures.

First, a competition compliance programme must have at the very least, a written manual that clearly and comprehensively explains the main aspects of competition law, potential risks, types of anticompetitive conduct, means of reporting this conduct, the person in charge of the programme, among other things. This manual must be available to all company personnel and must be permanently and easily accessible by all employees.

Second, training regarding proper compliance with the programme and the manual must be carried out within the company, ideally by an external competition expert. This training will encompass practical explanation of the extent of the programme, the internal competition policies of the agents and the internal procedures of the company regarding compliance with competition rules. Face-to-face training can be complemented with online courses or training, and its frequency will depend on the specific needs of the company. It is important to carry them out on a regular and updated basis, as competition is a very dynamic discipline, where doctrine and case law are constantly evolving.

As third and fourth measures, the FNE mentions monitoring and audits. Both are mechanisms that allow the identification of the level of effectiveness of the compliance programme, and both can be done by internal and external professionals. The FNE recommends that an audit is carried out each time there is a report of a possible infraction, and to carry out general preventive audits.

Finally, the FNE recommends disciplinary action is imposed on workers who do not comply with the compliance programme, indicating expressly the penalties to be faced by an offending employee. At the same time, establishing incentives for those employees who duly comply with the programme can act as an incentive that will encourage compliance with competition rules.

Relevant case law on competition compliance programmes in Latin Americas

In Chile, the TDLC has imposed compliance programmes as corrective measures in cartel cases.[68] Although this case law provides certain guidelines as to what the competition authorities may consider an effective compliance programme, it should always be borne in mind that these programmes have been imposed as a specific penalty and corrective response and, therefore, no longer follow a fully effective preventive objective.

Compliance programmes imposed as penalty measures have several characteristics in common, as the TDLC typically requires: (1) the implementation of a compliance programme that satisfies the requirements established by the FNE Guidelines on Competition Compliance Programmes, as a sign of deference to the prosecuting entity; (2) the creation of a compliance committee (which must be established in the statutes of the company and be responsible for proposing the appointment and removal of a compliance officer to the board of directors, and ensuring the correct performance of the officer's duties); (3) that the instituted compliance officer performs his or her role full-time and reports directly to the board of directors; (4) the inclusion of comprehensive competition compliance training, carried out by economists or lawyers who are experts in competition matters, for senior executives and administrative personnel, and any other individuals indicated by the compliance officer; and (5) the implementation of frequent competition audits that must consider, at least, the review of corporate email inboxes and records of calls from corporate phones, the incentives established in work contracts, the participation of the company in tender processes and in trade associations, among other things.

68 Ruling No. 160/2017, Case C 299-2015, Case C 184-2008 of the TDLC, FNE's claim against CMPC Tissue SA and others; Ruling No. 165/2018, Case C 312-2016, FNE's claim against Fresenius and others; Ruling No. 167/2019, Case C 304-2016, FNE's claim against Cencosud and others; Ruling No. 171/2019, Case C 292-2015, FNE's claim against CCNI SA and others; Ruling No. 172/2020, Case C 321-2017, FNE's claim against Industrial y Comercial Baxter de Chile Ltda and others; Ruling No. 179/2022, Case C 393-2020, FNE's claim against Inaer Helicopter Chile S.A. and others.

In Peru, in November 2021, Indecopi sanctioned 33 construction companies and 26 executives for forming a bid-rigging type cartel to divide among themselves 112 public bidding processes between the years 2002 and 2016. As a sanction, the companies and executives involved were sentenced to pay high fines and were ordered to implement compliance programmes for a period of five years, with the purpose of discouraging the formation of cartels and promoting the timely detection of anticompetitive practices.

Conclusion

The evolution of competition regulation in several jurisdictions has significantly raised the standards and requirements for companies to mitigate the growing legal exposure associated with anticompetition infringements. This poses a challenge for companies in having to adapt to changes and new standards, especially for those agents with a relevant market power that participate in risky or complex markets. As a result, the implementation of an effective competition compliance programme – the minimum requirements for which have been set fairly uniformly by the authorities of most Latin American jurisdictions – and a real commitment to comply with competition law must be considered today as one of the most essential elements of corporate compliance in Latin America.

CHAPTER 14

Demonstrating Compliance with Data Privacy Legislation

Palmina M Fava, Gabriel Silva, Christopher James and Martin Pereyra[1]

The data protection phenomenon originated in Europe and swept across Latin America in recent years. While Chile was the first country in the region to enact a law on data protection in 1999, several other countries followed this trend, including Argentina in 2000, Uruguay in 2008, Mexico in 2010, Costa Rica and Peru in 2011, Colombia in 2012, Brazil in 2018 and Panama in 2019, with many currently updating their previously enacted privacy laws.[2] Privacy legislation in Latin America often follows the European Union's General Data Protection Regulation (GDPR) model. Costa Rica, for instance, is engaged in a comprehensive reform of its data privacy laws based on the GDPR model. On 28 January 2021, Costa Rica proposed a reform of the existing data protection laws,[3] aiming to restructure the existing data protection agency (PRODHAB) and to adopt Convention 108 of the European Union on Protection of Personal Data.[4] The bill remains in discussion in the Costa Rican Congress.

---

1 Palmina M Fava, Gabriel Silva and Christopher James are partners, and Martin Pereyra is an attorney at Vinson & Elkins LLP. The authors would like to thank associates Gabriela Astolphi, Briana Falcon, Lillian Sun, and Meghan Natenson for their assistance in the preparation of this chapter.

2 https://www.eff.org/deeplinks/2020/09/look-back-and-ahead-data-protection-latin-america-and-spain.

3 https://www.giromartinez.com/news/costa-rica-comprehensive-reform-on-data-privacy.

4 https://www.larepublica.net/noticia/iniciativa-busca-incluir-la-proteccion-de-datos-como-un-derecho-autonomo-en-la-constitucion.

Although Chile was the first country to regulate data privacy in Latin America, its legal framework soon became obsolete and in need of reforms due, in large part, to the lack of an official data privacy authority and the imposition of low fines.[5] Inspired by the GDPR model, in 2017, Bill No. 11144-07 was introduced to the Chilean National Congress aiming to modernise the existing legal framework and to create a new data protection agency, which would allow for the enforcement of the data protection legislation. The approval process in Chile has been slow, but the bill was amended in October 2021 to incorporate the creation of an Agency for the Protection of Personal Data as the data protection authority. The bill was approved by the Chilean Senate and is currently under discussion in the Constitution, Legislation and Justice Committee of the Chamber of Deputies; it is expected to be enacted in 2023.[6]

Colombian data privacy laws are widely viewed as the most modern data protection laws in Latin America and enforcement has been noted favourably. For instance, on 26 November 2020, the Colombian data protection authority mandated that a videoconference service provider implement measures to secure the personal data of its users in Colombia in accordance with the existing data protection law.[7] Also, throughout 2020, several fines were imposed on companies for violation of the data protection rules. More recently, in May 2021, Colombia's data protection authority ordered WhatsApp to comply with measures meant to protect users' personal data, noting that the messaging app was not meeting 75 per cent of data protection rules.[8] The Colombian government also issued Decree 338 of 2022, which sets out guidelines for public entities to prevent and manage cyber incidents, identify critical public cyber infrastructures, and improve cybersecurity governance.[9]

Similarly, Mexico, Brazil and Argentina have undertaken measures to enhance data privacy protections. In 2010, Mexico adopted the Federal Law on the Protection of Personal Data in Possession of Individuals. Since then, the executive branch has issued several other regulations and guidelines establishing further parameters for the existing data protection law. In 2017, the General Law

5 https://www.dataguidance.com/notes/chile-data-protection-overview.

6 https://alessandri.legal/en/progress-on-personal-data-bill-in-2022/.

7 www.sic.gov.co/slider/superindustria-ordena-la-plataforma-zoom-reforzar-medidas-de-seguridad-para-proteger-los-datos-personales-de-los-colombianos.

8 https://www.reuters.com/technology/colombia-orders-whatsapp-comply-with-data-protection-rules-2021-05-26.

9 https://www.ventasdeseguridad.com/en/2022052322092/news/enterprises/decree-338-update-in-colombia-for-cybersecurity.html

for the Protection of Personal Data in Possession of Obligated Subjects entered into force, regulating, among other aspects, data protection in connection with the use of data held by public entities, including law enforcement agencies.[10] The Mexican data protection laws and regulations apply to all personal data information when it is processed (1) in a facility located in a Mexican territory; (2) anywhere in the world, if the information is processed on behalf of a Mexican data controller; (3) regardless of its location, if the Mexican legislation is applicable due to Mexico being part of an international convention; and (4) by using means located in Mexico.

As with other data protection laws throughout Latin America and the world, the Mexican, Brazilian and Argentinian laws and regulations broadly define personal data as any information pertaining to an identified or identifiable individual and impose stiff penalties for violations. For example, violation of privacy laws in Mexico may result in fines and imprisonment, including sanctions per violation calculated at many multiples of the Mexico City minimum wage (currently €138.9 per month). The law also provides for imprisonment (varying from three months to five years) depending on the seriousness of the violation.[11] Violation of privacy laws in Brazil may result in warnings and fines in the range of up to two percent of the annual global turnover for the breaching entity, but limited to a total amount of 50 million reais per infraction.[12] And, in Argentina, violations of privacy laws could result in both monetary fines and imprisonment.

Inspired by the GDPR, in 2018, Brazil enacted its long-awaited data protection law, the LGPD. The LGPD attempted to unify over 40 different statutes that previously governed the use of personal data in Brazil. But the LGPD only became effective in September 2020, and its enforcement provisions did not become effective until August 2021. The LGPD anticipated the creation of a federal agency (the Brazilian National Data Protection Authority (ANPD)), which was officially created in October 2020 after the Brazilian Senate appointed the first officers to serve as the decision-making body of this entity.[13] On 28 January 2021, the newly formed ANPD published its regulatory strategy for 2021 to 2023 and its work plan for 2021 to 2022. According to such strategies and plans, the agency aims to promote the strengthening of the culture of protection of personal data; establish an effective regulatory environment for the protection

10 http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf.

11 https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.

12 https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/.

13 https://www12.senado.leg.br/noticias/materias/2020/10/20/senado-confirma-primeira-diretoria-da-autoridade-nacional-de-protecao-de-dados.

of personal data; and improve the conditions for legal compliance.[14] In the work plan for 2021 to 2022, the agency established priority measures and time frames for implementation, with the most critical steps being the creation of the internal regulation and strategy plan for the ANPD, protection of data related to small- to medium-sized companies and start-ups, and the evolution of administrative rules regarding application of sanctions.[15] During 2021, the ANPD adopted and published a number of guidance and FAQs regarding the LGPD. For example, in May 2021, it published the Guidance for Personal Data Processing Agents and Data Protection Officers, which sets out non-binding guidelines for data processing agents and explains who may exercise the roles of a data controller, operator, or data protection officer.[16] In April 2022, it published a second version of the same guidance, clarifying several concepts under the LGPD and the previous guidance and providing practical examples and explanations.[17]

The LGPD applies to any personal data processing operation, carried out by a natural person or by a legal person under public or private law, regardless of the means by which such information is processed or the country where the information is stored, provided that the information is processed within a Brazilian territory; the processing activity has the purpose of offering or supplying goods or services or the processing of data is related to individuals located in Brazil; or the personal data has been collected in Brazil.[18] Notably, data that is anonymised is not considered personal data, unless the anonymisation process may be reversed by reasonable means.[19]

---

14 https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-planejamento-estrategico-para-2021-2023?mkt_.tok=eyJpIjoiT1RjMk56ZzBNbU00WlRKaSIsInQiOiI4WE5KXC9kUmRPV nlLWWJXUGhEUWxcL1RVWDI3K2xPaHpNXC9ub1p1b2F0V2tmb2xwU3B5NnNBeVA5azJWbVwvSzZaMGNDVzRMNE9GcnJMVkducWJWZDZDbFhVeTFqdm4xS2hFQWZVS2tIT01maEZHcFk2ZnZJYVwvNzRhdlVCaGx0YzlVIn0%3D.

15 https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313.

16 https://www.gov.br/anpd/pt-br/assuntos/noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf.

17 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf.

18 http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

19 http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Furthermore, in February 2022, the Brazilian Congress enacted an amendment to the Brazilian Constitution recognising the protection of personal data as a fundamental right.[20] The proposal underpinning the amendment also gives the federal government the authority to legislate on the processing of personal data of individuals.[21]

Pursuant to principles articulated in the Argentinean Constitution, Argentina has a comprehensive data protection legal framework established by Law 25.326/2000, as further regulated by Decree 1558/2001. Since 2017, the Agency for Access to Public Information (AAIP) has served as the data protection oversight authority in Argentina, responsible for enforcing the data protection law. Law 25.326/2000 applies throughout Argentina and to any processing of personal data carried out online.[22] In August 2022, AAIP opened the public consultation process to begin reforming Law 25.236/2000.[23] After this process, a new draft data protection bill was published in November 2022,[24] with many provisions modeled after the GDPR. For example, the draft bill expands the territorial scope of Law 25.326/2000 to apply to organisations outside of Argentina if they offer goods or services to, or monitor the behaviour of, people located in Argentina.[25] The draft bill also follows GDPR in introducing new definitions related to data and data processing, clarifying provisions on cross-border data transfers, adding new rights for data subjects, and implementing new requirements such as mandatory data protection impact assessments or the mandatory appointment of a data protection officer in specific situations.[26] There is currently no indication of when the bill will be discussed in the Argentinian Congress.

Panama and Uruguay also adopted additional data protection measures in 2021 that apply to the protection of personal data. In May 2021, the president of Panama approved Executive Decree No. 285, which regulates Panama's existing

---

20 https://www.zdnet.com/article/data-protection-becomes-a-fundamental-right-in-brazil/.

21 https://www.gov.br/anpd/pt-br/assuntos/noticias/senado-federal-aprova-proposta-de-emenda-a-constituicao-17-pec-17-2019-que-inclui-a-protecao-de-dados-pessoais-no-rol-de-direitos-e-garantias-fundamentais.

22 https://www.linklaters.com/en/insights/data-protected/data-protected---argentina#:~:text=No%20person%20can%20be%20compelled,be%20identified%20from%20that%20information.

23 https://iapp.org/news/a/argentina-draft-bill-on-personal-data-protection/.

24 https://www.argentina.gob.ar/noticias/presentacion-del-proyecto-de-ley-de-proteccion-de-datos-personales#:~:text=Por%20este%20motivo%2C%20el%20proyecto,la%20postulaci%C3%B3n%20a%20su%20cargo.

25 https://www.argentina.gob.ar/sites/default/files/proyecto_de_ley_de_proteccion_de_datos_personales_-_febrero_2023.pdf.

26 *id.*

Personal Data Protection Law by developing minimum requirements with which data controllers must comply when collecting information, as well as the conditions under which the consent of data subjects must be obtained. The decree also created the obligation to notify the national Data Protection regulator of the subjects of personal data breaches within a 72-hour period after the breach is discovered.[27] In September 2021, the Uruguayan data protection authority adopted Resolution No. 23/021 of 8 June 2021, which notably excluded the United States from the list of appropriate territories for the transfer of personal data without requiring prior administrative authorisations.[28]

Introduction to GDPR

On 26 May 2018, the GDPR went into effect. The GDPR applies to an organisation established in the European Union that processes personal data, whether that processing occurs in the EU, and to an organisation established outside the EU that markets goods or services to the EU or monitors the behaviour of individuals in the EU. Several companies based in Latin America trigger this second prong of the GDPR. Compliance with the GDPR, and the derogations of the various EU Member States, requires implementing various technical, administrative and organisational measures.[29]

Conducting a data inventory

Most entities will need to conduct a thorough review of data held, collected, or processed by the entity as a first step in complying with the GDPR. Through a review of this kind, often called data mapping or data inventory, an entity will gain insight into what personal data is collected and used, where such data is stored, processing activities, and retention practices. This information will allow the covered organisation to undertake (and later document) other compliance obligations, including creating a record of data processing activities as required under Article 30 of the GDPR and demonstrating a lawful basis for processing for each activity as required by Article 6 of the GDPR.

---

27 Article 37.

28 https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-23021.

29 As of 31 January 2021, the United Kingdom left the European Union. As part of that exit, the United Kingdom adopted a General Data Protection Regulation (UK GDPR) that is largely equivalent to the GDPR. Except as noted, guidance in this section also can be applied to the UK GDPR.

Identifying lawful bases for processing

Processing is only lawful under the GDPR to the extent that one of the bases listed in Article 6 applies to the processing activity. These bases include consent from the data subject (which can be withdrawn); performance of a contract; compliance with a legal obligation; demonstrated need for a task of public interest or official authority; and the existence of legitimate interests (where not overridden by the interest or fundamental rights or freedoms of the data subject). Although Article 6 states that processing is lawful where 'at least one' of the bases applies, the Article 29 Working Party's guidance provides that '[a]s a general rule, a processing activity for one specific purpose cannot be based on multiple lawful bases.' Companies should identify and document a lawful basis of processing for each of the activities identified in the data inventory and must furnish both the purpose of processing and its lawful basis when and where data is collected.

Understanding the rights of data subjects

In addition to requiring a lawful basis (e.g., consent or performance of a contract) for each processing activity, the GDPR provides the following rights to data subjects:

- Right to be informed. Data subjects have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.
- Right of access. Data subjects have the right to access and receive a copy of their personal data and other supplementary information.
- Right to rectification. Data subjects have the right to have inaccurate personal data rectified or completed if it is incomplete.
- Right to erasure. Data subjects have the right to have personal data erased. This is also known as the 'right to be forgotten.' The right is not absolute and only applies in certain circumstances.
- Right to restrict processing. Data subjects have the right to request the restriction or suppression of their personal data.
- Right to data portability. Data subjects have the right to obtain and reuse their personal data for their own purposes across services.
- Right to object. Data subjects have the right to object in relation to all or a portion of the personal data held by an entity. Data subjects also may object to a particular purpose for which their data is processed.
- Rights related to automated decision-making. Data subjects have the right not to be subject to a decision that produces legal effects or significantly impacts the data subject based solely on automated processing, including profiling.

Prohibitions on special categories of data

According to Article 9 of the GDPR, any data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,' as well as 'genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation,' is prohibited unless it meets one of the exceptions set out in Article 9. The most notable and widely applicable Article 9 exception is 'explicit consent' to the processing for one or more specified purposes given by the data subject. The Working Party guidance suggests that 'explicit consent' is a more stringent requirement than ordinary Article 6 consent. Specifically, the Working Party has suggested that a written statement, signed by the data subject where appropriate, is one means of demonstrating this requirement. This specific consent exception does not apply where European Union or Member State law prohibits such processing of special categories of data.

Businesses with identified invested stakeholders are more likely to achieve successful compliance. A successful privacy team will be cross-discipline, including parties with technological expertise, as well as those with insight into current and planned business activities. In addition, Article 37 requires a business to appoint a data protection officer (DPO) under the GDPR when:

- it is a public authority or body;
- it conducts regular and systematic monitoring of data subjects on a large scale;
- the business's core activities consist of processing on a large scale of special categories of data or of personal data relating to criminal cases; or
- it is required to do so by Member State law.

A DPO will guide the organisation's GDPR compliance efforts, while serving as a point of contact for data subjects and working with data protection authorities as necessary. DPOs should remain available to company leadership and the privacy team, while maintaining sufficient independence. If an organisation appoints a DPO even when not required by the GDPR, all the requirements of the GDPR related to DPOs remain applicable. Therefore, appointing a 'data protection officer' versus a 'data privacy officer' should be considered carefully. If an organisation decides that a DPO should not be appointed, that decision should be documented for later reference.

Contracting with data processors

Article 29 explicitly prevents processors from processing personal data except on the controller's instructions. Article 28 provides details on documenting these instructions by written agreement. In particular, Article 28 dictates that controllers

'use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of [the GDPR] and ensure the protection of the rights of the data subject.' Contracts under Article 28 should include:

- the subject matter, duration, nature and purposes of the processing;
- the controller's documented instructions for processing;
- the categories of personal data to be processed, as well as the categories of impacted data subjects;
- the controller's obligations and processor's promises to assist with the controller's compliance efforts; and
- the processor's obligation to implement technical and organisational security measures, maintain confidentiality, delete or return personal data at the conclusion of the relationship, submit to audits, and bind sub-processors to requirements under the GDPR.

Choosing a data transfer mechanism

The GDPR also regulates the processing of data within the European Economic Area (EEA), as well as transfers of personal data outside of the EEA. Under the GDPR, there are three scenarios in which an entity legitimately can transfer personal data to a receiver outside the EEA: (1) the receiver is located within an area covered by an adequacy decision; (2) appropriate safeguards have been established to protect individuals' rights to their personal data; or (3) an exception, such as explicit consent, covers the transfer.

Adequacy decisions are made by the European Commission (the Commission) and establish that a given country has adequate data protection and privacy measures. The countries with current adequacy decisions are: Andorra, Argentina, Canada (for commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, and the United Kingdom (pending approval). In 2016, the Commission issued a partial adequacy decision for the United States, ruling that only personal data transfers covered by the EU–US Privacy Shield (the Privacy Shield) provide sufficient protection. On 16 July 2020, however, the Court of Justice of the European Union (CJEU) announced its decision in case C-311/18, better known as Schrems II, upholding the use of standard contractual clauses but striking down the Privacy Shield. This is the second time in five years that the CJEU found a safe harbour programme between the European Union and United States inadequate.

In March 2022, the European Commission and United States announced a preliminary agreement to implement a new Trans-Atlantic Data Privacy Framework to replace the previous Privacy Shield, and this is expected to provide

a durable basis for trans-Atlantic data flows. Under the new Framework, the United States has committed to put safeguards in place to ensure that any surveillance activities are necessary and proportionate in the pursuit of defined national security objectives and to establish a related independent redress mechanism. Although the Framework is still a work in progress, US President Joseph Biden issued an executive order in October 2022 to implement the United States's surveillance-related commitments.[30]

For transfers that do not fall within the scope of an existing adequacy decision, 'appropriate safeguards' must be established. While the GDPR lists several kinds of appropriate safeguards, one of the most common is the SCCs. SCCs are template clauses that are preapproved by the Commission that companies can use in their contracts to ensure sufficient data protection and GDPR compliance. In June 2021, the Commission published new SCCs that place more responsibilities on data importers, such as additional representations and warranties, new sensitive data and accuracy obligations, expanded security and data breach requirements, and more direct liability to individuals and authorities in Europe for data importers.[31] Companies were required to migrate all existing international data transfer agreements entered into before 27 September 2021 to the new SCCs by 27 December 2022. At this point, companies should not be using prior SCC forms without an adequacy decision. The United Kingdom is a special case. It has not adopted the Commission's new SCCs, but it received an adequacy decision from the Commission, which means SCCs currently are not required for transfers of personal data from the European Union to the United Kingdom. However, the United Kingdom's adequacy decision carries with it a 'sunset' clause under which the decision will automatically terminate on 27 June 2025, unless renewed.

Other compliance obligations

The GDPR's requirements are numerous and multifaceted. Companies beginning to work toward compliance should seek the advice of counsel. For additional information on the specific compliance and documentation requirements contained in the GDPR, please reference the table below.

30 https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/

31 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

Requirement/definition	Reference
Lawful bases for processing	Article 6
Access	Article 15
Disclosure of purpose of collection, source, use and third-party sharing	Articles 13, 14, 15
Erasure (deletion)	Article 17
Portability	Article 20
Opt out/object	Article 21(2)–(3) (for direct marketing purposes)
Data protection agreements	Article 28
Data protection impact assessments	Article 35
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, by reference to certain information.
Data subject	A natural person whose personal data is processed by a controller or processor.

Jurisdictional differences in privacy regimes

Data protection regimes can vary dramatically from nation to nation and even from state to state within the United States. What qualifies as sensitive personal information in one nation, requiring more stringent consent and processing requirements, may receive less protection in another nation. Some nations require specific data protection programme elements that can be more onerous on a company, such as the GDPR's 'privacy by design' control environment requirements, registration of processing databases with national supervisory authorities, or the appointment of a specific data protection officer to oversee privacy issues.

Companies may find it beneficial to target investment in or shift operations to jurisdictions with fewer data protection requirements. Depending on the type of data on which the company relies, and its degree of global integration, there are significant potential compliance cost savings even among countries in Latin America that have recently heightened their data oversight. But in an increasingly global economy that relies on cross-border marketing, internet traffic and business partners, those benefits may be limited. Before starting to forum shop, companies must consider not only where their data will be stored or processed, but from whom the data will be collected and where it will be transferred. Data privacy laws often reach beyond national borders when their residents' data is at issue.

For example, if a company collects personal information from citizens and residents in the European Union, even if it hosts its website or processes the data in Panama, the data is still subject to the GDPR requirements. Segregating data

into separate databases with more stringent protections based on the country of origin is possible, but requires additional administrative overhead. If a company intends to establish operations in Brazil or Ecuador that would rely on international data transfers from other countries, it will be required (either by contract or by law) to follow the data protection rules of the origin country. And some countries prohibit the transfer of data internationally unless the destination country has data protection laws that are at least as robust as their own. As discussed in the previous section, the European Union's GDPR mandates strict international transfer standards. The privacy regimes of Argentina, Brazil and Colombia also incorporate this type of comparative protection. So by setting up shop in a jurisdiction with few data protection laws, a company may restrict the ability to efficiently interact with companies or even internal divisions of the same company in other parts of the world.

Even if a company's aim is not to engage in regulatory arbitrage, but more simply to evaluate opportunities for international expansion, it is critical to understand the differences in data protection laws among neighbouring countries. These differences may require significant modifications to data processing policies, procedures and security that could result in major capital expenses for the company, or even subject it to liability for noncompliance. Below are some examples of factors that are treated differently under the laws of various jurisdictions discussed elsewhere in this chapter.

Definition of sensitive personal information

Most privacy regimes recognise that certain types of personal information are more intimate or sensitive, requiring enhanced protection or consent procedures when companies collect and use the data. This usually does not include directory-type information (names, addresses, phone numbers, emails) or transactional data (purchase history, etc.), which would qualify as personally identifiable information subject to some protections, but not sensitive information requiring enhanced protection.

In many Latin American countries, enhanced protections are provided for information more intimately linked to an individual's personal, physical or moral characteristics, such as racial and ethnic origin; religious, political or philosophical beliefs and affiliations; membership in labour unions; and information related to an individual's health and sex life. Many jurisdictions, including Colombia, Costa Rica, Mexico, Brazil, the European Union and some US states offer enhanced protections for biometric data (fingerprints, retina scans, facial recognition, etc.). Genetic information is also afforded specific protections in Costa Rica, the United States, Mexico, Brazil and European Union Member States. Notably, though,

Chile does not require special treatment of these categories. In Argentina, biometric data is only considered to be sensitive if it can reveal additional information, the use of which may potentially result in the discrimination of the data subject.[32]

Mexico's data privacy regime includes a more expansive definition of sensitive personal information than many other jurisdictions, specifically covering pictures, videos, geolocation and the data subject's signature. It is also one of the few regimes in the region to include banking information as a sensitive category.[33]

Consent-conscious jurisdictions

The definition of sensitive information is commonly accompanied by restrictions on use that are predicated on specific notice to, or consent from, the data subject. Informed consent is often required before processing sensitive data, and almost always before selling or disclosing that information to any third parties. In some jurisdictions, though, consent is required before a company can collect or process even non-sensitive personal information. A company that has built its data protection policies on the rules of one nation may open itself up to liability by applying those policies in a jurisdiction that demands a greater degree of control for data subjects.

For example, Costa Rica's Law on the Protection of Persons Regarding the Processing of their Personal Data makes it mandatory to obtain informed and express consent from data subjects to process any personal data. That consent must specify (among other things) the purpose for collecting the data, how the data will be processed, and all recipients and parties with access to the data. Additional consents are required before a company can transfer that data to a third party.

Similarly, Argentina's Personal Data Protection Act states that data processing is only legal with prior, express and informed consent of the data subject. But a number of exceptions apply that broadly carve out categories of personal information companies typically collect. No consent is required to process directory-type information, including name, address, date of birth or even taxpayer identification numbers. Nor is consent required when the data arises from a contractual or professional relationship with a data subject. Use of data for marketing, provision

32 AAIP Resolution 4/2019, available at http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318874/norma.htm.

33 The United States also requires additional safeguards when dealing with data provided to financial institutions or credit agencies.

of credit services or by third-party service providers, is also allowed without consent (though is limited by other rules). Sensitive data, however, may only be collected and processed where necessary and with consent.

Mexico requires some level of consent for all processing of personal data, but allows implicit consent (where the data subject is given notice of the use and an opportunity to opt-out) for processing personal information, generally. Heightened thresholds for consent are required for processing more sensitive data. Express consent (opt-in) is required to process financial or asset data, and express written consent is necessary to process sensitive personal information.

Again, segregating data by degree of sensitivity and place of origin is possible. It is even recommended in some circumstances – for example, more sensitive data may be protected with additional encryptions or be subject to access restrictions to reduce the potential harm of a data breach. But it may be particularly onerous to maintain different standards and protocols for different employees, customers, and business partners in different locations. And if a company's use of the data (analytics, marketing, etc.) would be diminished by segregating along jurisdictional lines, the value in collecting the data in the first place could be reduced.

Breach notification requirements

Possibly the most notorious and feared event in the world of data processing is the breach. Whether the result of hacking, phishing, insider misappropriation, or stolen device, a data breach that compromises the security of a data subject's information (sensitive or otherwise) can cause substantial harm to a company's customers. For that reason, many jurisdictions require that breaches be disclosed to data subjects, government authorities, and sometimes even the media. And while some of the world's largest companies have publicly fallen victim to significant data breaches, breach notification rules can still subject a company to substantial reputational harm and business disruptions.

Several Latin American countries require strict and robust disclosures:

- Colombia's Statutory Law 1581[34] requires both a data controller (the entity that collects and directs use of the data) and the data processor (the entity that carries out the processing instructions) to notify the Superintendent of Industry and Commerce of a security breach, or even a known risk of a breach, within 15 days;

34 Sections 17 and 18.

- Costa Rica's Executive Decree No. 37554-JP[35] requires notification to data subjects and to the national data protection authority (PRODHAB) within five business days. Companies must also complete a thorough review of the breach and its impact during that short time period, and incorporate details of the breach and remediations in their notification; and
- Mexico and Brazil require breach notifications, but only under certain circumstances where the breach is likely to materially affect the property or moral rights of the data subject (Mexico) or likely to result in a risk of harm to the data subjects (Brazil).

While there are currently no breach notification requirements in Chile or Argentina, as a best practice, companies should follow recommended guidelines by their data protection authority. For example, while Argentina's Personal Data Protection Law does not require breach notification, the Agency for Access to Public Information (AAPI) has published Recommended Security Measures calling for data controllers to notify the AAPI about the details of the breach and measures the data controller has taken to mitigate and prevent data breaches.[36] Argentina's new draft data protection bill would impose an obligation to notify the AAIP of a data breach without undue delay and within 48 hours if the breach is likely to result in a risk to data subjects' rights.[37] In Chile, the Commission for the Financial Market (CMF) requires banks and financial institutions to notify CMF of data breaches within 30 minutes of acknowledgement of the breach.[38]

It is critical to remember that data protection laws are often drafted to protect the residents of that jurisdiction, wherever their data is processed. A breach that results in the disclosure of unencrypted personal information of Californians or Belgians will require notification pursuant to those jurisdictions' privacy rules, even if the hacked server was located in Chile, for example. The common rule for evaluating any jurisdictional nuance is to understand the source and use of the data at issue.

35 Articles 38 and 39.

36 AAPI Resolution 47/2018 Annex I, G.1.2 and G.1.3, and Annex II, E.1.2 and E.1.3, available at http://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/312662/norma.htm

37 https://iapp.org/news/a/argentina-draft-bill-on-personal-data-protection/.

38 Updated Compilation of Rules issued by the Chilean Commission for the Financial Market, Chapter 20-8.

Registration requirements

One consideration that is perhaps more straightforward is whether the jurisdiction in which the company plans to process data requires registration of data processing activities with the national authority. This type of registration is not required in most US states (with some specific exceptions for data brokers and telemarketers). But it is required in numerous Latin American jurisdictions and can be a significant administrative burden. For example, Costa Rica's Law on the Protection of Persons Regarding the Processing of their Personal Data No. 8968,[39] requires any entity that manages a database containing personal information, and that distributes, discloses or commercialises such personal information in any manner, to register with PRODHAB. Some exceptions and exemptions exist, including for entities that manage databases for entirely internal purposes and for financial institutions governed by other specific bank secrecy regulations. But for those entities that must register, a substantial submission is required, including details about the data owner, an appointed employee responsible for the databases, a list of all processors and transfer recipients, the type of data to be stored, the purposes and foreseen uses, collection procedures, technical safeguards and risk assessments, and a certified copy of minimum security protocols that details all processes followed by the company to manage the data.

Similarly, Colombia's Statutory Law 1581, in addition to the breach notification rules described above, created the National Register of Databases and requires mandatory registration of databases that store and process personal data by any data controller entities that have total assets above 100,000 tax value units (approximately 3.63 billion Colombian pesos or US$1.07 million). Argentina's Data Protection Authority (AAIP) also maintains a National Registry of Personal Databases.[40] To be deemed a lawful database, all archives, registries, databases and data banks – whether public or private – must be registered. The registration does not require disclosure of the contents of the database, but rather a more general description of the database, its creation, maintenance, and details of compliance with various aspects of Argentina's data protection laws. In contrast, there are no registration requirements in Brazil or Mexico, and only public databases must be registered with Chile's Civil Registry and Identification Service.

39 Article 21, with definition guidance from Article 2(j) of Executive Decree No. 37554-JP, and Article 1(j) of Decree No. 40008-JP.

40 Sections 3 and 21 of the Personal Data Protection Act.

In sum, substantial differences exist in the substantive and administrative application of data protection laws from nation to nation. Depending on how a company's current data compliance programme is constructed, those differences can present either an opportunity or a potential liability pitfall when considering entering a new market. And operating within a global economy often requires attention to multiple regimes at once. There is no secret safe harbour where companies can seek shelter from oversight. There is also no easy one-size-fits-all global compliance solution, and the rate of legislative change occurring in Latin America over the last several years is evidence that companies will need to continue to stay abreast of the applicable privacy rules and to adapt accordingly.

Data compliance programmes

While developing a programme that addresses the significant requirements governing the use, collection and treatment of individuals' personal information in our increasingly globalised world may appear to be a substantial challenge, resources exist to help meet the challenge and to avoid the liabilities that derive from failing to mitigate these risks. When embarking on developing or updating a data compliance programme, companies can be guided by the fair information practice principles (FIPPs), which underpin all data privacy laws. Those principles include awareness, consent, participation, security and enforcement. The key questions when developing or updating such a programme, as outlined above, can generally be traced back to these FIPPs, including the initial requirement of data mapping and inventory, asking what data is held, how it is used, and what the lawful bases are for processing it; determining what data subject rights pertain to the data; and assessing whether prohibitions on special categories of data apply. Appointing a DPO who is responsible for these questions and staying abreast of the applicable regulations is crucial to the success of the programme. Moreover, having a well-designed data compliance programme in place, implemented, tested, and continuously updated, will not only help prevent violations of data privacy laws, including serious data security breaches, it will help the company defend itself from potential lawsuits and regulatory investigations should incidents occur.

Emerging litigation trends in data privacy and data protection

Privacy-related litigation has been on the uptick in the United States, including large-scale class action cases brought on behalf of hundreds and sometimes tens of thousands of plaintiffs that can generate damages in the hundreds of millions of dollars. These emerging litigation trends are important to note for Latin American companies doing business in or serving customers and website visitors located in the United States.

Biometric privacy laws

For several years now, plaintiffs' firms have been bringing claims concerning the use of individuals' biometric identifiers, such as fingerprints, retinal scans and facial recognition. As at 1 March 2023, three states have implemented legislation regulating the use of biometrics: Texas, Illinois and Washington. Several additional states are considering similar legislation.

Illinois' Biometric Information Privacy Act (BIPA) has drawn some of the most attention due to the number and size of cases that have been brought. For example, in *Cothron v. White Castle*, where the Illinois Supreme Court held that each use of a fingerprint system to authenticate employees entailed a separate violation of the BIPA. If the claims are upheld, White Castle estimates that its damages could exceed US$17 billion and involve a class of as many as 9,500 current and former employees. In Texas, the state government has pursued privacy violations against Facebook and Google related to biometric information harvested from uploaded images, videos and voice data. Companies that employ this kind of technology either for internal uses or as customer-facing services should monitor this space closely.

Wiretapping claims

There has been a recent emergence of wiretapping-type claims brought under the California Invasion of Privacy Act (CIPA), which prohibits any person from using electronic means to 'learn the contents or meaning' of any communication 'without consent' or in an 'unauthorized manner'.[41] The new wave targets online tracking tools that collect data about internet visitors' interactions with websites. Websites that use third-party vendors to process user forms or online chat functions, or that use 'session replay' software – a programme that records a website visitor's keystrokes and mouse movements to create a replay of user's interactions with the website – have been frequent targets for this type of litigation. The wiretapping statutes contain a 'party exception' for the website operator itself, because they are considered the intended recipients of the communication and cannot eavesdrop on their own conversations.[42] And that exception may extend to the operator's third-party vendors as long as the information collected is used

41 Cal. Penal Code § 631(a).

42 See *In re Facebook Internet Tracking Litig.*, 956 F.3d 589, 607 (9th Cir. 2020) (citing *Warden v. Kahn*, 160 Cal. Rptr. 471, 475 (1979).

exclusively for the operator's internal purposes.[43] CIPA liability is also limited to interceptions of a communication's 'content' rather than more basic 'record information'. Data collections that are limited to details such as the date and time of visit, IP address, location and browser type would not violate the statute.[44]

Artificial intelligence

As the uses of artificial intelligence (AI) have multiplied, multiple jurisdictions have taken steps to respond to the privacy implications. For example, a class action case is pending in California regarding Google's AI assistant, alleging that users may have had their reasonable expectation of privacy violated when Google Assistant recorded their conversations.[45] Additionally, in September 2022, the European Commission released the proposed AI Liability Directive, which would require national courts to compel providers of 'high-risk' AI systems, as defined by the European Union's AI Act, to disclose relevant evidence to potential claimants.[46] Examples of high-risk AI systems include biometric identification systems, AI systems used in education, employment, or worker management, and AI systems used to evaluate individuals' creditworthiness.[47] If passed, the Directive would create a rebuttable 'presumption of causality' linking non-compliance with the damage caused by the AI system. This presumption would be applied by default to high-risk AI systems and difficult to overcome.[48]

Video Privacy Protection Act

The Video Privacy Protection Act, or VPPA, is a US data privacy statute enacted in 1988 that prohibits 'video tape service provider[s]' from disclosing video viewing histories of their subscribers. 18 U.S.C. § 2710(b)(1). The impetus for the legislation was US Supreme Court nominee Robert Bork's contentious confirmation process, which resulted in Judge Bork's video rental history being published by the press. Though the VPPA was originally understood to apply in the context of tangible materials like cassette tapes, that began to change in the early 2000s with the rise of video streaming on the internet. Frequently, companies use third

43 *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823 (N.D. Cal. 2021); *Williams v. What If Holdings, LLC*, No. C 22-03780 WHA, 2022 WL 17869275 (N.D. Cal. Dec. 22, 2022).

44 *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073 (C.D. Cal. 2021).

45 https://www.reuters.com/technology/google-must-face-voice-assistant-privacy-lawsuit-us-judge-2021-07-02/.

46 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496.

47 https://artificialintelligenceact.eu/the-act/.

48 *id.*

party advertising or analytics tracking in conjunction with their streaming video content. Dozens of class action lawsuits have been brought in the last two years under the VPPA against companies in a variety of industries because of their use of these third-party tracking tools. The viability and scope of these types of claims will be heavily shaped in the next few years.

CHAPTER 16

Recent Trends in Mitigating US Sanctions Risks in Latin America

Ryan Fayhee, Diego Durán de la Vega, Tyler Grove and Anna Hamati[1]

It has been over a year since we published our initial chapter regarding how best to identify and mitigate US sanctions risk in Latin America. To supplement our 2022 publication, this chapter aims to provide an overview of recent trends in US sanctions and how Latin American companies can continue to mitigate such risks. We first provide a brief background of the relevant sanctions authorities, followed by an overview and analysis of trends in US sanctions regulatory developments and enforcement actions, then conclude with recommendations on how Latin American companies can mitigate those risks.

Sanctions background

Sanctions are a foreign policy tool that allow the US president, upon declaring a national emergency, to prohibit a wide range of transactions involving 'property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States'.[2] 'Person' includes both natural persons and entities. The US Department of the Treasury's Office of Foreign Assets Control (OFAC) is the primary agency responsible for administering and enforcing economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats

1 Ryan Fayhee, Diego Durán de la Vega and Tyler Grove are partners, and Anna Hamati is an associate at Hughes Hubbard & Reed LLP.

2 50 U.S.C. § 1702(a).

to the national security, foreign policy or economy of the United States. There are more than 35 US sanctions programmes administered by OFAC, while other departments, including the US Departments of State, Commerce, Homeland Security, and Justice, may also play an important role.

Sanctions may be comprehensive in nature, prohibiting commercial activity with an entire country, as in the case of Syria, Iran, Cuba, North Korea and certain Russian-occupied regions of Ukraine, or they may be more targeted, blocking certain transactions with specific entities, groups or individuals. OFAC imposes targeted sanctions by routinely adding and removing entries on its Specially Designated Nations (SDNs) and Blocked Persons List (SDN List), which contains more than 6,000 listings. All property and interests in property of SDNs that are in the United States or in the possession or control of US persons are blocked[3] and all transactions by US persons or within (or transiting) the United States that involve any property or interests in property of designated or blocked persons are prohibited unless authorised by a general or specific licence issued by OFAC or exempt. Additionally, non-US persons can risk becoming sanctioned themselves for engaging in certain transactions with persons identified on OFAC's SDN List. As illustrated, sanctions are an expansive and flexible foreign policy tool that can be easily imposed or removed to achieve foreign policy objectives, evidencing their appeal to US policymakers.

Sanctions trends overview – regulatory developments in Latin America, Russia and other regions

In 2022, the US utilised sanctions in response to numerous geopolitical issues across the globe, reinforcing the use of sanctions as its preferred foreign policy tool, most notably in the case of Russia. Below, we summarise the US government's recent actions in Latin America, followed by recent actions in Russia and other regions.

3 See OFAC Frequently Asked Question 9, which defines blocking as, 'Another word for it is "freezing."' It is simply a way of controlling targeted property. Title to the blocked property remains with the target, but the exercise of powers and privileges normally associated with ownership is prohibited without authorisation from OFAC. Blocking immediately imposes an across-the-board prohibition against transfers or dealings of any kind with regard to the property.'

Nicaragua

On 24 October 2022, OFAC sanctioned the Nicaraguan mining authority General Directorate of Mines (DGM) and one official of the Government of Nicaragua, pursuant to Executive Order (EO) 13851.[4] Additionally, President Biden signed a new EO that amends EO 13851 and expands the Treasury's authority to hold the Ortega-Murillo regime accountable for its continued attacks on Nicaraguans' freedom of expression and assembly. The new EO also gives the Treasury the authority to target certain persons that operate or have operated in the gold sector of the Nicaraguan economy, and any other sector identified by the Secretary of the Treasury in consultation with the Secretary of State. Furthermore, the new EO provides expanded sanctions authorities that could be used to prohibit new US investment in certain identified business sectors in Nicaragua, the importation of certain products of Nicaraguan origin into the United States, or the exportation, from the United States, or by a United States person, wherever located, of certain items to Nicaragua. The imposition of these sanctions and the US effort to expand its sanctions authorities with respect to Nicaragua signal that the US is prepared to impose further sanctions on Nicaragua if the country continues to act contrary to US foreign policy interests.

In conjunction with the announcement of the Nicaragua-related actions, the Under Secretary of the Treasury for Terrorism and Financial Intelligence, Brian Nelson, noted that, '[t]he Ortega-Murillo regime's continued attacks on democratic actors and members of civil society and unjust detention of political prisoners demonstrate that the regime feels it is not bound by the rule of law,' and '[w]ith President Biden's new Executive Order, we can and will use every tool at our disposal to deny the Ortega-Murillo regime the resources they need to continue to undermine democratic institutions in Nicaragua.' The US sanctions against Nicaragua, as well as the actions against Russia, exemplify the use of sanctions as a blunt force foreign policy tool to isolate persons acting contrary to US interests from financial markets and incentivise a change in behaviour.

Paraguay

On 26 January 2023, OFAC sanctioned Horacio Manuel Cartes Jara (Cartes), the former president of Paraguay, and Hugo Adalberto Velazquez Moreno (Velazquez), the current vice president, for, 'their involvement in the rampant

4 See Press Release, Treasury Sanctions Nicaragua Directorate of Mines and Government Official Responsible for Decades of Violence, Dep't. of the Tres. (24 October 2022).

corruption that undermines democratic institutions in Paraguay."[5] OFAC also sanctioned Tabacos USA Inc, Bebidas USA Inc, Dominicana Acquisition SA, and Frigorifico Chajha SAE, for being owned or controlled by Cartes. OFAC designated these individuals and entities pursuant to EO 13818, which implements the Global Magnitsky Human Rights Accountability Act and targets perpetrators of serious human rights abuse and corruption around the world. Such actions by the US government also illustrate its continued preference for sanctions as a foreign policy tool and its willingness to use sanctions against heads of state to achieve foreign policy objectives.

Venezuela

The US also took sanctions-related actions against Venezuela in 2022. While OFAC's recent Russia, Nicaragua and Paraguay-related actions illustrate how the US government will impose sanctions when persons or countries engage in activity that is against the US's policy interests, recent Venezuela actions illustrate how OFAC is willing to lift sanctions when a person or entity exhibits an interest in engaging more meaningfully with US-supported interests or otherwise adjusts its behaviour. Specifically, on 26 November 2022, the US moderately eased its sanctions on Venezuela's oil sector by issuing Venezuela-related General License (GL) 41, which authorises Chevron Corporation to resume limited natural resource extraction operations in Venezuela, and Venezuela-related GL 8K, which extends the authorisation for US companies to engage in certain limited maintenance operations in Venezuela or involving Venezuela's national oil company, Petróleos de Venezuela, SA, until 26 May 2023.[6] In the corresponding press release for these actions, OFAC noted that the two GLs were issued in response to:

- the Unitary Platform[7] and the Maduro regime's 26 November 2022 announcement of the resumption of talks in Mexico City;
- a humanitarian agreement focused on education, health, food security, flood response, and electricity programmes that will benefit the Venezuelan people; and

5 See Press Release, Treasury Sanctions Paraguay's Former President and Current Vice President for Corruption, Dep't. of the Tres. (26 January 2023).

6 See Press Release, Treasury Issues Venezuela General License 41 Upon Resumption of Mexico City Talks, Dep't. of the Tres. (26 November 2023).

7 The Unitary Platform, or Plataforma Unitaria, is a Venezuelan opposition political alliance made up of civil society, trade unions, retired military personnel, political parties, and deputies of the 2016–2021 National Assembly.

an agreement on the continuation of talks focused on the 2024 elections. OFAC noted that the issuance of the two GLs 'reflects longstanding US policy to provide targeted sanctions relief based on concrete steps that alleviate the suffering of the Venezuelan people and support the restoration of democracy.'[8]

Russia

In addition to the recent sanctions actions related to Latin America, the United States, along with a significant number of other countries, imposed an extraordinary set of economic and trade sanctions on Russia and Belarus in response to Russia's invasion of Ukraine. The key Russia-related actions include the imposition of a comprehensive embargo on the so-called Donetsk People's Republic and Luhansk People's Republic of Ukraine,[9] broad new prohibitions for US persons on making new investments in Russia[10] or providing certain services to Russia (including accounting, trust and corporate formation, management consulting, and quantum computing services),[11] as well as a ban on the provision of services related to the maritime transportation of crude oil and petroleum products of Russian-origin (the Price Cap Policy).[12] The US also expanded its prohibitions against dealings in debt or equity of certain Russian entities, implemented bans on the exportation of US dollar banknotes and luxury goods, and banned the importation of Russian energy products, gold, fish, seafood, alcoholic beverages, and non-industrial diamonds to the United States.[13]

In addition to these actions, the United States added to the SDN List over 1,500 entities and persons operating in Russia, including Russia's largest financial institutions (VTB Bank, Sberbank and Alfa-bank), Russian elites and supporters of its president, persons operating in Russia's defence, industrial, financial, technology and manufacturing sectors, among others, key Russian government officials (including the Russian Duma and its members), and prominent Russian

8 See *id.*

9 See E.O. 14065 (21 February 2022).

10 See E.O. 14066 (8 March 2022), E.O. 14068 (15 March 2022), and E.O. 14071 (6 April 2022).

11 See Determination Pursuant to Section 1(a)(ii) of Executive Order 14071 (8 May 2022) and Determination Pursuant to Section 1(a)(ii) of Executive Order 14024 (15 September 2022).

12 See Determination Pursuant to Section 1(a)(ii), 1(b), and 5 of E.O. 14071 (3 February 2023), Determination Pursuant to Section 1(a)(ii) of E.O. 14071 (3 February 2023), and Guidance on Implementation of the Price Cap Policy for Crude Oil of Russian Federation Origin (3 February 2023).

13 See, e.g., Directive 1A, Prohibitions Related to Certain Sovereign Debt of the Russian Federation (22 February 2022) and Directive 3, Prohibitions Related to New Debt and Equity of Certain Russia-related Entities (24 February 2022).

businessmen (as well as their aircraft and yachts).[14] As a result, US persons are prohibited from virtually all transactions involving these parties and any entities that they own, directly or indirectly, fifty percent or more.

The significant set of actions the United States took, and continues to take, against Russia in response to its invasion of Ukraine illustrates that sanctions remain the foreign policy tool of first resort for the United States. Additionally, the United States's unprecedented coordination with its allies on the use of sanctions to fulfil common foreign policy goals and enforcement objectives indicates that the private sector can expect not only the increased use of sanctions going forward, but also more comprehensive, coordinated sanctions actions that span multiple jurisdictions. For example, the United States coordinated its 24 March 2022 sanctions action against 400 individuals and entities comprised of Russian elites, the Duma and more than 300 of its members, and defence companies, in close coordination and partnership with the European Union and the G7. Additionally, in December 2022, the United States, the 27 Member States of the European Union, the members of the G7, and Australia (collectively, the Price Cap Coalition) adopted a price cap of US$60/barrel on seaborne crude oil of Russian origin. These actions by the US illustrate both its continued preference to utilise sanctions to achieve foreign policy objectives and the increasingly coordinated nature of the United States's sanctions.

Other regulatory action

Separately, while Russia was the primary focus of the United States's sanctions actions over the past year, there were also a number of non-Russia-related sanctions actions. For example, OFAC targeted persons evading US sanctions on Iranian oil, Iranians engaged in cyberattacks, and actors in Iran's ballistic missile programme.[15] Additionally, OFAC implemented sanctions in the virtual currency space, including designating darknet market Hydra and virtual currency exchange Garantex, and two virtual currency mixers, Blender.io and Tornado Cash.[16] Such

14 See, e.g.,, Press Release, U.S. Treasury Announces Unprecedented & Expansive Sanctions Against Russia, Imposing Swift and Severe Economic Costs, US Dep't of Tres. (24 February 2022) and Press Release, Treasury Sanctions Kremlin Elites, Leaders, Oligarchs, and Family for Enabling Putin's War Against Ukraine, US Dep't of Tres. (11 March 2022).

15 See, e.g., Press Release, Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity, Dep't. of the Tres. (14 Sep. 2022) and Press Release, Treasury Sanctions Key Actors in Iran's Ballistic Missile Program, Dep't. of the Tres. (30 March 2022).

16 See, e.g., Press Release, Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex, Dep't. of the Tres. (5 April 2022), Press Release, U.S. Treasury Issues First-Ever Sanctions on a Virtual

actions illustrate that even when pressing geopolitical issues take priority in US foreign policy, like Russia's ongoing assault on Ukraine, OFAC continues to devote resources to all of its sanctions programmes, demonstrating its commitment to comprehensively enforcing all of its sanctions.

Sanctions trends overview

Civil Penalty and Secondary Sanctions Enforcement Actions Civil Penalty Enforcement Actions

OFAC is responsible for the civil enforcement of US sanctions laws and regulations, and the US Department of Justice (DOJ) and the US Attorneys may pursue criminal investigations and enforcement actions for willful violations of US sanctions laws. Notably, OFAC's regulations are enforced on a strict liability basis, which means that OFAC does not need to prove intent or fault to bring an enforcement action and issue a civil penalty. There are numerous ways the US government learns of potential sanctions violations, including through voluntary self-disclosures, suspicious activity reports, referrals from other government agencies or foreign governments, blocked and rejected transaction reports, and through publicly available information, such as media reports. OFAC's Economic Sanctions Enforcement Guidelines at 31 C.F.R. 501 Appendix A outline the factors for calculating the base penalty amounts for violations, including an analysis of factors which can be mitigating or aggravating, such as a willful or reckless violation of the law, awareness of the conduct at issue, cooperation with OFAC, and the existence, nature, and adequacy of a compliance programme, among others.[17]

Over the past year, OFAC has issued a number of enforcement actions. In 2022, 14 parties paid a total of US$42.66 million to OFAC to settle potential civil liability for apparent violations of OFAC sanctions programmes, an increase from a total of US$20.896 million paid by 20 parties in 2021 and US$23.56 million paid by 16 parties in 2020. The 2022 enforcement actions involved violations or apparent violations of the following OFAC sanctions programmes:

Currency Mixer, Targets DPRK Cyber Threats, Dep't. of the Tres. (26 May 2022) and Press Release, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash, Dep't. of the Tres. (8 August 2022).

17 See Economic Sanctions Enforcement Guidelines, Appendix A to 31 C.F.R. Part 501 (OFAC Enforcement Guidelines).

Cuba, Iran, Ukraine, Syria, Venezuela, North Korea, Non-Proliferation, Counter Narcotics, Sudan, and a violation of OFAC's Reporting, Procedures and Penalty Regulations.[18]

Notably, a recent trend in the sanctions enforcement space is an increased focus by OFAC on the 'causation' theory, that is, non-US persons 'causing' US banks to violate sanctions prohibitions. The general provisions rely on the following language: 'Any transaction by a US person or within the United States that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in this part is prohibited.'[19] OFAC is increasingly relying upon these expansive 'causation' provisions as the basis for enforcement actions targeting conduct occurring outside the United States by non-US persons, based on the nexus of US financial institutions' involvement in a US dollar transaction.

The 'causation' theory is significant for Latin American companies because it illustrates that, even if a Latin American company does not have any apparent US nexuses in its business operations besides processing related transactions through the US financial system, OFAC could pursue enforcement actions against companies for having 'caused' a US financial institution to violate US sanctions if it engages in prohibited activity. While OFAC was previously focused on enforcing sanctions against the financial institutions processing such sanctionable activity, it has turned its focus to the companies which cause the financial institutions to process US dollars linked to sanctionable activity. Such actions by OFAC reinforce the importance for Latin American companies to ensure that they ring fence any high-risk activity from US touchpoints, or they may risk becoming the target of an OFAC enforcement action.

This trend is illustrated by OFAC's April 2022 settlement with Toll Holding Limited (Toll), an Australian-based freight forwarding and logistics company, based on OFAC's determination that Toll caused over 2,900 payments to flow through the US financial system in connection with shipments that involved sanctioned jurisdictions or sanctioned persons. Previously, on 14 January 2021, the DOJ and OFAC reached resolutions with PT Bukit Muria Jaya (BMJ), an Indonesia-based paper products manufacturer, that directed payments for its North Korean exports to its US dollar bank account at a non-US bank, which

18 See Civil Penalties and Enforcement Information, U.S. Dept. of the Tres., available at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information.

19 See, e.g., 31 C.F.R. 542.205 of the Syrian Sanctions Regulations and 31 C.F.R. 560.203 of the Iranian Transactions and Sanctions Regulations.

caused US banks to clear wire transfers related to these exports. Additionally, on 16 July 2020, the DOJ and OFAC announced parallel resolutions with Essentra FZE Company Limited (Essentra), a UAE-based supplier, for selling cigarette products it knew to be ultimately destined for North Korea. OFAC concluded, among other things, that Essentra's receipt of three payments into its bank accounts at the non-US branch of a US bank caused the branch (a US person) to export financial services to North Korea. Finally, while this enforcement action was not based on the 'causation' theory as the target was a US person, it highlights the sanctions risk of using US dollars: on 27 May 2022, OFAC entered into an enforcement action with Banco Popular de Puerto Rico, a Puerto Rican bank, which processed 337 transactions totalling US$853,126 in violation of US sanctions on behalf of two individuals who were low level employees of the Government of Venezuela.[20]

While OFAC's use of the 'causation' theory in enforcement actions has increased over the past few years, such enforcement actions did not come without warning. Specifically, when OFAC issued its Framework for OFAC Compliance Commitments in May of 2019 (OFAC Framework), OFAC included a section specifically providing guidance on the sanctions risk of the use of the US financial system in prohibited activity.[21] The OFAC Framework was published in order to provide organisations subject to US jurisdiction, as well as foreign entities that conduct business in or with the United States or US persons, or that use US-origin goods or services, with a framework on the essential components of a sanctions compliance programme. The document also outlines how OFAC may incorporate these components into its evaluation of apparent violations and resolution of investigations resulting in settlements and includes an appendix that offers a brief analysis of some of the root causes of apparent violations of US economic and trade sanctions programmes OFAC has identified during its investigative process.

Section 5 of the Framework, 'Utilizing the U.S. Financial System, or Processing Payments to or through U.S. Financial Institutions, for Commercial Transactions Involving OFAC-Sanctioned Persons or Countries,' notes that:

20 See Civil Penalties and Enforcement Information, U.S. Dept. of the Tres., for a list of OFAC's enforcement actions, available at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information.

21 See A Framework for OFAC Compliance Commitments, OFAC, https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf (OFAC Framework).

Many non-US persons have engaged in violations of OFAC's regulations by processing financial transactions (almost all of which have been denominated in US dollars) to or through US financial institutions that pertain to commercial activity involving an OFAC-sanctioned country, region or person. Although no organisations subject to US jurisdiction may be involved in the underlying transaction – such as the shipment of goods from a third country to an OFAC-sanctioned country – the inclusion of a US financial institution in any payments associated with these transactions often results in a prohibited activity (e.g., the exportation or reexportation of services from the United States to a comprehensively sanctioned country, or dealing in blocked property in the United States). OFAC has generally focused its enforcement investigations on persons who have engaged in wilful or reckless conduct, attempted to conceal their activity (e.g., by stripping or manipulating payment messages, or making false representations to their non-US or US financial institution), engaged in a pattern or practice of conduct for several months or years, ignored or failed to consider numerous warning signs that the conduct was prohibited, involved actual knowledge or involvement by the organisation's management, caused significant harm to US sanctions programme objectives, and were large or sophisticated organisations.[22]

These 'causation' theory enforcement actions, coupled with OFAC's guidance regarding the US financial system in the OFAC Framework, signal that the US government will continue to enforce sanctions against non-U.S. persons, even if the transaction is completed outside of the U.S., if the US financial system is involved. Based on these recent enforcement actions, non-U.S. companies, including in Latin America, should take notice of the growing risk of both civil enforcement by OFAC and criminal enforcement by the DOJ for the use of the US financial system in connection with sanctionable activity, as we predict the US government will continue to target this activity.

Secondary sanctions

In addition to civil enforcement actions, OFAC also enforces its sanctions via secondary sanctions. As highlighted above, non-US persons can become sanctioned themselves, that is, added to OFAC's SDN List, for engaging in certain significant activity with sanctioned persons. Some recent Latin American-related secondary sanctions enforcement actions include the following: On 9 October 2020, OFAC sanctioned Nicaraguan financial institution Cooperativa De Ahorro Y Credito Caja Rural Nacional RL for having materially assisted,

22 OFAC Framework at 10.

sponsored, or provided financial, material, or technological support for, or goods or services in support of, Banco Corporativo, SA, an entity identified on OFAC's SDN List.[23] Additionally, on 1 December 2020, OFAC designated Jhon Fredy Zapata Garzon pursuant to the Foreign Narcotics Kingpin Designation Act for materially assisting the international narcotics trafficking activities of the Clan del Golfo. Three of his family members and associates were also designated along with four businesses they own or control.

Another secondary sanctions enforcement example is from 2 March 2023, when OFAC sanctioned eight Mexican companies linked to a timeshare fraud on behalf of the Cartel de Jalisco Nueva Generacion (CJNG), a violent Mexico-based organisation that traffics a significant proportion of illicit fentanyl and other deadly drugs that enter the US. These eight companies, Servicios Administrativos Fordtwoo, SA de CV, Integracion Badeva, SA de CV, JM Providers Office, SA de CV, Promotora Vallarta One, SA de CV, Recservi, SA de CV, Corporativo Title I, SA de CV, Corporativo TS Business Inc, SA de CV, and TS Business Corporativo, SA de CV were sanctioned for being owned, controlled or directed by, or having acted or purported to act for or on behalf of, directly or indirectly, SDN CJNG.[24] These recent actions illustrate OFAC's expansive sanctions authority to add non-US persons to the SDN List despite the absence of a US nexus in their activities. Such actions emphasise the need for Latin American companies to have a risk-based know-your-client (KYC' programme and screening procedures in place to ensure they are not dealing with any persons who carry sanctions risk.

Key themes and implications

These recent trends in the US's sanctions regulatory developments and enforcement environment offer insight into where the future of sanctions is headed and provide an opportunity for Latin American companies to use this insight to improve their sanctions compliance efforts and mitigate potential risk.

Overall, the US's sanctions regulatory developments illustrate a number of key trends: sanctions remain a preferred foreign policy tool to influence behaviour and achieve the US government's foreign policy objectives; the US government's recent coordination on sanctions with its allies indicates continued future international cooperation and more comprehensive multi-jurisdictional sanctions; and

23 See Press Release, Treasury Sanctions Nicaraguan Financial Institution and Officials Supporting Ortega Regime, Dep't of the Tres. (9 Oct. 2020).

24 See Press Release, Treasury Sanctions CJNG-Run Timeshare Fraud Network, Dep't. of the Tres. (2 March 2023).

the US will continue to calibrate its sanctions based on its target's behaviour by increasing sanctions when such behaviour goes against US policy objectives, as seen in the Russia context, and lifting sanctions when the target engages in favorable behaviour, as seen in the Venezuela context.

These trends offer some key lessons for Latin American companies. First, and most importantly, sanctions will continue to be the preferred foreign policy tool of first resort for the United States. Additionally, sanctions will more frequently be coordinated amongst allied nations and implemented on a multijurisdictional level moving forward. Accordingly, we can expect increasingly frequent rounds of coordinated and complex sanctions in the future. For Latin American companies that engage in international business, or subject themselves to US jurisdiction via the use of the US dollar or other US touchpoints, these trends indicate that such companies' sanctions risk will continue to grow. Even if Latin American countries are not using a US nexus in their normal business operations, they could still risk being designated themselves if they engage in certain activities with persons identified on OFAC's SDN List.

In our previous chapter, we outlined some ways that Latin American companies can mitigate their sanctions risk, which we continue to recommend in this chapter. These recommendations include: ensure appropriate, risk-based compliance procedures are in place; establish KYC or counterparty diligence and screening procedures; identify and ring-fence US touchpoints from high-risk transactions; and consider voluntarily disclosing any identified violations. We also recommend companies take steps to monitor sanctions developments, as the US is frequently implementing new sanctions and modifying existing sanctions, as illustrated above. We further recommend, as needed, that Latin American companies take steps to familiarise themselves with the sanctions programmes in all of the jurisdictions in which they operate, given the increasingly coordinated and global nature of sanctions.

Separately, trends in the United States's sanctions enforcement actions also highlight key takeaways for Latin American companies. Specifically, and as illustrated above with respect to civil penalties, the United States is asserting broader jurisdictional reach over non-US persons that are engaging in transactions that have no direct contact with the United States, other than making or receiving payments in US dollars. Accordingly, Latin American companies should refrain from making or receiving US dollar payments involving OFAC-sanctioned jurisdictions and persons, as such a US nexus alone causes otherwise permissible conduct to fall under US jurisdiction. To sufficiently mitigate this risk, we

recommend that Latin American companies consider incorporating these policies within their broader compliance programme to ensure compliance with OFAC sanctions.

Additionally, the secondary sanctions enforcement actions are significant as they highlight that Latin American companies should maintain a KYC programme and screening procedures in place to ensure they are not dealing with any sanctioned persons, as such activities could lead to an entity being identified on OFAC's SDN List.

Conclusion

Increasingly, sanctions have become the US's preferred response when geopolitical issues arise and a key tool to accomplish its foreign policy and national security objectives. Considering the importance of sanctions in the US's broader mission, we anticipate the trends outlined above, including increased use of sanctions, future coordinated sanctions actions across multiple jurisdictions, the calibration of sanctions based on a target's behaviour, and increased enforcement actions against non-US persons who involve the US financial system in sanctionable activity or engage in other sanctionable activity, will continue. By maintaining awareness of such US sanctions trends and activities by OFAC, Latin American companies can take the necessary steps to ensure they have the policies and procedures in place to prevent future violations.

CHAPTER 17

How Argentina's Financial Services Industry is Managing Risk in an Evolving Environment

Maximiliano D'Auro and Gustavo Papeschi[1]

Introduction

Significant anti-corruption laws have been enacted in Latin America in the past decade, as well as country-specific anti-corruption compliance guidelines. This chapter does not intend to cover all the implications related to risk management in the financial services industry in Argentina, let alone Latin America. Instead, we briefly address the current status in Argentina, as well as the particularities that a risk-based approach to anti-bribery and corruption (ABC) programmes should consider in implementing an adequate integrity programme for financial services providers (FSPs).

A matter of self-perception and the adequacy of any ABC programme

Comparing anti-money laundering and ABC programmes: FSP point of view

The financial services industry has often been in the eye of the storm as regards matters relating to money laundering or the failure to prevent it. Several cases (many of them of massive proportion) have populated the mainstream news and legal forums during the past decade.

Because of that, regulations forced the industry to allocate large amounts of resources to create and maintain anti-money laundering (AML) departments, policies and procedures.

1 Maximiliano D'Auro and Gustavo Papeschi are partners at Beccar Varela.

After many years, FSPs have become used to this new paradigm for doing business. Over time, they have made it an essential part of their day-to-day operations and have strongly embraced the many benefits of a robust AML programme. The strong enforcements made both locally and internationally have made Argentine institutions realise the severity of the new regulations and act accordingly.

In Argentina (and probably in many other places), that is not currently the case for ABC programmes in FSPs. While FSPs have addressed AML for many years, the same cannot be argued with reference to ABC programmes. Argentine financial institutions have not yet allocated to ABC programmes the same kind and amount of resources as they have with AML initiatives.

Local subsidiaries of foreign institutions may be in a better position. The reason for that is the extraterritorial application of foreign anti-bribery laws (the most relevant being the US Foreign Corrupt Practices Act (FCPA)). In that sense, the FCPA provisions apply broadly to three categories of persons and entities: (1) 'issuers' and their officers, directors, employees, agents and shareholders; (2) 'domestic concerns' and their officers, directors, employees, agents' and shareholders; and (3) certain persons and entities, other than issuers and domestic concerns, acting while in the territory of the United States.[2] Moreover, Argentina has been at the centre of many bribery investigations and settlements based on the FCPA, including Siemens Aktiengesellschaft, Olympus Latin America, Inc, Helmerich & Payne Inc, Ralph Lauren Corporation, Stryker Corporation, Zimmer Biomet Holdings Inc, IBM, Bridgestone Corporation and Ball Corporation, to name

2 Released in November 2012, A Resource Guide to the U.S. Foreign Corrupt Practices Act [the FCPA Guide], among other information, specifies which persons and entities are covered by the FCPA's anti-bribery provisions. The FCPA Guide can be accessed at https://www.justice.gov/criminal-fraud/fcpa-guidance.

just a few.[3] To this day, it remains one of the top-12[4] countries for conducting underlying FCPA enforcement actions, with 15 enforcement actions[5] (i.e., proceedings brought by the US Securities and Exchange Commission (SEC), the US Department of Justice (DOJ) or both against individuals or entities based on violations of the FCPA or FCPA-related misconduct).

There is a simple explanation for it: Argentina enacted its major AML legislation in 2000 (although its enforcement came many years after that) but the Corporate Criminal Liability Act for corruption-related offences[6] (the Act) was only passed in late 2017. Hence for a large period, there was no local legal incentive for companies to develop robust anti-corruption control environments.

Although many financial institutions already had some kind of ABC programme before the enactment of the Act (mostly just a general code of conduct or similar and, in many cases, inherited from their holding companies), those were not (or, in some cases, are not) as well developed as the AML programmes. At the very least, they lack the same allocation of resources as the AML programmes.

In parallel with increased attention to ABC, AML efforts continue to increase substantially. This is not only because of the increase of formal banking transactions caused by the global covid-19 crisis (the majority of which are made by electronic means), but also because of new challenges that the near future requires. The most important one currently is the transactions regarding cryptocurrencies. Although the Argentine AML's authority has warned about the relevant challenges when dealing with this kind of assets (warning about the risks involved and

---

3 *Siemens Aktiengesellschaft* (https://www.justice.gov/opa/pr/former-siemens-executive-pleads-guilty-role-100-million-foreign-bribery-scheme); *Olympus Latin America, Inc* (https://www.justice.gov/criminal-fraud/fcpa/cases/olympus-latin-america-inc); *Helmerich & Payne Inc* (https://www.justice.gov/opa/pr/helmerich-payne-agrees-pay-1-million-penalty-resolve-allegations-foreign-bribery-south); *Ralph Lauren Corporation* (https://www.justice.gov/opa/pr/ralph-lauren-corporation-resolves-foreign-corrupt-practices-act-investigation-and-agrees-pay); *Stryker Corporation* (https://www.sec.gov/news/press-release/2013-229); *Zimmer Biomet Holdings Inc* (https://www.justice.gov/opa/pr/zimmer-biomet-holdings-inc-agrees-pay-174-million-resolve-foreign-corrupt-practices-act); *IBM* (https://www.justice.gov/atr/case-document/plaintiffs-proposed-findings-fact-public-version); *Bridgestone Corporation* (https://www.justice.gov/atr/case-document/file/489806/download); *Ball Corporation* (https://www.sec.gov/litigation/admin/2011/34-64123.pdf).

4 See Stanford Law School Foreign Corrupt Practices Act Clearinghouse, Statistics & Analytics, https://fcpa.stanford.edu/geography.html.

5 *id.*

6 Corporate Criminal Liability Act No. 27401 of 8 November 2017 (Arg.) (Ley de Responsabilidad Penal de la Personas Jurídicas), https://www.legiscompliance.com.br/legislacao/norma/124.

requiring a strengthened review of these transactions), no comprehensive regulations have been yet enacted.[7] In the same sense, the Argentina AML authority has not broadened the definition of 'reporting entities' to expressly include trading platforms. FSPs have enriched their treatment to deal with this (rather) recent new form of transactions, but the lack of clear regulations (at least, in Argentina) has prevented the full management of this risk.

The FSPs' self-perception

Other than the legislative reason, an interesting phenomenon we have experienced in the case of financial institutions is that although their self-perception of risk with regard to AML issues is rather high, their self-perception with regard to ABC risks is rather low.

At least in appearance, they seem to have justifiable reasons for that:

- They are highly sophisticated companies, with a great deal of internal controls. Although those controls are not necessarily to address ABC issues, they generally have the effect of preventing any off-the-record outcome of funds or valuables; in a way, their main business is being accountable for the funds they manage.
- Although they are heavily regulated by the relevant supervisory authority (Central Bank, Securities Authority, etc.), the technical and professional nature (as opposed to political) of these regulators makes any type of corrupt behaviour unlikely.
- Generally, their core business is not related to the state as a client. They are not public-work contractors, customs brokers or any other company whose core business is based on their relationship with government. Therefore, their self-perception is that any non-regulatory contact with government officials is rather limited. While middle management's contacts are regular, they are mostly technical in nature, and although contact of a political nature may exist, this typically involves high-level management. Therefore, the chances of occurrence of any act of bribery are lower.

7 We may see changes in near future. For example, last year, the government sent to the National Congress a bill to modify the AML Law No. 25.246. This bill included certain specific regulation regarding the activities related to virtual assets and established that Virtual Asset Providers were to be included within the category of AML Obliged Subjects. To date, the bill has not been approved by the National Congress, https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2022/PDF2022/TP2022/0009-PE-2022.pdf.

Is this self-perception accurate? We believe not. Although the reasons listed above may help to reduce any ABC risk, this reduction is far from material.

In that sense, recently, major fines or settlements have involved large banks and other companies from the financial industry:

Barclays, based in the United Kingdom, agreed to pay US$6.3 million to settle violations of the FCPA's internal accounting controls and record-keeping provisions in connection with its hiring practices in Asia (27 September 2019);[8]

Deutsche Bank AG agreed to pay more than US$16 million to resolve violations of the FCPA's internal accounting controls and record-keeping provisions in connection with its hiring practices (22 August 2019);[9]

Goldman Sachs Group Inc agreed to pay, as part of coordinated resolutions, more than US$2.9 billion, which included more than US$1 billion to settle the SEC's charges for violating FCPA's anti-bribery, books and records, and internal accounting controls provisions in connection with the 1Malaysia Development Berhad (1MDB) bribe scheme (22 October 2020); also, in December 2019, former Goldman Sachs Group Inc executive Tim Leissner had agreed to a settlement with the SEC that included a permanent bar from the securities industry, for engaging in the 1MDB bribery scheme to secure contracts for Goldman Sachs;[10]

World Acceptance Corp (WAC), a South Carolina-based consumer loan company, accepted to pay US$21.7 million to resolve charges that it violated FCPA anti-bribery, books and records, and internal accounting controls provisions, arising out of a bribery scheme orchestrated by its former Mexican subsidiary (6 August 2020);[11]

Asante Berko, a former executive of a foreign-based subsidiary of a US bank holding company, was charged by the SEC with orchestrating a bribery scheme to help a client to win a government contract to build and operate an electrical power plant, in violation of the FCPA; according to the SEC, the firm's compliance personnel took appropriate steps to prevent the firm from participating in the transaction and is not being charged (13 April 2020);[12]

---

8 SEC Enforcement Actions: FCPA Cases, https://www.sec.gov/enforce/sec-enforcement-actions-fcpa-cases.

9 *id.*

10 *id.*

11 *id.*

12 *id.*

- Deutsche Bank AG agreed to pay more than US$43 million in disgorgement and PJI (prejudgment interest) to settle charges that it violated the books and records and internal accounting controls provisions of the FCPA in connection with improper payments to intermediaries in China, the UAE, Italy and Saudi Arabia (8 January 2021);[13] and
- Credit Suisse Group AG agreed to pay nearly US$475 million to US and UK authorities, including nearly US$100 million to the SEC, for fraudulently misleading investors and violating the FCPA in a scheme involving two bond offerings and a syndicated loan that raised funds on behalf of state-owned entities in Mozambique (19 October 2021).[14]

Although it is true that the core business of financial entities is not strictly based on their relationship with state authorities as other high-risk companies, they also do regular state business in a country like Argentina:[15] they expand territorially, for which they need to get permits to open new branches; they deal with judges (both judicial and administrative) to solve any disputes with their clients, partners or the state; they make corporate gifts to reinforce their client relationships; they organise marketing events, for which they need the relevant permits; and, most importantly, they do have business with the national government, provinces, municipalities, other state bodies or state-owned companies (e.g., payroll services for state-owned companies or state agencies, and public-debt services as arrangers, underwriters) but simply treat them as any other corporate counterparty.

Whether higher or lower, FSPs (as any other company) are subject to substantial ABC risks. All aspects of an organisation (internal policies, culture, interactions, etc.) need to be taken into consideration to ensure that an ABC programme is adequate under the Corporate Criminal Liability Act, and other applicable laws and rules in the matter. Furthermore, FSPs' compliance progammes must be 'adequate', as required under the Corporate Criminal Liability Act (i.e., the same requirement levels as any other company). A more detailed explanation of the requirements for adequate compliance programmes is given in the section headed 'The integrity programme adequacy'.

---

13 *id.*

14 *id.* Please note that the Department of Justice's resolution was not based on the FCPA. The company was ultimately charged with conspiracy to commit wire fraud. See Debevoise FCPA Update, January 2022, pp. 6–8 for more information.

15 Ranked as 66 of 180 in the 2019 Transparency International report on the Corruption Perceptions Index.

Corporate Criminal Liability Act and Anti-Corruption Office Guidelines

Long overdue

The introduction of the Corporate Criminal Liability Act has meant, among other things, the fulfilment of the long overdue obligation to make legal persons liable for bribery-related acts that Argentina assumed when signing the Organisation for Economic Co-operation and Development (OECD) Anti-Bribery Convention. The lack of implementation of corporate liability for these types of crimes had been considered in several reports by the OECD Working Group on Bribery in International Business Transactions, the last of which was the 2017 Phase 3 bis evaluation report. Its fulfilment has been a clear sign of the renewed interest Argentina has in carrying out its obligations, clearing its way towards becoming a full member of the OECD[16] and adapting its legal system to the international standards in the fight against corruption.

Main purpose

In a very brief summary, the Corporate Criminal Liability Act has made companies liable for the criminal consequences of certain bribery-related crimes committed by individuals on behalf of the company or for its benefit or interest.

In addition (and probably as important), the Act defines the concept of an integrity programme as the set of actions, mechanisms and internal procedures promoting integrity, supervision and control, oriented to prevent, detect and correct irregularities and criminal acts listed in the Act.[17] Although the law does not require companies to implement an integrity programme, it is highly advisable to do so, not least because it could be used as a defence in a criminal investigation. Furthermore, they are mandatory if the company does business with the national government.

Besides, in respect of FSPs, implementing effective compliance programmes became imperative after Argentina's landmark case in anti-corruption enforcement, the Notebooks scandal.[18] Made public in 2018, the case revealed a massive corruption plan that had taken place between 2005 and 2015 involving public officials and the private sector. Some of the people under investigation were, in

16 González Guerra, Carlos M; Tamagno, María José, 'Ley de responsabilidad penal de la persona jurídico' in *Compliance, anticorrupción y responsabilidad penal empresaria*, González Guerra, Carlos M; et al.; directed by Saccani, Raúl Ricardo; Durrieu, Nicolás, 1st. ed. (Buenos Aires: La Ley, 201).

17 Corporate Criminal Liability Act No. 27401 (footnote 6, above), Article 22.

18 National Chamber of Cassation in Criminal and Correctional Matters, Docket No. CFP 9608/2018.

fact, directors within the financial departments at the time the facts were under scrutiny,[19] who had close connections with the national government. Moreover, the scandal affected the value of several companies' shares (including some in the banking system).[20]

Argentine legislation's 'long arm' and international cooperation

Although the Corporate Criminal Liability Act was conceived from a local point of view, following the 'long arm' doctrine set forth in foreign legislation, it has also included provisions to extend the Argentine criminal courts' reach beyond the national borders.

The Act has amended Article 1 of the Argentine Criminal Code to broaden the Code's territorial scope. Consequently, and in addition to covering (1) crimes committed or with effects in Argentina and (2) those committed abroad by Argentine officials in favour of their functions, the Act has included a new case. For the purposes of the newly included crime provided in Article 258 bis of the Criminal Code (namely, bribery of a foreign official), the Argentine Criminal Code shall also be applicable for actions committed by individuals or entities domiciled in Argentina, even if the action is committed abroad.[21] For these purposes, the Criminal Code broadly defines foreign officials as 'any person from another state, or any territorial entity recognised by Argentina, designated or elected to comply a public function, at any level or governmental territorial division, or in any kind of organism, agency or public company in which such state has direct or indirect influence'.[22]

Furthermore, Argentina is a member of several multilateral, regional and bilateral treaties that facilitate cooperation with other jurisdictions. Many of them specifically target corruption crimes.[23] Moreover, Law 24,767 on International Cooperation in Criminal Matters is applicable when no treaty exists with other countries.

---

19 Official information regarding the case is available at https://www.cij.gov.ar/causas-de-corrupcion.html.

20 'El "efecto cuadernos" llegó a los mercados y golpeó fuerte al Merval', La Política Online (7 August 2018), https://www.perfil.com/noticias/economia/el-efecto-cuadernos-llego-a-los-mercados.phtml.

21 Criminal Code of the Argentine Nation, Article 1, http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm.

22 *id.*, at Article 258 *bis*.

23 The treaties to which Argentina is a party can be accessed at http://www.cooperacion-penal.gov.ar/tratados-internacionales.

Law 24,767 sets forth the principle of 'wide and prompt' cooperation.[24] This means that if judicial assistance is required by a relevant foreign authority, under the conditions established by this Law, Argentine authorities should cooperate. In this regard, the principle of reciprocity is the main condition for cooperation: in the absence of a treaty that requires cooperation, the assistance of Argentine authorities is subordinated to the existence or offering of reciprocity.

The central authority designated by Argentina for all cooperation treaties regarding criminal matters (and treaties containing norms on criminal matters) is the Ministry of Foreign Affairs and Worship. The only exception is the Treaty of Mutual Legal Assistance in Criminal Matters with the United States, in which the designated authority is the Ministry of Justice and Human Rights.

Some agreements concern specific cases. For example, in 2019, a prosecutor signed an agreement with Brazil's Public Ministry to access evidence collected in that country concerning the payment of bribes by Odebrecht to Argentine public officials in Operation Car Wash.[25]

There are several government authorities, such as the Federal Revenue Agency and the Financial Information Unit, that are part of international networks of cooperation.[26]

The integrity programme adequacy

For any integrity programme to be effective, it must be adequate for the relevant company. This adequacy standard dictates that the content of the integrity programme shall have a direct relationship with the risks of the activity in which the company engages, its dimension and its economic capacity.

24 Law 24,767 on international cooperation in criminal matters (Arg.), http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/41442/norma.htm.

25 Announcement of the agreement in the news section of Argentina's Public Prosecutor's Office website (19 June 2019), https://www.fiscales.gob.ar/procuracion-general/soterramiento-del-sarmiento-se-firmo-el-acuerdo-con-autoridades-brasilenas-para-acceder-a-pruebas.

26 For example, Argentina's financial information unit is part of Egmont Group and has signed several memorandums of understanding (MOUs) for the exchange of information with foreign counterparts. A list of the states with which MOUs have been signed can be accessed at https://www.argentina.gob.ar/uif/internacional/convenios.

Following the enactment of the Corporate Criminal Liability Act, Decree 277/2018[27] entrusted Argentina's Anti-corruption Office to establish guidelines to help legal entities comply with the provisions of Sections 22 and 23 of Law 27,401.[28] Consequently, the Anti-corruption Office approved the Guidelines on Integrity Programmes through Resolution 27/2018[29] (the Guidelines).

These Guidelines aim to 'provide technical guidance for companies, civil society organisations, other legal entities, state agencies, members of the judicial system and the professional community'. In this sense, 'they must be understood as complementary to the various and rich specialised literature on compliance, available in Argentine and foreign sources'.

Furthermore, the document points out that even if it provides suggestions to design and implement integrity programmes, they must be necessarily tailored to each legal entity's risks, needs and characteristics, and adapted to the context in which they operate and to their associated risks. For these reasons, the Guidelines highlight that carrying out a risk assessment prior to the design and implementation of the programme is a key step and goes into it in depth.

As mentioned above, the adequacy rule applies to all companies, including FSPs. Any particular risk (or lack thereof) to the relevant FSP should be initially and regularly assessed, balanced, and reflected in the integrity programme, as is the case for any other type of company.

In addition, when designing compliance programmes, FSPs should comply with other federal laws that also aim to tackle corruption. For instance, on 15 May 2019, the Argentine National Congress enacted a law that allows companies to make financial contributions to political campaigns, within certain limits. Law No. 27,504 establishes that, if made in cash, donations should be made via the banking system so that the donor can be identified, and the contribution traced reliably.[30] This requirement gives banks a more relevant role regarding transparency in political funding.

---

27 Published in the Official Gazette on 6 April 2018.

28 These are the sections establish the adequacy standard.

29 Published in the Official Gazette on 4 October 2018. The Anti-corruption Office has subsequently developed other guidelines aimed at small and medium-sized enterprises and the public sector.

30 Law 27,504 establishes that contributions 'must be made only through bank transfer, bank deposit accrediting identity, electronic mediums, bank cheques, credit or debit cards, or platforms and digital applications'.

We move on to the several elements that both the Corporate Criminal Liability Act and the Guidelines mandate or recommend should be included in any integrity programme.[31]

The Act provides that (1) the ethical code, policies, and procedures of integrity, (2) the rules of integrity in public tender processes and other interactions with the public sector, and (3) training and awareness should be mandatory, while other elements are only advisable.[32] Nonetheless, our belief is that all the elements listed in the Act should be included (or at least addressed) to guarantee the adequacy of the integrity programme.

As both the Act and Guidelines follow the generally accepted international standards in the subject matter, it is not necessary to provide a full description of each of them. Instead, we describe the specific particularities applicable to FSPs for the relevant elements of an integrity programme, as our experience on the matter has taught us. We address only those where particular considerations should be made.

Although we do not comment on them, the following elements are also mentioned in law as advisable elements of an integrity programme: internal whistleblower systems; protection of whistleblowers from retaliation; due diligence in mergers and acquisitions and other corporate transformations; and periodic monitoring and assessment of the adequacy of an integrity programme.[33]

The elements of a successful integrity programme

Ethical code, policies and procedures

These are essential parts of an integrity programme because they summarise the FSP's general policies. These documents should clearly contain values, ethical patterns, prohibitions, and sanctions and be reader-friendly.[34]

As any element of an integrity programme, an ethical code should reflect the proper risks of the activity in which the company engages (financial, in this case), its dimension and its economic capacity.

---

31 This was a novel approach by Argentinean legislators at that time, as other flagship legislations such as the FCPA or UKBA do not mandate or describe the elements of a compliance programme (at least in the laws themselves).

32 Corporate Criminal Liability Act No. 27,401 (footnote 6, above), Article 22.

33 *id.*, at Article 23.

34 FSPs are often large organisations with thousands of employees. For general policies to be read and understood, the target audience must be identified, and the deployment and communication of policies must be built around their needs.

FSPs' integrity programmes should be respectful of the specific activity to be carried out by the FSP, whether it is a bank, a credit card company, an underwriter, or a broker-dealer. It is quite a common practice for the specific companies within a financial group to adopt the group's ethical code (as well as other elements of the group's integrity programmes).

Although this practice provides for the coherency of a group's ABC programme, one should avoid using an ethics code that is specific to one company as it is likely to be inadequate for another (a bank and a credit card company are not the same, even if they belong to the same group). Furthermore, an ethics code may not be sufficiently broad to be applicable to all companies in the group, given that it will lose effectiveness. If the latter approach is chosen, a complementary ethics code should be adopted in each company.

A similar situation may arise when trying to adapt the ABC programme of a foreign holding company to a local FSP. The reality of a foreign FSP (and risks) will never be the same as a local FSP – from something as simple as the exchange rate (e.g., a US$50 limit per permissible gift may not be much in Zurich but it will be an opulent gift in Argentina) to something as complex as the ability to terminate an employee agreement because of an ABC matter.

Wrongful adaptations may not only make an integrity programme ineffective but may also prevent the financial activity of the company, as it may turn out to be an obstacle (without technical justification).

The foregoing should not be interpreted as a rejection of the derivative work that is based on foreign ABC legislation, the most relevant being the FCPA. Argentine firms, lawmakers and attorneys have not only studied and used foreign legislation for technical purposes, but the potential consequences from foreign authorities are also borne in mind at the time of designing and implementing integrity programmes.

Integrity in public tenders

Integrity in public tender process and other interactions with the public sector relate to specific rules and procedures to prevent corruption during bids, tenders, entering into contracts with the government and any other interaction with the public sector. No other element of an integrity programme is more often neglected in the financial industry. There is a general self-perception that an FSP's business (particularly in the case of banks) does not involve interaction with the public sector. State clients are generally not perceived as such, particularly in Argentina.

This phenomenon usually (but not only) appears in three lines of business: (1) credit agreements with state-owned companies; (2) payroll services for the benefit of state agencies and state-owned companies; and (3) perhaps the most neglected of all, issuance of public debt bonds (mostly sub-sovereign debt).

These lines of business are usually simply regarded as corporate banking (particularly the first two); in fact, they belong to the general corporate banking department. Although general compliance rules and controls are usually applied (typically addressed to prevent private corruption), no particular rules for dealing with state-owned or state agencies are in place. It is quite common for banks to simply trust in the word of the state-owned company or agency in the sense that no particular procedure or tender is necessary.

But, perhaps, the riskiest line of business may be found when dealing with public debt bonds, whatever the capacity of the bank (lender, underwriter, arranger, etc.). Bank officials usually deal in informal terms and off-the-record meetings within a fast-paced environment. No public tender rules are usually complied with, regardless of how substantial the involved fees may be. Furthermore, these issuances are generally highly controversial (given their political nature) and often subject to very strict public and media scrutiny. They are therefore very risky from a reputational point of view. In that sense, because of the renegotiation of the sovereign public debt in the context of the Argentine crisis between 1998 and 2002 (known as Megacanje, in which a substantial part of the payment of the sovereign public debt was delayed in consideration of higher interest rates), many high-ranking public officials were indicted, including the then Minister of Economy and president. Furthermore, many high-ranking officers at both domestic and foreign banks were also implicated in the criminal case.[35]

The often used term 'it is what it is' would not hold in a court of law or public opinion.

Because of the foregoing, very close attention should be given to these interactions. However fast-paced they might be, a record should be made of every meeting and other interactions. Furthermore, all informal communications should be avoided (e.g., use of private messaging systems, such as WhatsApp). There is a tendency to believe that these types of communications should not be regarded as 'official business', a belief that should clearly be eradicated.

35 'Piden el procesamiento de Cavallo por el "megacanje"', Noticias Clarín (July 2006) <https://www.clarin.com/ultimo-momento/piden-procesamiento-cavallo-megacanje_0_SJtIEJATe.html>.

Training of directors, administrators and employees

The training of directors, administrators and employees is essential to create a culture of integrity. Members of the FSP and third parties should be prioritised according to risks, and training should be adapted to their needs, characteristics, and the company's operational capacity, among other things.

In the case of FSPs, particular attention should be given to the different natures of AML and ABC measures. They may look the same but (needless to say) they are quite different. It is all too common when assessing an FSP's compliance programme for even senior officers to fail to see the need for ABC training, arguing that they have already been trained in AML matters.

It is also interesting to note that, all too often, the main (or sole) training given on ABC issues is focused principally on foreign legislation (the FCPA, UK Bribery Act, etc.). In some cases, that training is provided by foreign law firms.

Regardless of the immense value of this type of training (mostly for those FSPs that may have liability in respect of that legislation), it is of the utmost importance to provide training specifically adapted and construed to the local reality, including to provide an adequate defence. Moreover, with the enactment of the Corporate Criminal Liability Act and the Guidelines, any training should be primarily focused on local legislation and circumstances.

Finally, an important consideration is the general dispersion of an FSP's business in contrast with its management. Branches and offices are located through vast territories, but decision-making processes are often centralised. It is of the utmost importance that employees' and officers' training includes these distant branches and offices. A simple bribe made to a local police officer to keep a small distant branch under surveillance may have disastrous implications for the entire organisation.

Third-party due diligence

There is no need to highlight the importance of third-party due diligence to evidence the integrity and trajectory of third parties, business associates and intermediaries prior to contacting them or during the business relationship. In particular, consideration should be given to the broad liability that the Corporate Criminal Liability Act attributes for acts carried out in the name, interest or benefit of an undertaking.[36]

36 Corporate Criminal Liability Act No. 27401 (footnote 6, above), Article 2.

In the case of FSPs, the importance of this issue is no different, especially given the fact that FSPs are sometimes prevented by the applicable regulations from engaging in activities not related to their core financial activity.[37]

Periodic risk assessment

An adequate programme should be adjusted to the company's risks, dimension, and economic capacity. Thus, according to the Guidelines, a periodic risk assessment is essential to ensure the adequacy of the programme.

It is particularly true in the case of fintechs, but no less true for general FSPs, that financial business is always evolving. New technologies and, consequently, more regulations are created each day. As an FSP's business evolves and its internal organisation changes, a periodic risk assessment becomes more and more necessary.

Tone from the top

The commitment of top management to the programme should be 'visible and unequivocal', as the Corporate Criminal Liability Act and the Guidelines provide.

As has been mentioned, FSPs are highly regulated activities. Although the technical aspects of the regulations are usually carried out by mid-level officers, high-level officers (particularly those at large banks) are usually in direct contact with high-level public officers (e.g., the head of the Central Bank and the Secretary of Finance). It is quite usual to have both a consultancy and a lobbying activity, typically with other major banks.

Although it is difficult to refrain from these types of interactions (which, in general, are compliant with the law), the high profile of the people involved creates a major risk. Therefore, clear, written records of any interaction should be kept; if this is not possible, the interaction should be avoided.

In clear relation to the above notion, the Corporate Criminal Liability Act takes this aspect into consideration and provides the ranking of the officer or employee involved in the bribery action to graduate the entity's criminal sanction.[38]

Internal investigations

According to the Guidelines, it is essential to have an investigation protocol approved by the governing body to detect and mitigate risks, and to justify sanctions for violations.

---

37 Central Bank's Regulation of Ancillary Services to the Financial Activity and Permitted Activities.

38 Corporate Criminal Liability Act No. 27401 (footnote 6, above), Article 8.

In the case of FSPs, there is one investigative particularity that should be taken into consideration: an FSP (particularly a bank) has the ability to easily access a very important (and private) part of an employee's life, namely a bank account (employees are often clients of the bank in which they work).

Although hard to believe, we have found that many employees in charge of internal investigations were not aware of the many serious implications of accessing these records for such a purpose. Not only may they be severely punished by privacy and bank secrecy laws, but also any product of the investigation would be deemed useless in a judicial or administrative case.

Internal officer

For large companies, the Guidelines suggest having an individual or even a team specifically for the function of developing and monitoring the programme. In smaller companies, this function can be assumed by a member of the company that has other duties.

In the case of FSPs, a very common query is whether the compliance officer's role may be taken by the AML officer. Although the particular circumstances of the FSP should be taken into consideration, we believe that it is not advisable to concentrate both these activities in just one person (regardless of the subordinates the individual may have). Although we are of the opinion that both functions may be under the same direction, there should be a specific manager for ABC issues and another for AML issues. That does not mean that both departments would not be able to share common efforts, within the limits and confidentiality requirements provided by AML regulations. In fact, it is highly advisable that they do. In that sense, many of the databases and investigations resources used for AML tasks may be used in ABC efforts.

Compliance with relevant regulatory requirements

In a highly regulated activity such as finance, it is quite common that, in addition to specific ABC and AML regulators, activity-specific regulators often have their own set of AML or ABC guidelines, rules and procedures.

It is important that an FSP's internal organisation allows the involvement of the compliance department in any interaction with the regulator that may involve any kind of AML or ABC issue, even if carried out by a completely unrelated department.

Risk management systems

It is important to highlight how ISO Standard 37001 (on anti-bribery management systems) has affected FSPs.

First, banks willing to comply with ISO 37001 are required to implement specific anti-bribery management systems.

In many countries, some banks seek to obtain ISO 37001 certification. For instance, in 2017, Crédit Agricole Group was the first French bank to obtain this certification.[39] Banco del Pacífico was the first financial entity to obtain ISO 37001 certification in Ecuador, in 2019.[40]

Although there are Argentine companies[41] and state bodies[42] certified under the rules, as at January 2022, no Argentine bank has obtained ISO 37001 certification.

Challenges that the global pandemic has triggered and are here to stay

The global pandemic caused by covid-19 has deeply changed the world and the way we do things. As with many other aspects of life, risk management has also changed dramatically, particularly with regard to FSPs.

Among other consequences arising out of social distancing measures everybody had to adopt back then, the most relevant one from a risk management perspective has been the significant and exponential increase in banking and financial transactions made through electronic means. Although this is true around the globe, in Latin America (where informal and off-the-book transactions still exists in considerable proportion), the rise of e-commerce and exponential growth of certain fintech providers allowed large portions of low-income sectors to be incorporated in the formal banking system.

---

39 'Crédit Agricole Group, 1st French bank to obtain ISO 37001 certification', Caceis Investor Services (October 2017), https://www.caceis.com/de/medien/news/aktualitaet/article/credit-agricole-group-1st-french-bank-to-obtain-iso-37001-certification/detail.html.

40 'Banco del Pacífico es la primera institución financiera con certificación de Gestión Antisoborno, Banco del Pacífico (December 2019), https://bancopacificoprensa.ec/banco-del-pacifico-es-la-primera-institucion-financiera-con-certificacion-de-gestion-antisoborno.

41 Krom, Andrés,'Una empresa argentina se convirtió en la primera en sacar un certificado anticorrupción en la región', *La Nación* (July 2018), https://www.lanacion.com.ar/economia/reconocieron-a-edesur-por-sus-politicas-antisoborno-nid2150563.

42 'Normas anticorrupción, transparencia y reputación de las empresas: debate de expertos en un Congreso Internacional de Compliance en Morón', Infobae (September 2019), https://www.infobae.com/sociedad/2019/09/21/normas-anticorrupcion-transparencia-y-reputacion-de-las-empresas-debate-de-expertos-en-un-congreso-internacional-de-compliance-en-moron.

Even if both the development of electronic transactions and e-commerce and the inclusion of low-income sectors has occurred during recent years, the global pandemic has certainly forced or, at the very least, sped up the process substantially.[43]

This increase in electronic financial transactions has mainly brought to light two challenges (which already existed before), both affecting the traditional banking system as well as non-banking financial providers (including fintech).

From a cybersecurity standpoint, the increase in the quantity and amounts of transactions has exposed them (more than ever) to more and more attacks (just as an example, Banco de México directed that throughout April and November 2020, five financial entities reported cyber attacks).[44] Locally, in 2021 alone, many public agencies such as the Civil Registry and the Public Attorney's Office have experienced data breaches as a consequence of cyber attacks.[45] As a consequence, the relevance of IT security has increased substantially. In a recent survey, it was reported than 96 per cent of respondents said that they would modify their cyber-security strategy during 2021.[46]

From an AML perspective, the onboarding of a new universe of clients and the need for providing a quick screening creates a trade-off with the speed of the detection measures, which may result in a less-than-ideal screening process in the context of a rapid growth expansion. With regard to non-banking providers, they are only partially and indirectly subject to regulations addressed to the financial-banking system, the insurance market, the securities market or the credit card market; however, there is a not a comprehensive regulation that encompasses all of the fintech activity undertaken in Argentina (which continues to increase in scope and kind of services).

Moreover, although FSPs responded to these new challenges in an effective and efficient way, most of them are also battling the lack of economic means to do so, which is a consequence of the general crisis that still drags Argentina's economy.

---

43 https://www.infobae.com/america/agencias/2020/11/13/bancarizacion-aumenta-en-latinoamerica-durante-la-pandemia.

44 https://www.jornada.com.mx/notas/2020/12/06/economia/crecieron-con-la-pandemia-fraudes-a-usuarios-de-la-banca-admite-el-bdem.

45 https://www.lanacion.com.ar/tecnologia/un-ataque-informatico-del-que-todavia-persisten-dudas-sobre-su-alcance-dejo-sin-sistema-interno-al-nid19112021 and https://www.lanacion.com.ar/tecnologia/sigue-la-preocupacion-por-la-difusion-online-de-los-datos-de-argentinos-del-registro-nacional-de-las-nid22102021.

46 https://www.pwc.com.ar/es/prensa/el-impacto-de-la-pandemia-genero-un-aumento-de-la-inversion-en-ciberseguridad-en-las-empresas-de-todo-el-mundo.html.

Conclusion

Argentina has taken its first steps towards the implementation of adequate ABC laws and regulations. The Argentine financial industry has also done so. Although it is difficult to assess any progress at this early stage, key decision-makers are increasingly showing an interest in allocating resources to comprehensive integrity programmes. This investment is not only a matter of funds. High-level officers are increasingly willing to go the extra mile with ABC efforts and considerations.

Any efforts towards strengthening ABC measures is more than justified. Throughout Argentina's recent political and economic history, financial entities (particularly those of foreign capitals) have been the target of investigations, accusations and criminal procedures, especially in respect of their role in sovereign debt. Whether those (mostly politically based) accusations are justified or not, financial entities need to be especially careful, not only because of the recent political history, but also because of the evolution of both foreign and domestic legislation on the matter.

Following the covid-19 crisis, FSPs face new challenges regarding cybersecurity and new non-traditional currencies and means of operation (e.g., bitcoin and other cryptocurrencies) that, although present before lockdowns, have never before been the focus of the management of risks as they are now. These new challenges are met within a general economic context where the efficient use of resources would also be a challenge itself.

Part IV

Trends to Watch

CHAPTER 18

The Growth of Legislation Targeting Private Corruption

Ben O'Neil and Elissa N Baur[1]

Introduction

While essentially all countries criminalise public bribery, laws regarding private corruption have been slower to emerge. Only a few nations that criminalise public bribery also prohibit domestic private bribery, and an even smaller subset of these countries criminalise transnational private bribery.[2] Private corruption, however, affects both the private and public sectors.[3] Aside from resulting in higher risks and decreased efficiencies for companies, private corruption affects the functioning of whole economies by increasing costs and reducing the quality of consumer goods and services, as well as threatening national security.[4] Private corruption even affects how corporations structure themselves: studies have shown a causal link between multinational corporations structuring foreign subsidiaries as wholly owned subsidiaries in countries and higher levels of perceived private corruption.[5]

---

1 Ben O'Neil is a partner and Elissa N Baur is an associate at McGuireWoods LLP.

2 Boles, Jeffrey R, 'The Two Faces of Bribery: International Corruption Pathways Meet Conflicting Legislative Regimes', 35 *Mich. J. Int'l L.* 673 (2014) https://repository.law.umich.edu/mjil/vol35/iss4.

3 See Boles (footnote 2, above).

4 *id.*; see also Johannsen, L; et al., 'Private-to-private corruption: Taking business managers' risk assessment seriously when choosing anti-corruption measures', 2016 OECD Integrity Forum (April 2016); Sartor, Michael A; Beamish, Paul W, 'Private Sector Corruption, Public Sector Corruption and the Organizational Structure of Foreign Subsidiaries', *J. of Bus. Ethics*: 1 to 20 (4 April 2019).

5 See Sartor and Beamish (footnote 4, above).

The effects of private corruption have become even more apparent in the wake of the worldwide privatisation movement, which involves the delegation of traditional systems such as education, prisons, healthcare and welfare to the private sector. Moreover, the 'emergency spending' environment in response to the covid-19 pandemic has provided new temptation and opportunity to engage in private corruption throughout the world. As governments increasingly transfer their functions from the public to the private sector, the effects of private corruption on the public are exacerbated.[6] The public is thus increasingly the ultimate victim of private corruption.

Overview of regulation of private corruption

The regulation of private bribery varies across jurisdictions, from a total absence of regulation in many countries to the UK Bribery Act, which is widely regarded as the most severe private anti-bribery legislation in the world. While some countries have national legislation specifically targeting private corruption, others, such as the United States, target private corruption through a fragmented combination of existing laws.

United Nations Convention Against Corruption

The United Nations Convention Against Corruption (UNCAC), which was adopted by the United Nations General Assembly on 31 October 2003 and came into force on 14 December 2005, establishes standards, measures and rules to help Member States strengthen their anti-corruption legislation.[7] While previous international corruption treaties had applied exclusively to public corruption, UNCAC specifically addresses private corruption by encouraging ratifying states to criminalise both public and private commercial bribery.[8]

UNCAC includes preventive measures applicable to both the public and private sectors, including accounting standards for private companies, and mandatory and permissive criminalisation obligations. The Convention also includes

6 See Boles (footnote 2, above).

7 UN Office on Drugs and Crime, UN Convention against Corruption [UNCAC] (2004), https://www.unodc.org/unodc/en/corruption/tools_and_publications/UN-convention-against-corruption.html.

8 The Inter-American Convention Against Corruption (1996) and the United Nations Convention against Transnational Organized Crime and the Protocols Thereto (2004), for example, only address public corruption: www.oas.org/en/sla/dil/inter_american_treaties_B-58_against_Corruption.asp; https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf.

obligations with respect to public and private sector bribery, trading in influence and illicit enrichment.[9] Although the regulation of private bribery is not mandatory under UNCAC, the proposed measures for regulating and criminalising private bribery signal the international community's disapproval of private corruption and the importance of taking action against it. To guide Member States in fulfilling their obligations under the treaty, UNCAC also produced a toolkit that proposes ways for signatory states to monitor and improve their anti-corruption frameworks.[10] There are currently 187 signatories to UNCAC, including most countries in Latin America.[11]

Regulation of private corruption in the United Kingdom and Europe

Both the United Kingdom and the European Union have been at the forefront of implementing legislation targeting private corruption. In the United Kingdom, the UK Bribery Act treats private and public bribery as the same offence through statutory language that prohibits active and passive bribery without differentiating between public and private actors.[12] The merging of public and private bribery serves to underscore that private bribery is part of a larger family of bribery offences, and raises awareness of the existence and significance of private bribery.[13] Many view this type of comprehensive bribery statute as essential to directing attention to the prosecution of corruption in private forms.[14]

The European Union regulates private corruption through the Council Framework Decision 2003/568/JAI on combating corruption in the private sector, which encourages Member States to take measures to criminalise private corruption, though in a less comprehensive manner than the UK Bribery Act.[15]

---

9 Moyer, H, *Anti-Corruption Regulation 2019*, Getting the Deal Through, Law Business Research (2019), https://gettingthedealthrough.com/area/2/jurisdiction/16/anti-corruption-regulation-mexico.

10 UN Office on Drugs and Crime, The Global Programme against Corruption: UN Anti-Corruption Toolkit (3rd Edition 2004), https://www.un.org/ruleoflaw/files/UN_Anti%20Corruption_Toolkit.pdf.

11 See map showing UNCAC Signature and Ratification Status, https://www.unodc.org/documents/treaties/UNCAC/Status-Map/UNCAC_Status_Map_Current.pdf.

12 See Boles (footnote 2, above).

13 *id.*

14 *id.*

15 Simões, P; et al, 'Motivações e efeitos da corrupção privada – que no Brasil ainda não é crime' (29 July 2019); Instituto Compliance Brasil; Council Framework Decision 2003/568/JAI of 22 July 2003, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003F0568&from=en.

Regulation of private corruption in Latin America

In Latin America, only three countries have passed laws expressly criminalising private bribery, while Brazil has a proposed law criminalising private corruption pending in its Congress. Colombia, Chile and Venezuela have implemented legislation targeting private corruption with varying degrees of success.

In 2011, Colombia specifically incorporated commercial bribery into its Criminal Code under Article 250A by Law No. 1474, which carries a penalty of between four and eight years in prison as well as a fine.[16] This law, however, currently only applies to bribery by a corporate representative and requires there to be damage to the company.[17] Colombia may also punish private corruption through the existing crimes of illicit enrichment and embezzlement.[18]

In 2016, Venezuela passed its Law Against Corruption, which specifically criminalises private corruption regardless of its effect on the public sector. Violations of this Law carry a penalty of between two and eight years in prison and a fine of 100 per cent of the bribe offered (irrespective of the amount potentially gained) or received. Companies found to have engaged in private bribery can also be removed from the state's Sole Register of Persons that Engage in Economic Activities.[19]

Chile recently criminalised private corruption by adding bribery between private parties and fraudulent administration to its Criminal Code with the passage of Law No. 21121 in November 2018. Under Article 287 of the Criminal Code, private bribery is now punishable by imprisonment and a fine for anyone

16 Beltrán, M, 'Colombia –Global bribery offenses guide', DLA Piper (4 December 2019), https://www.dlapiper.com/en/global/insights/publications/2019/09/bribery-offenses-guide/colombia; Valderrama, F; Rodriguez, L, 'Protected legal interest in private corruption felony in Colombia: Systemic analysis and connection with the unfair competition law', Revista del Instituto de Ciencias Jurídicas de Puebla: No. 35, 159 (22 September 2014), https://www.redalyc.org/pdf/2932/293242147009.pdf.

17 UNCAC Executive Summary, Colombia (15 October 2014), https://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/ImplementationReviewGroup/ExecutiveSummaries/V1406898-1e.pdf; 'Principales Tipologías de Corrupción en Colombia', United Nations Office on Drugs and Crime and Fiscalía General de la Nación (November 2018), https://www.fiscalia.gov.co/colombia/wp-content/uploads/Tomo-VIII.pdf.

18 See 'Principales Tipologías de Corrupción en Colombia' (footnote 17, above).

19 Ley Contra la Corrupción y para la Salvaguarda del Patrimonio Público, Transparencia Venezuela, https://transparencia.org.ve/project/ley-contra-la-corrupcion-y-para-la-salvaguarda-del-patrimonio-publico; Zajia, M; et al., 'Anti-Corruption in Venezuela', Global Compliance News, Baker McKenzie Venezuela, https://globalcompliancenews.com/anti-corruption/anti-corruption-in-venezuela.

who receives or offers a bribe.[20] This addition to the Criminal Code also criminalises fraudulent administration of the property of another under Article 470, of which companies can be victims.[21]

Mexico's anti-corruption system

Corruption has long been an entrenched problem in Mexico. Companies doing business there cite diverged funds, money laundering and bribery as recurring concerns; a majority of Mexican businesses consider corruption to be 'business as usual'.[22] The pernicious effects of corruption have become even more apparent in the wake of government efforts to curb drug-related violence in Mexico.[23]

In response to the scattered and impotent efforts that have characterised its anti-corruption efforts in the past, the Mexican Congress voted in 2015 to amend its constitution to renovate its anti-corruption apparatus, creating the National Anti-Corruption System (SNA) an organisation led by a board with civilian oversight that coordinates between existing anti-corruption institutions at the state and federal levels that had previously operated with limited resources or methods for coordination.[24]

The SNA was created through the General Law on Administrative Responsibilities (GLAR), passed in 2015, which mirrors the US Foreign Corrupt Practices Act (FCPA) in many key respects. For example, GLAR applies to both

---

20 Cousiño, F; et al., 'Corrupción entre privados es ahora delito en Chile', Alessandri Abogados (22 November 2018), https://www.alessandri.legal/corrupcion-entre-privados-es-ahora-delito-en-chile; Izquierdo, L, 'Chile continúa su avance en materias de anticorrupción', PwC Chile, https://www.pwc.com/cl/es/Publicaciones/Chile-continua-su-avance-en-materias-de-anticorrupcion.html; Ley Núm. 21.121, Biblioteca del Congreso Nacional de Chile, https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/108068/133368/F-1931174227/LEY-21121_CHILE.pdf.

21 See Cousiño (footnote 20, above).

22 Cabello, A; Santos, D, 'Anti-Corruption Proposals for the Mexican Energy Sector', Wilson Center Mexico Institute (2016), https://www.wilsoncenter.org/publication/anti-corruption-proposals-for-the-mexican-energy-sector; Rodríguez, A, 'Emprendedurismo y Corrupción', La Corrupción en México: Transamos y No Avanzamos (2015), Instituto Mexicano para la Competitividad.

23 Kaiser, M; Rios, V, 'Mexico's Anti-Corruption Spring', The Missing Reform: Strengthening The Rule of Law in Mexico, Wilson Center Mexico Institute (2018), https://www.wilsoncenter.org/sites/default/files/media/documents/publication/the_missing_reform_strengthening_the_rule_of_law_in_mexico.pdf.

24 Chavez, C; et al., 'Mexico's national anti-corruption system: The politics of integrity', Westlaw Journal White-Collar Crime: 33 No. 02, 03 (2018); Hinjosa, G; Meyer, M, 'The Future of Mexico's National Anti-Corruption System', Report, 'WOLA: Advocacy for Human Rights in the Americas (August 2019).

individuals and corporations, requires companies to maintain internal compliance controls, and includes substantive anti-bribery provisions and significant monetary penalties for companies found to have engaged in corruption.[25] Unlike the FCPA, however, the extraterritorial reach of GLAR is limited and its application to private corruption is unclear as it focuses on corruption in the context of securing public contracts.[26] Accordingly, while the SNA includes provisions that could be used to target private corruption, it remains to be seen whether it will be used as such, given the government's current priority of targeting public corruption.

Brazil's attempts to regulate private bribery

In the wake of the *Lava Jato* (*Operation Car Wash*) and *FIFA* investigations, support has coalesced around the regulation of private corruption in Brazil.[27] The *FIFA* scandal brought to light extensive private corruption among individuals involved in the 2014 World Cup in Brazil, including the conviction in the United States of José Maria Marin, who served as head of the Brazil's 2014 World Cup Committee, for taking over US$6 million in bribes for media and marketing rights related to Brazilian and South American soccer tournaments.[28] Marin's conviction came in the wake of the larger *FIFA* case, which revealed widespread private corruption among soccer and media executives.

The *Operation Car Wash* investigation, which has uncovered widespread corruption in Brazil's public sector, has further spurred interest in regulating private corruption in Brazil, as the scandal has entangled powerful private companies.[29] While there have been various attempts to pass laws penalising private corruption, Brazil does not currently regulate commercial bribery.[30]

---

25 See Chavez (footnote 24, above).

26 See Chavez (footnote 24, above).

27 See Simões (see footnote 15, above); see also Frazão, F, 'Projeto prevê criminalizar corrupção privada no País', Estadão (14 July 2018), https://politica.estadao.com.br/noticias/geral,projeto-preve-criminalizar-corrupcao-privada-no-pais,70002401821.

28 'FIFA bans convicted Brazilian soccer official Marin for life', Associated Press (15 April 2019), https://www.dailyherald.com/article/20190415/sports/304159944; see also 'Fifa corruption: Brazil's José Maria Marin jailed for four years', BBC (22 August 2018). Available at: https://www.bbc.com/sport/football/45277581.

29 See Frazão (footnote 27, above).

30 Prado, R, 'Clawback Corrupção Privada e as Novas Medidas Contra a Corrupçã', Consultor Penal (16 November 2018).

Interest in regulating private corruption in Brazil, however, has grown in recent years. For example, the National Strategy to Combat Corruption and Money Laundering (ENCCLA), founded in 2003 by the Brazilian Ministry of Justice, is a network of more than 70 private and public institutions, including the federal police, federal prosecutors, Office of the Comptroller General, the Brazilian Securities and Exchange Commission.[31] In 2018, ENCCLA selected private corruption as its area of focus and as such has taken the lead in creating proposals for measures to fight private corruption.[32]

Furthermore, several bills are currently pending in the Brazilian legislature that would criminalise private corruption. For example, in 2020, a bill was introduced to criminalise the demand, request or receipt of undue advantages between a third party and a partner, officer, administrator, employee or representative of a private legal entity.[33] Under this legislation, private corruption would be punishable by two to six years imprisonment and a fine.[34] Similarly, a bill to reform the Penal Code through the proposed New Brazilian Penal Code includes a provision making private bribery a crime – specifically, Article 172 of the bill would criminalise the receiving of an advantage by an employee or representative of a company in exchange for favourable treatment by a third party. Companies could face fines, debarment from public contracts, confiscation of assets, and mandatory temporary or permanent winding up, and the individuals involved could face a prison sentence of between one and four years.[35]

Although Brazil does not currently penalise private bribery as an independent crime, scholars have suggested that Brazil could start to prosecute private bribery through other existing laws that partially cover corruption in the private sector, such as those regulating unfair competition or fraudulent administration.[36]

First, the unfair competition portion of the National Law on Industrial Property[37] already criminalises commercial bribery between competing companies for anticompetitive purposes, but this law is limited in its application to the anticompetition sphere and to companies within the same industry. Because most

31 Ayres, C, 'Anti-Bribery in Brazil: 2017 Developments', FCPA Américas (2018), https://fcpamericas.com/english/anti-money-laundering/anti-bribery-brazil-2017-developments/#.

32 *id.*

33 See PL 4480/2020.

34 *id.*

35 Teixeira, A, 'Considerações introdutórias sobre o crime de corrupção privada', Comentários ao Direito Penal Econômico Brasileiro, 534; see also www.criminal.mppr.mp.br/arquivos/File/Acao5_Memoria_1_Reuniao_13_03_18.pdf.

36 *id.*

37 Law No. 9279 of 1996, Article 195, Paragraphs IX and X.

instances of private corruption occur between provider and consumer companies rather than between competing companies, the unfair competition law has been insufficient to fully target private corruption, evincing the need for more comprehensive legislation.

Second, private corruption might alternatively be tackled under the existing law against fraudulent administration of financial institutions (Law No. 7492 of 1986). Although this law could be applied to certain types of private corruption, it is limited to regulating financial institutions. In addition, pursuing a fraudulent administration conviction based on private bribery might be held unconstitutional as not being defined with sufficient particularity as required by Article 5 of the Brazilian Constitution.[38] While existing laws are insufficient to properly combat private corruption in Brazil, their increased use to target the activities they do cover should serve as a warning to the private sector of the government's willingness to prosecute those who participate in private-to-private corruption.

Brazil's increased enforcement activities against public officials who have participated in corruption also could indicate a willingness to target private corruption. At the very least, the sheer number of proposed laws targeting private corruption demonstrates that it is likely to be the government's next focus in its fight to identify and eliminate corruption.[39]

Laws regulating private corruption in the United States

The United States has a robust framework of laws, regulations and policies for targeting private corruption at the state and federal levels. While there is no specific federal law prohibiting bribery between private parties, 38 states have enacted commercial bribery statutes that criminalise private bribery and corruption at the state level, while other states prosecute commercial bribery under

38 Article 5, Paragraph XXXXIX.

39 Brazil's 2020–2025 Anticorruption Plan reflects a further emphasis on targeting corruption more broadly. This five-year plan aims to improve the country's prevention, detection, and accountability mechanisms to combat corruption and delineates 142 actions to achieve that goal. Key measures of the plan address, inter alia, providing greater guidance for corporate compliance programmes and leniency agreements, strengthening international cooperation and inter-agency coordination, enhancing whistleblower protections, improving public integrity and regulations of lobbying, enhancing resources for investigations, and increasing resources for investigations. With concrete deadlines in place for each action, the government plans to implement 80 per cent of the actions by 2022. See https://www.gov.br/pt-br/noticias/justica-e-seguranca/2020/12/governo-lanca-plano-anticorrupcao; https://www.gov.br/cgu/pt-br/anticorrupcao/plano-anticorrupcao.pdf.

generic fraud statutes.[40] States with specific commercial bribery statutes often define the crime as when one 'confers, or offers or agrees to confer, any benefit upon any employee, agent or fiduciary . . . with intent to influence his conduct in relation to his employer's or principal's affairs'.[41]

Private corruption is not per se criminalised at the federal level because the US Constitution reserves for states the power to prosecute most crimes absent a sufficient basis for federal jurisdiction.[42] However, there are a variety of federal statutes that can be used to address private corruption, including the mail and wire fraud statutes, securities and antitrust laws, the FCPA and the Travel Act.[43] Federal regulators and prosecutors have also targeted private corruption through various other federal causes of action, such as antitrust, securities fraud, conspiracy, the Money Laundering Control Act, the Hobbes Act,[44] civil and criminal provisions of the Racketeer Influenced and Corrupt Organizations Act and 18 USC Section 666 (known as the federal funds bribery statute).[45] These federal statutes have provided a solid framework for the federal prosecution of commercial bribery in the United States, which has increased in recent years.[46] The Travel Act, the FCPA, and mail and wire fraud statutes have been of particular importance in the federal regulation of private corruption.

---

40 As at 2017, US states with commercial bribery statutes include Alabama, Alaska, Arizona, California, Colorado, Connecticut, Delaware, Florida, Hawaii, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Dakota, North Carolina, Pennsylvania, Rhode Island, South Carolina, South Dakota, Texas, Utah, Virginia, Washington and Wisconsin. UNCAC Executive Summary, United States of America (June 2012) <https://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/ImplementationReviewGroup/18-22June2012/V1251970e.pdf>; see also Rendleman, D, 'Commercial Bribery: Choice and Measurement Within a Remedies Smorgasbord', *Washington & Lee Law Review*, Vol. 74 (2017), 369, https://scholarlycommons.law.wlu.edu/wlulr/vol74/iss1/7.

41 New York Penal Code, Section 180.03, https://www.nysenate.gov/legislation/laws/PEN/180.03.

42 UNCAC Executive Summary (footnote 37, above) at 13.

43 Ala'i, Padideh, 'The United States' Multidimensional Approach to Combatting Corruption', *Articles in Law Reviews & Other Academic Journals*, 316 (2015) <https://digitalcommons.wcl.american.edu/facsch_lawrev/316>.

44 18 USC §1951 amendment to 1934 Anti-Racketeering Act.

45 See Moyer (footnote 9, above) at 157; see also Ala'i (footnote 40, above).

46 See UNCAC Executive Summary (footnote 37, above), at 13.

The Travel Act encompasses the federal prosecutions predicated on violations of state commercial bribery laws involving interstate travel or transportation in the aid of racketeering enterprises.[47] Thus, a person who crosses state lines to commit an act of commercial corruption can be held liable under the state's commercial bribery statutes and under common law tort causes of action.[48] In states that lack a commercial bribery statue, the Travel Act can be used to prosecute acts of interstate bribery through the unfair trade practice laws of those states under the theory that bribery confers an unfair advantage in the marketplace.[49]

The FCPA can also be used to target private corruption through its books and records and internal control provisions. In particular, the FCPA's books and records provision requires publicly traded companies to maintain books and records with 'reasonable detail' to prevent the false or off-the-books accounts that, among other things, are often used to conceal commercial bribery. The FCPA also imposes on publicly traded companies the obligation to adopt appropriate internal accounting controls that, among other things, decrease the occurrence of bribery and other forms of corruption.[50] Internal controls must be adequate to ensure to a reasonable degree that all transactions and assets are authorised by management.[51] Indeed, the absence of such controls has been tied to financial fraud, commercial bribery and embezzlement by company employees.[52]

The mail and wire fraud statutes have also been used to federally prosecute private corruption.[53] These statutes, as amended by the honest services law, prohibit the use of interstate communications such as the mail system, phone or internet in furtherance of a 'scheme to defraud' a person of their tangible property rights or intangible right to 'honest services'.[54] Since the 1940s, courts have recognised a

---

47 Green, S, 'Official and Commercial Bribery: should they be distinguished?', Cambridge University Press (2005), at 43 to 44 .

48 See Moyer (footnote 9, above), at 157.

49 *id.*

50 *id.*

51 *id.*

52 See Ala'i (footnote 43, above).

53 18 USC §§ 1341, 1343 and 1346. Section 1341 makes it a crime to use the mail to execute a 'scheme or artifice to defraud' or to obtain money or property through false or fraudulent pretences, representations or promises. Section 1343 makes it a crime to use interstate wire communications, such as telephone, internet, television or radio transmissions, to do the same. Section 1346 provides that a 'scheme or artifice to defraud' includes a 'scheme or artifice to deprive another of the intangible right of honest services'. See Green (footnote 47, above), at 44.

54 See Moyer (footnote 9, above), at 157; see also 18 USC §§ 1341, 1343, 1346 (2006).

wide range of conduct, including bribery, kickbacks or undisclosed self-dealing in breach of a fiduciary duty, and even international conduct as a 'scheme to defraud' a corporation by denying its right to an employee's 'honest services'.[55]

However, in 2010, the Supreme Court limited the applicability of the 'honest services' theory of the mail and wire fraud statutes to bribery and kickback schemes, eliminating undisclosed self-dealing from the statutes' purview.[56] Some believe the Court's decision has had a chilling effect on the number of 'honest services' prosecutions brought in the United States, though the prosecution of top FIFA officials for 'honest services' violations in 2017 may suggest otherwise.[57] Thus, while the mail and wire fraud statutes allow for the federal prosecution of private sector corruption based on the illegal use of mail or interstate wire communications for bribery and kickback schemes, the lack of clarity surrounding the boundaries of its application may hamper its usefulness and demonstrate the need for a more comprehensive federal framework regulating private sector corruption.[58]

Given the aggressive pursuit of commercial bribery charges by US federal prosecutors in recent years, companies should be aware that even insubstantial involvement of the US mail, phone, internet or banking systems in carrying out acts of private corruption could trigger a federal criminal investigation.[59]

Separately, the prevalence of anonymous shell companies in the United States has been a salient concern for international and domestic anti-corruption efforts, as they have been used to facilitate money laundering, organised crime, terrorism

---

55 See Moyer (footnote 9, above), at 157; see Congressional Research Service, 'Bribery, Kickbacks and Self-Dealing' (30 January 2019) at 22, https://fas.org/sgp/crs/misc/R45479.pdf; see also Green (footnote 47, above), at 44; Dechert LLP, 'Private Commercial Bribery: The Next Wave of Anti-Corruption Enforcement?', at 4 (April 2010); see also *United States v. Pasquantino*, 544 US 349 (2005) (holding that a plot to defraud the government of Canada of tax revenue violated the wire fraud statute); see also *Shushan v. United States*, 117 F.2d 110 (5th Cir. 1941).

56 *Skilling v. United States*, 561 US (2010).

57 Pak, B, 'Private Sector Honest Services Fraud Prosecutions After Skilling v. United States', 66 DOJ *J. Fed. L. & Prac.* 149, 152 (2018); see also Schwartz, M; Zack, J, 'A New Federal Theory of Corruption?', Boies Schiller Flexner LLP (11 December 2017), https://www.bsfllp.com/news-events/a-new-federal-theory-of-corruption.html; Ruiz, R, '2 Top Soccer Officials Found Guilty in FIFA Case', The New York Times (22 December 2017), https://www.nytimes.com/2017/12/22/sports/soccer/fifa-trial.html.

58 Clark, S, 'New Solutions to the Age-Old Problem of Private-Sector Bribery', *Minnesota Law Review*, Vol. 378 (2013) at 2294, 2318, https://scholarship.law.umn.edu/mlr/379 (arguing that the FCPA should be amended to include private-sector bribery).

59 See Dechert LLP (footnote 55, above), at 4.

financing, and other illicit activities. Although the United States has a robust regulatory and enforcement framework to combat private corruption, a critical gap identified by both international bodies and domestic authorities is the lack of systematic disclosure of beneficial ownership information for a variety of legal entities in the United States.[60] The absence of transparency amplifies the potential for abuse of shell companies as vehicles for corrupt conduct.

At the start of 2021, the United States took a significant step towards reducing this vulnerability by passing the Corporate Transparency Act (CTA), which was part of legislation considered to be the most significant reform to the country's anti-money laundering regime since the 2001 Patriot Act.[61] Significantly, the CTA mandates the creation of a government-maintained database of beneficial owner[62] information and requires certain legal entities to report such information to the government – or else face criminal or civil penalties.[63] Specifically, 'reporting companies'[64] must disclose their beneficial owners': full legal name; date of birth; current residential or business address; and unique identifying number from an acceptable identification document or FinCEN identifier.[65] Entities exempt from the reporting requirements include, among others, publicly traded companies and their wholly owned subsidiaries, companies that employ 20 or more employees

60 See FATF, Mutual Evaluation Report of the United States, 2016, at https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf; National Money Laundering Risk Assessment 2018, US Department of Treasury, at https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf; EU-US trade and investment relations: Effects on tax evasion, money laundering and tax transparency, European Parliamentary Research Service, European Parliament, at https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/598602/EPRS_IDA(2017)598602_EN.pdf

61 The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H.R. 6395 (Conference Report 2 December 2020), 116th Cong. (2020) (Conf. Report).

62 Except for certain exceptions (see Conf. Report at 2956:10 – 2957:8), a 'beneficial owner' is generally 'an individual, who, directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise—exercises substantial control over the entity' or who 'owns or controls not less than 25 percent of the ownership interests of the entity' (*id.* at 2955:24 – 2956:9).

63 'Willfully providing or attempting to provide false or fraudulent beneficial ownership information to FinCEN, or willfully failing to report complete or updated beneficial ownership information, is punishable by: (i) a civil penalty of up to $500 per day for each day that the violation continues or has not been remedied; and (ii) a fine of up to $10,000, imprisonment up to two years, or both.' Id. at 2999:16 – 25.

64 'Reporting companies' include corporations, limited liability companies, and similar US entities, as well as foreign companies that are registered to do business in the United States. See *id.* at 2958:21 – 2959:10.

65 *id.* at 2958:21 – 2959:10; 2974:1 – 17.

on a full-time basis in the United States, companies that have an operating presence at a physical location in the United States, and companies that filed US tax returns demonstrating more than US$5 million in gross receipts or sales.[66]

Although the information would not be public, FinCEN – the agency responsible for maintaining the database – may disclose beneficial ownership information to federal, state, and local law enforcement authorities engaged in investigations and national security or intelligence activity.[67] The information may also be shared with foreign authorities under certain circumstances pursuant to a request by a federal agency on their behalf.[68] In addition, FinCEN may disclose beneficial ownership information to financial institutions subject to customer due diligence requirements with the consent of the reporting company, and to federal regulatory agencies, subject to certain requirements, such as security and confidentiality protocols to be set by the US Treasury Department.[69]

These requirements represent a significant change to the laws regarding corporate formation in the United States. While beneficial owners may still remain anonymous from private parties, their identities must now be disclosed to United States, or even foreign, law enforcement authorities. As a result, the use of 'shell' entities in the United States as part of schemes to engage in private corruption and criminal activity is likely to decrease.

Regulation of private corruption by multilateral development banks

As billions of dollars flow from multilateral development banks (MDBs) to governments in developing countries to address the pandemic and other development needs, the temptation and opportunity to engage in private corruption appear particularly ripe in the current 'emergency spending' environment. Unsurprisingly, in this climate, MDBs have placed renewed emphasis on updating their protocols to punish and deter a broad range of private corruption. Companies that bid on and receive MDB-financed contracts are often required to acquiesce to MDB jurisdiction in investigating and sanctioning a broad range of private corruption activity. Companies found to violate these MDB rules governing private corruption face stiff, potentially operation-ending penalties.

66 See *id.* at 2958:21 – 2968:20.
67 See *id.* at 2980:14 – 2982:9.
68 See *id.*
69 See *id.* at 2982:10 – 2987:18.

MDBs have developed robust sanctions systems to punish and deter a broad range of practices encompassing private corruption. For example, the World Bank Group's sanctions system, one of the most sophisticated MDB anti-corruption regimes, has used its enforcement authority in the global fight against corruption for over 20 years.[70] To support these efforts, the World Bank's sanctioning system consists of highly capable anti-corruption units that investigate and address at least five types of illicit conduct (Sanctionable Practices), all of which may be used as tools to punish and deter private corruption activity:

- coercive practices: 'impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party';
- collusive practices: 'an arrangement between two or more parties designed to achieve an improper purpose, including to influence improperly the actions of another party';
- corrupt practices: 'the offering, giving, receiving or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party';
- fraudulent practices: 'any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation'; and
- obstructive practices: '(i) deliberately destroying, falsifying, altering or concealing of evidence material to the investigation or making false statements to investigators in order to materially impede a Bank investigation into allegations of a corrupt, fraudulent, coercive or collusive practice; and/or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation, or (ii) acts intended to materially impede the exercise of the Bank's contractual rights of audit or access to information.'[71]

Sanctions under the World Bank's sanction system can range from a letter of reprimand to permanent debarment, as well as payment of restitution to a party harmed by a party's misconduct. Furthermore, in 2010, several of the most prominent MDBs entered into the Agreement for Mutual Enforcement of Debarment Decisions, which provides for mutual and reciprocal enforcement of debarment decisions made by any one of the MDBs against entities that are found

70 https://www.worldbank.org/en/topic/governance/brief/anti-corruption.

71 https://www.worldbank.org/content/dam/documents/sanctions/otherdocuments/osd/WBGSanctions_Procedures_April2012_Final.pdf.

to have engaged in sanctionable practices (the Cross-Debarment Agreement). Accordingly, a company sanctioned by the any MDB for private corruption may find itself automatically cross-debarred from obtain financing from other MDBs based on the same sanctionable practices. For repeat players in the MDB-financed project space, crippling sanctions and the Cross-Debarment Agreement can have devastating and operation-ending effects on even the most prominent providers and institutions.

How to identify kickbacks within private companies

Kickbacks involve the negotiated remuneration of an individual for facilitating a transaction and are generally considered a higher risk in free market countries.[72] Kickback schemes almost always occur during the purchase or bidding phase of a transaction between two companies, and are often disguised as management or consultancy fees. However, kickback schemes do not always involve the payment of cash, but can rather involve hidden interests in other companies, employment opportunities or tangible gifts.[73]

While the line between sales processes and kickbacks is difficult to draw, companies can implement robust monitoring policies to help prevent and identify kickbacks in the corporate setting. While companies should implement whistle-blower mechanisms sufficient to encourage the reporting of kickback schemes, whistleblowers usually report wrongdoing after it has already occurred.[74] For this reason, it is important for companies to take steps to prevent and detect kickback schemes before they come to fruition. This can be done through the creation of internal investigative units and software aimed at spotting indicators of kickbacks.[75]

Indicators of kickback schemes vary according to the type of industry and transaction. For example, the involvement of middlemen or third parties in brokering a transaction where none is needed is a potential indicator that kick-backs may be present.[76]

---

72 As opposed to highly regulated or bureaucratic countries, where public corruption is a greater risk – see https://latinlawyer.com/chapter/1177364/anti-corruption-in-latin-america.

73 'Guide to Combating Corruption & Fraud in Development Projects – Potential Scheme: Bribes and Kickbacks', International Anti-Corruption Resource Center (2020), https://guide.iacrc.org/potential-scheme-bribes-and-kickbacks.

74 *id.*

75 See Johannsen (footnote 4, above).

76 'Five Types of Kickback Fraud', *The Whistleblower Lawyer*, https://www.thewhistleblowerlawyer.com/five-kickback-fraud; Koukios, J; et al., 'Anti-Corruption in Latin

In the purchase context, high prices, high-volume purchases or unusual approval patterns may indicate the existence of a kickback scheme. In the bidding context, unexplained delays, bidding irregularities in favour of a small group of contractors, or unjustified sole-source awards are often signs that bribes and kickbacks are being offered and accepted.[77] In the sales context, experts suggest comparing prices paid for goods or services with market rates to identify continued purchases of high-priced, low-quality goods or unexplained favourable treatment of certain vendors.[78]

Corporate bribes and kickbacks often produce a paper trail that can successfully be detected and followed with the aid of robust accounting procedures, including internal investigative units using software to spot indicators of kickbacks. Increased oversight of operations with a high risk of corrupt practices not only aids in the detection of kickbacks but has also been shown to prevent them.[79]

Ultimately, companies can take steps to prevent kickback schemes by designing policies that clearly define prohibited conduct and conflicts of interest.[80] Clear policies and training of employees can help create business environments that value ethical behaviour as the best way to serve a company's interests.[81] In addition, the inclusion of anti-corruption clauses in contracts, which allow contracts to be terminated if any party has engaged in any form of corruption, can help prevent kickbacks and signal to potential business partners a company's disapproval of the practice.[82]

America', *The Guide to Corporate Crisis Management*, First Edition (28 November 2018), Latin Lawyer, Law Business Research, https://latinlawyer.com/chapter/1177364/anti-corruption-in-latin-america.

77 See Campos, J Edgardo; Pradhan, Sanjar, 'The Many Faces of Corruption: Tracking Vulnerabilities at the Sector Level', The International Bank for Reconstruction and Development/The World Bank (2007) at 174, https://openknowledge.worldbank.org/bitstream/handle/10986/6848/399850REPLACEM1010FFICIAL0USE0Only1.pdf?sequence=1.

78 Auditing and Investigating Fraud Seminar, Association of Certified Fraud Examiners (2012), https://www.fraudconference.com/uploadedFiles/Fraud_Conference/Content/Course-Materials/presentations/23rd/ppt/post-Aud02-Corruption.pdf.

79 See Johannsen (footnote 4, above).

80 'Could Kickbacks Happen at Your Company' (March 2017), Dulin, Ward & Dewald, Inc, https://dwdcpa.com/blog/could-bribery-and-kickbacks-happen-at-your-company.

81 Rose-Ackerman, S, 'Measuring Private Sector Corruption', 5 U4 Anti-Corruption Resource Centre (September 2007), https://www.cmi.no/publications/2755-measuring-private-sector-corruption.

82 Peace, B, 'Roundtable: Lava Jato and Its Impact on Investigations in Latin America', *The Guide to Corporate Crisis Management*, First Edition (28 November 2018), Latin Lawyer, Law

Conclusion

As awareness of the prevalence and nefariousness of private corruption grows, more countries have decided to take steps to combat private corruption aggressively within and beyond national borders. The United States and United Kingdom have differing but equally forceful means of combating private corruption. In Latin America, certain countries have been taking up the mantle of passing legislation that criminalises private corruption, though the success of implementing these reforms has been varied across jurisdictions. With growing international interest in preventing and penalising private corruption, companies should meticulously design policies and procedures to detect and eliminate corrupt practices.

Business Research, https://latinlawyer.com/chapter/1177365/roundtable-lava-jato-and-its-impact-on-investigations-in-latin-america.

CHAPTER 19

The Rise of ESG as a Social Pillar in Latin America

Ruti Smithline, Hayley Ichilcik, James M Koukios, Lauren Navarro and Stephanie Pong[1]

What is ESG?

Environmental, social and corporate governance (collectively referred to as ESG) is generally used to describe criteria or standards by which companies can be measured with respect to a broad range of socially desirable ends. These data points are then incorporated into the decision-making and risk management process for investors, financial institutions, customers and government agencies or regulators, among others. Each of the three areas of ESG (referred to herein as 'Pillars') are defined by different factors. Environmental criteria are used to assess the Environmental Pillar and a company's impact on the natural environment (e.g., reductions in carbon emissions, use of renewable energy sources, and waste management). The Social Pillar (also referred to as the 'Stakeholder Pillar') considers how a company manages its relationships with stakeholders, which includes shareholders, employees, suppliers, customers and the communities within which the company operates. Under the Corporate Governance Pillar, various criteria examine how a company is operated – most notably focusing on the role and composition of executive management or the board of directors, the

1 Ruti Smithline, Hayley Ichilcik, James M Koukios and Lauren Navarro are partners, and Stephanie Pong is an associate, at Morrison & Foerster LLP. The authors would like to thank William Quamina, a trainee solicitor in the firm's London office, for his contributions to this chapter.

distribution of rights and responsibilities among directors, shareholders, and other participants in the company, and how these participants interconnect to promote the company's ongoing success.

The Social Pillar of ESG is often overshadowed by the other two pillars because it is more difficult to define and measure. The Social Pillar has a broad remit, covering how companies manage their relationships with all stakeholders, not just shareholders, as noted above. Because of this coverage, risks under the Social Pillar can affect company performance, growth, and reputation. While, for example, environmental matters are particularly significant in certain industries (e.g., oil and mining), the Social Pillar affects every company, regardless of geographical location or sector.

ESG awareness and implementation in Latin America have generally trailed behind when compared to Europe, North America, and East Asia. That said, the disruption and changes caused by the covid-19 pandemic helped put social matters top of mind for organisations globally, including in Latin America. The Latin American and Caribbean economies suffered more in the wake of the pandemic compared to the rest of the Western world, one reason being that a large proportion of jobs in these economies requires close physical proximity in contact-intensive sectors (e.g., restaurants, retail stores, and public transportation), compared to around 30 per cent for emerging markets.[2] Latin American economies have since garnered positive economic growth, reflecting the bounceback of service sectors and employment to pre-covid-19 pandemic levels; however the momentum of growth has been stifled by inflationary pressures.[3]

Against this backdrop, we see an increased focus in Latin America on the adoption of ESG practices to help guide corporate decision-making and manage corporate risk, specifically related to how companies impact on their employees and other stakeholders. For example, during the covid-19 pandemic, salary subsidies and loans to support employment and retention became common in Argentina, Brazil, Chile, Colombia, Mexico, and Peru, assuming certain criteria were met (e.g., firm size, compensation levels, and financial loss as a result of the covid-19

2 Samuel Pienknagura, Jorge Roldós and Alejandro Werner, 'Pandemic Persistence Clouds Latin America and Caribbean Recovery', IMF Blog, October 2020, https://www.imf.org/en/Blogs/Articles/2020/10/22/blog-whd-reo-october-pandemic-persistence-clouds-latam-and-caribbean-recovery.

3 Gustavo Adler, Nigel Chalk and Anna Ivanova, 'Latin America Faces Slowing Growth and High Inflation Amid Social Tensions', IMF blog, February 2023 https://www.imf.org/en/Blogs/Articles/2023/02/01/latin-america-faces-slowing-growth-and-high-inflation-amid-social-tensions.

pandemic).[4] In addition, both the financial industry and government regulators are driving ESG-related efforts and Latin American governments are increasingly relying on ESG-related criteria as instruments to address social and environmental matters, including ongoing consequences of the covid-19 pandemic.

We have also seen how government regulation has pushed companies towards a greater focus on social issues – one example being the US sanctions on goods connected to Xinjiang, imposed in December 2021. These sanctions prohibit imports from the Xinjiang region of China unless businesses can prove that their goods were produced without the use of forced labour.[5] The European Union is set to introduce a similar regulation, but one with a much broader remit as it aims to ban products in the EU market that have been made with forced labour.[6]

Though outside Latin America, such regulations are illustrative of a broader shift and increasing emphasis on ESG-related issues, and the Social Pillar in particular. Moreover, such regulation in Asia likely foretells the future for similar issues in Latin America, where awareness and implementation of ESG practices have generally lagged relative to other regions in the world. Put simply, ESG (and specifically the Social Pillar) has the world's attention and is here to stay, even if different regions are at different phases of implementation.

Unpacking the 'S' in ESG

As noted above, the Social Pillar predominantly concerns how a company manages its relationships with stakeholders other than just shareholders. This assessment covers a number of key areas including:

- employees (e.g., labour rights and conditions, salaries and benefits, diversity and inclusion, workplace harassment and discrimination, health and safety, and whistleblower protection);
- suppliers (e.g., corruption and exploitation within supply chains);
- customers (e.g., product safety and liability, product labelling or selling practices, and data privacy protection); and

4 International Monetary Fund, 'Latin American Labor Markets during COVID-19', October 2020, https://www.imf.org/en/Publications/REO/WH/Issues/2020/10/13/regional-economic-outlook-western-hemisphere.

5 Aamer Madhani, 'U.S. imposes sanctions on China over human rights abuses of Uighurs', PBSO News Hour, December 2021 https://www.pbs.org/newshour/world/u-s-imposes-sanctions-on-china-over-human-rights-abuses-of-uighurs.

6 Press Release from the European Commission, 'Commission moves to ban products made with forced labour on the EU market', September 2022 https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5415. The Proposed Regulation is currently under review by the EU Parliament and Council.

- general stakeholders (e.g., human rights violations, human trafficking, and intrusions on local indigenous groups or other community groups).

The importance of the Social Pillar is increasingly evident through the focus of governments, regulators, consumers and citizens on one element in particular, the supply chain. Indeed, many jurisdictions, such as the United States, the United Kingdom and the European Union, have introduced a legal framework imposing obligations on companies in relation to the sources of their goods and services and the impact on their supply chains. A key example in recent years is the growth of legislation against modern slavery (i.e., slave-like exploitation, including human trafficking and forced labour).[7] Other aspects of the Social Pillar also include an increased focus on issues around diversity and inclusion, indigenous rights, personal privacy and other social issues – all of which are relevant to a wide range of stakeholders in a globalised world.

For its part, Latin America has not yet established a rigorous legal framework against which social issues can be assessed; however, consequences for non-compliance in this area can still be far-reaching and apply more broadly to a company – even if the conduct is contained within Latin America. In particular, if the underlying concern has any nexus to another country, whether through the organisational structure or location of the principal office, it can result in potentially significant consequences for a company.

Making progress under the Social Pillar can often require significant effort. Nevertheless, the potential impact of failings in this area can be serious. Reputational harm and negative brand publicity can discourage consumers from purchasing goods or services, dissuade investors from providing financing, and even result in stifling business to a halt. Other consequences of non-compliance or ineffective measures include financial risk (e.g., fines and injunctions), legal risk (e.g., employment law and other legal violations) and regulatory risk (e.g., financial criminal offences related to proceeds from illicit activity).

Measuring the Social Pillar

Although there is no global standard against which to measure success in this area, a number of frameworks are nonetheless instructive – including the UN Sustainable Development Goals (UN SDGs), Global Steering Group for Impact Investment (GSG), Global Reporting Initiative (GRI), UN Guiding Principles

7 Arathi Sethumadhavan, 'How to Stop Modern Slavery', World Economic Forum, January 2021, https://www.weforum.org/agenda/2021/01/how-to-stop-modern-slavery.

Reporting Framework, World Benchmarking Alliance, Sustainability Accounting Standards Board, Impact Reporting and the Investment Standards, and World Economic Forum.

The UN SDGs, adopted by all UN Member States in 2015 as part of the 2030 Agenda for Sustainable Development, contain 17 sustainable development goals aimed at tackling systemic global economic, social, and environmental challenges.[8] Of particular relevance to the Social Pillar are:

- UN SDG 4: Quality Education (e.g., providing training opportunities to employees, including women, to help increase the number of adults who have technical and vocational skills);
- UN SDG 5: Gender Equality (e.g., implementing policies to end all forms of discrimination against women within the company, ensuring women have full and effective participation and equal opportunities for leadership at all levels of company decision-making);
- UN SDG 8: Decent Work and Economic Growth (e.g., promoting decent job creation, providing equal pay for work of equal value, taking immediate and effective measures to eradicate forced labour and end modern slavery within company operations and supply chains, securing the elimination of child labour from business activities and supply chains, protecting the labour rights of workers, and promoting safe working environments for all workers including migrant workers);
- UN SDG 10: Reducing Inequality (e.g., ensuring equal opportunities in company recruitment and promotion criteria or processes, implementing non-discrimination policies and reporting procedures, and providing training on discrimination including unconscious bias); and
- UN SDG 16: Peace, Justice and Strong Institutions (e.g., considering human rights violations, exploitation, and trafficking in compliance risk assessments).

In 2019, the World Economic Forum's International Business Council (IBC) flagged the lack of consistency and comparability of metrics, arising from the existence of multiple ESG reporting frameworks, as preventing companies from credibly demonstrating their progress on sustainability and their contributions to the UN SDGs to all of their stakeholders.[9] Consequently, the IBC invited the

8 United Nations, 'Transforming our world: the 2030 Agenda for Sustainable Development', August 2015, https://sdgs.un.org/2030agenda.

9 Deloitte, EY, KPMG, PwC and World Economic Forum, 'Measuring Stakeholder Capitalism Towards Common Metrics and Consistent Reporting of Sustainable Value Creation',

World Economic Forum, in partnership with Deloitte, EY, KPMG and PwC, to coordinate a set of universal ESG metrics and recommended disclosures that could be consistently reflected in a company's annual report. This process culminated in a set of 21 'core metrics' and 34 'expanded metrics' related to ESG.

The core metrics comprise more established quantitative metrics that are likely already being recorded by companies (e.g., employee diversity statistics) or metrics that can be calculated based on readily available information (e.g., pay equality ratios through comparative compensation analysis for each employee category taking into account gender and ethnic considerations). The expanded metrics are a combination of more advanced metrics and disclosures which are less likely to be found in existing practice and standards. These include the number of discrimination and harassment incidents within a company, the status of the incidents and actions taken, and the total amount of monetary losses as a result of any related legal proceedings.

The Social Pillar in Latin America

We have seen a few examples of how the increased focus on the Social Pillar in Latin America has worked in practice – examples that also underscore how these issues can have a real impact on businesses operating in the region.

One example highlights a focus on supply chain issues – specifically, Olam International is facing an enforcement action by Brazilian prosecutors for allegedly failing to address child and slave labour abuses in its supply chain.[10] Brazilian prosecutors filed the lawsuit against the cocoa processor in January 2021 and are seeking around 300 million reais (approximately US$58 million) in damages. In another example, over 200,000 Brazilian claimants (comprising individuals, businesses and municipal governments) affected by the devastation of the collapse of the Fundão dam in 2015 launched proceedings in the United Kingdom against the English ultimate parent company of the Brazilian dam operator.[11] This case is one of the latest in a trend by which English courts have shown their openness to consider claims of alleged violations of business and human rights abroad.

September 2020, https://www3.weforum.org/docs/WEF_IBC_Measuring_Stakeholder_Capitalism_Report_2020.pdf.

10 Fabio Teixeira, 'Olam International is being sued by Brazilian prosecutors for allegedly failing to address labor abuses in its supply chain', Thomas Reuters Foundation News, August 2021, https://news.trust.org/item/20210812130016-jf5im.

11 Jason Allen, 'Case Note: Município de Mariana & Ors v BHP Group plc, BHP Billiton plc and BHP Group Ltd: [2020] EWHC 2930 (TCC)', Blackstone Chambers, February 2021, https://www.blackstonechambers.com/news/case-note-munic%C3%ADpio-de-mariana-ors-v-bhp-

Of course, company strategy does not operate in a vacuum and so any decisions are necessarily influenced by the local economy and political landscape, as well as pressure from the media and other organisations. The unique circumstances of different Latin American countries across these factors means that any individual company's approach to the Social Pillar, including the practical steps that can be taken to mitigate risks under the Pillar, must be tailored with that context in mind. Nonetheless, as these examples illustrate, multinational companies operating in Latin America should remain vigilant as to the possibility of labour and human rights violations (among other areas covered by the Social Pillar) that could affect other parts of its corporate brand and structure.

Relevant social legal frameworks in Latin America

Governments of Latin American countries are at different stages of implementing legal frameworks on social issues. In addition to governmental regulation, a number of private companies and non-government bodies have created voluntary initiatives along these lines. For example, some Latin American countries are members of GSG. Established in 2015, GSG is dedicated to impact on investment and entrepreneurship to benefit people and the environment. It currently covers 35 countries through 30 National and Regional Advisory Boards, including Central America and Latin American countries (including Argentina, Brazil, Chile, Colombia, Costa Rica, Mexico and Uruguay). The Regional Advisory Boards promote and facilitate the development of impact investment in the countries in which they operate. GSG encourages the incorporation of ESG factors into decision-making or reporting activities, even when not required by local legislation. GSG also encourages taking positive steps to combat social issues (e.g., pledging to end forced labour and cutting ties with businesses profiting from slavery, including marginalised groups and victims of conflict in employment).

In addition, a number of private companies in the region participate in the UN Global Compact, a non-binding UN pact calling for private businesses worldwide to respect labour rights, the environment, and human rights by adopting sustainable and socially responsible policies.

---

group-plc-bhp-billiton-plc-and-bhp-group-ltd. See also *Município de Mariana & Ors v BHP GROUP (UK) LTD (formerly BHP GROUP PLC) and BHP Group Ltd* [2022] EWCA Civ 951.

Countries	Member of GSG	Number of organisations participating in UN Global Compact[12]
Argentina	Y	391
Brazil	Y	1,525
Chile	Y	137
Colombia	Y	597
Costa Rica	Y	35
Mexico	Y	883
Peru	N	116

Brazil

Brazil has an established legal framework for employment and labour rights at both a national and federal level. Specifically, Brazilian Law (Law No. 13,146/2015) sets quotas for the employment of disabled persons depending on the size of the organisation. In addition, Brazilian Law (Law No. 7,716/1989) criminalises situations where employment is denied or impeded by a private company based on race, ethnicity, religion or national origin. Furthermore, Brazilian Law (Law No. 14,133/2021) prohibits companies that have been legally convicted for the exploitation of child labour or the submission of workers to conditions analogous to slavery from participating in bidding processes.

In 2022, the Brazil's National Monetary Council (CMN) and the Brazilian Central Bank (BCB) issued a number of resolutions aiming to improve the rules for the management of social, environmental and climate risks applicable to financial institutions and other institutions under BCB's purview, resolutions that also included the requirements related to the establishment of social, environmental and climate responsibility policies and related to the implementation of actions designed to ensure effectiveness of such policies.[13] The Brazilian president has also approved Decree No. 11,129/2022, which changes the methods public authorities use to evaluate companies' compliance programmes. In 2022, the country also saw the presentation of the Brazilian Bill (PL 572/22), which will enact a national framework on business and human rights framework that aims to establish guidelines to enforce national and international standards on the

12 As of 24 February 2023.

13 Resolution CMN No. 4,943/2021, Resolution CMN No. 4,945/2021 and Resolution BCB No. 151/2021, which became effective on 1 July 2022, and Resolution CMN No. 4.944/2021 and Resolution BCB No. 139/2021, which will become effective on 1 December 2022.

protection of human rights, and the promotion of related public policies. In other words, corporations will be held accountable for violations of human and labour rights, including activities in their subsidiaries, suppliers and any other entities in the global value chain, a regulation that would bring Brazilian legislation closer to international or globally recognised ESG standards.

However, until Brazilian Bill 572/22 comes into force, which is currently under negotiation, the only unified standard with respect to upholding human rights in companies in Brazil is voluntary. The November 2018 National Guidelines for Business and Human Rights (Decree No. 9,571/2018) detail the concepts in the UN Guiding Principles on Business and Human Rights for companies operating in Brazil. Although, in general there is no express legal obligation to present reports or disclosures relating to human rights issues, companies in certain sectors, such as the mining industry, are subject to disclosure requirements for violations in these areas. In fact, Brazil was one of the first countries in Latin America to mandate ESG regulation in the financial sector. Certain Brazilian financial institutions are required to manage ESG risks and to establish an environmental and social responsibility policy in accordance with Brazilian regulation (Resolution No. 4327/2014 and Resolution No. 4557/2017). More recently, starting in 2022, Brazilian banks are required to consider ESG risks alongside traditional financial risks (BCB Resolution 139/2021).

Despite its relatively more developed legislative framework compared to other Latin American countries, Brazil does not yet have a National Action Plan (NAP) on Business and Human Rights, as the federal government's attempted public bid (in collaboration with the private sector) was later cancelled.[14]

As a private sector initiative, the Brazilian Business Council for Sustainable Development (CEBDS) is a non-profit civil association that brings 60 of the largest Brazilian organisations together to implement sustainable business practices – including providing employees with human rights awareness training, establishing diversity and inclusion committees to develop inclusive strategies, and encouraging support networks (e.g., for LGBTQ+ employees).[15] The CEBDS directly affect over 1 million jobs across Brazil.[16]

---

14 Brazil, ICLG – Environmental, Social & Governance Law 2023, https://iclg.com/practice-areas/environmental-social-and-governance-law/brazil.

15 CEBDS, 'Breaking down walls and building bridges: diversity, inclusion and equity', June 2019, https://cebds.org/publicacoes/quebrando-muros-e-construindo-pontes-diversidade-inclusao-e-equidade/#.YhyjdavP1aQ.

16 CEBDS, 'About us', https://cebds.org/en/about-cebds/about-us/.

Since 2004, Brazil has maintained a 'dirty list' of employers, made up of companies and individuals who have been found guilty of using slave labour. Although there is currently no legal punishment for a company or individual who is on this list, those featured are barred from receiving public financing and have limited access to private loans. In 2022, evidence emerged that offenders connected with previous political regimes were able to avoid the 'dirty list'.[17] An increase in the number of companies being investigated by the Labour Protection Office that same year, as well as a recent political shift, may signal further improvement to come.

Chile

Since becoming the first Latin American country to launch the UN Global Impact in October 2001,[18] Chile has continued to put social issues at the forefront of companies' agendas. In 2017, the Chilean government published its first NAP on Business and Human Rights (2017–2019), which contains 158 action points for specific government institutions based on stakeholder recommendations and other relevant agendas, including the UN 2030 Sustainable Agenda and UN SDGs. [19] On 4 March 2022, Chile published its second NAP; however, this has received criticism for being hastily approved, reflecting a lack of civilian participation (particularly that of indigenous people and vulnerable groups), and containing little emphasis on the responsibility of private companies to respect human rights.

In November 2021, the Financial Market Commission (CMF), the Chilean financial regulator, issued secondary legislation, General Rule No. 461, which amends the structure and content of annual reports of certain organisations, including banks, insurers, issuers of publicly offered securities and general fund managers.[20] General Rule No. 461 specifically sets out the obligation to report on

17 Beth Duff-Brown, Stanford Health Policy, 'Investigation Into the "Dirty List" of Slave Labor in Brazil Focus of Prize-Winning Thesis', 9 June 2022, https://healthpolicy.fsi.stanford.edu/news/investigation-%E2%80%98dirty-list%E2%80%99-slave-labor-brazil-focus-prize-winning-thesis.

18 UN News, 'Chile first in Latin America to launch Global Compact, UN agency reports', https://news.un.org/en/story/2001/10/17022-chile-first-latin-america-launch-global-compact-un-agency-reports.

19 Chile National Action Plan on Business and Human Rights, 2017, https://media.business-humanrights.org/media/documents/files/documents/NATIONAL_ACTION_PLAN_ON_BUSINESS_AND_HUMAN_RIGHTS_.pdf.

20 Comisión Para El Mercado Financiero, 'CMF issues regulation incorporating sustainability and corporate governance requirements in Annual Reports', November 2021, https://www.

ESG factors, such as information on people who provide services to the company, including aspects of diversity, pay gaps, occupational safety, and workplace harassment and discrimination.

Although there is no single government body dedicated to promoting ESG in Chile, there are a number of public agencies that have implemented initiatives to promote sustainability and responsible investment practices.[21] For example, the CMF are working on an amendment of the new reporting obligations under NCG 386 aimed at strengthening the adoption of ESG principles.

To put the effectiveness of Chile's NAPs and other regulatory measures into context, in January 2022 the ILO and the World Benchmarking Alliance released a human rights snapshot of 29 Chilean companies, scoring them against the United Nations Guiding Principles on Business and Human Rights.[22] Chile scored nine points out of the maximum score of 24 points, showing that there is still plenty of room for improvement.

That said, Chile has demonstrated a more recent commitment to ESG-related topics in general. For example, in March 2022, Chile became the first country in the region to issue a sovereign sustainability-linked bond. This US$2 billion bond adheres to the Paris climate accords and includes commitments to reduce carbon dioxide emissions and increase renewable energy production to 60 per cent of electricity needs by 2032. With this new issuance, Chile has placed over US$33 billion in socially and environmentally responsible bonds in the past three years, being the only country in the world to have such sustainability-linked bonds.[23] Along similar lines, on 13 June 2022, Chile published its Climate Change Framework Law, which includes a binding target of net zero emissions by 2050,

---

cmfchile.cl/portal/principal/613/w3-article-49809.html.

21 Cristián Eyzaguirre, Francisco Guzmán, and Benjamín Sáa, 'Getting The Deal Through, ESG and Impact Investing 2021, Chile', 2021, Carey, https://www.bloomberglaw.com/product/blaw/document/28219833896.

22 Pontificia Universidad Católica de Chile, 'Primer Diagnóstico Empresas y Derechos Humanos Chile 2022', https://sostenibilidadcorporativa.uc.cl/images/investigacion/Primer_Diagnostico_Empresas_y_DDHH_Chile_2022.pdf.

23 Ryan Jeffrey Sy, 'World's 1st Sovereign Sustainability Linked Bond issued by Chile', S&P Global Intelligence, 4 March 2022, https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/world-s-1st-sovereign-sustainability-linked-bond-issued-by-chile-69226229.

creating cross-agency and departmental coordination and cooperation beyond the Ministry of the Environment to make carbon emissions compliance, targeting, and goals a matter of national importance.[24]

Colombia

Colombia published its first National Action Plan (NAP) on Business and Human Rights (2015–2018) in December 2015, and its second edition (2020–2022) in December 2020, which captured covid-19 considerations. The second NAP serves as a tool for companies, regardless of size or sector, to promote, protect, and repair the human rights of workers and families affected by decreased income and suspended employment contracts, among other negative impacts of the covid-19 pandemic.[25] There has not yet been any announcement of a third edition.

An award-winning online platform,[26] the SDG Corporate Tracker Colombia, assists companies in assessing their contribution towards achieving the UN SDGs.[27] The initiative is supported by the GRI, the National Planning Department of Colombia, and the UN Development Programme. Over 670 companies have registered on the platform. The tracker assists with the information collection process as well as reporting and analysis of ESG performance against GRI standards related to (1) employment rights and labour conditions;[28] (2) community interests;[29] (3) supply chain risks;[30] and (4) customer welfare.[31]

---

24 Robert Currie Ross, 'Chile Adopts New Climate Change Framework Law: A Paradigm Shift', 22 June 2022, Climate Law Blog, Sabin Center for Climate Change Law, Columbia Law School, https://blogs.law.columbia.edu/climatechange/2022/06/22/chile-adopts-new-climate-change-framework-law-a-paradigm-shift.

25 Colombia National Action Plan on Business and Human Rights, December 2020, http://www.derechoshumanos.gov.co/Prensa/2020/Documents/Plan-Nacional-de-Accion-de-Empresa-y-Derechos-Humanos.pdf.

26 Global Reporting Initiative, 'Breaking new ground for SDG reporting in Colombia' https://www.globalreporting.org/news/news-center/breaking-new-ground-for-sdg-reporting-in-colombia/.

27 UN SDG Corporate Tracker Colombia, https://sdgs.un.org/partnerships/sdg-corporate-tracker-colombia-sdg-ct.

28 e.g., GRI 401: Employment, GRI 403: Occupational Health and Safety, GRI 404: Training and Education, GRI 405: Diversity and Equal Opportunity, GRI 406: Non-discrimination, GRI 407: Freedom of Association and Collective Bargaining, GRI 408: Child Labour, GRI 409: Forced or Compulsory Labour.

29 e.g., GRI 411: Rights of Indigenous Peoples, GRI 413: Local Communities.

30 e.g., GRI 414: Supplier Social Assessment.

31 e.g., GRI 416: Customer Health and Safety, GRI 417: Marketing and Labelling, GRI 418: Customer Privacy.

Mexico

Mexico's Constitution sets out a general framework on human rights, child labour and slavery issues, implemented at both the national and the federal level. Relevant legislation includes the State Trafficking in Persons Law prohibiting forced labour; the Federal Labour Law concerning working conditions and employment issues, including striking and unionisation; and the Federal Regulations on Health and Safety at Work, which sets minimum standards of environmental, health and safety conditions in the workplace.[32],[33]

In 2020, the Mexican government published a National Human Rights Programme 2020–2024, which includes a section dedicated to business and human rights.[34] This followed an attempt to develop a specific Human Rights and Business Programme (2015–2018) to promote greater respect for human rights in business activities.[35] In its third UN Voluntary National Review in 2021, the Mexican government underscored a continued commitment to correct historical social debts by implementing measures focused on closing inequality gaps, eradicating poverty, and ending corruption, among other topics.[36]

In Mexico, like in Colombia, progress in these areas and towards achieving other UN SDGs is being tracked via an online platform, which was launched in 2018.[37] The platform, titled 'Information System of Sustainable Development Goals (SIODS)', provides a centralised location for data from various Mexican

32 Carlos Escoto, Mariana Herrero, Marianela Romero Aceves, Lorena Kiehnle Barocio, 'Mexico: Environmental, Social & Governance Law 2022', ICLG.com, December 2021, https://iclg.com/practice-areas/environmental-social-and-governance-law/mexico.

33 US Department of Labor, 'Child Labor and Forced Labor Reports: Mexico', December 2020, https://www.dol.gov/agencies/ilab/resources/reports/child-labor/mexico.

34 Mexico National Human Rights Program 2020–2024, December 2020, http://derechoshumanos.gob.mx/work/models/Derechos_Humanos/PNDH/Documentos/DOF-Diario_Oficial_de_la_Federacion-PNDH_2020-2024_Programa.pdf.

35 Government of Mexico, 'Addressing Human Rights in All Spaces and Environments: Working Group on Business and #DDHH', March 2017, https://www.gob.mx/segob/articulos/abordar-los-derechos-humanos-en-todos-los-espacios-y-entornos-grupo-de-trabajo-sobre-empresas-y-ddhh?idiom=es.

36 Mexico Voluntary National Review, 2021, InfNalVol_FPAN_DS_2021_es.pdf (agenda2030.mx).

37 International Institute for Sustainable Development SDG Knowledge Hub, 'Mexico's SDG Portal Brings Functionality to Reporting', August 2018, https://sdg.iisd.org/news/mexicos-sdg-portal-brings-functionality-to-reporting.

governmental departments and agencies.[38] It also allows users to track indicator data and targets related to the UN SDGs at a provincial level, and compare them against the national average collected by the government.

More recently, in February 2023, as part of the United States–Mexico–Canada Agreement, Mexico issued a resolution that aims to prohibit the import of goods produced with forced labour.[39] The commitment under the tripartite trade agreement comes into effect as of May 2023 and will establish a process whereby civilians (as well as the government) can instigate an investigation into the provenance of a company's goods. Another recent and noteworthy ESG-related update in Mexico (beyond the 'S' specifically), includes the fact that Mexico's pension fund regulator (CONSAR) has published rules regarding investment strategies that include an obligation to analyse companies' social responsibility credentials, which became effective in January 2022. As a result of these rules, retirement funds in Mexico will be required to incorporate sustainability criteria in their methodologies, prioritise ESG investments in their portfolios, and advocate within the public companies in which they are represented for compliance with such principles.[40]

Peru

In 2018, Peru adopted its third National Human Rights Plan (PNDH) 2018–2021, setting forth five strategic alignments that correspond to the UN SDGs. The fifth strategic alignment highlights the duty of private and public companies to progressively implement international human rights standards.[41] Following the Organisation for Economic Co-operation and Development (OECD) Responsible Business Conduct Policy Review on Peru in 2020,[42] the Peruvian government published a National Action Plan (NAP) on Business and Human

38 Information System of Sustainable Development Goals, https://www.agenda2030.mx/#/home.

39 Press Release from the Office of the United States Trade Representative, February 2023, 'Statement from Ambassador Katherine Tai on Mexico's Action on Imports Produced with Forced Labor', https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/february/statement-ambassador-katherine-tai-mexicos-action-imports-produced-forced-labor.

40 Environmental, Social & Governance Law Mexico 2022, Global Legal Group.

41 Peru Support Group, February 2018, https://perusupportgroup.org.uk/2018/02/peru-sets-out-human-rights-plan.

42 Organisation for Economic Co-operation and Development, 'OECD Responsible Business Conduct Policy Reviews: Peru', 2020, https://www.oecd.org/daf/inv/mne/oecdresponsiblebusinessconductpolicyreviewsonperu.htm.

Rights (2021–2025) in 2021.[43] The NAP contains recommendations for companies to strengthen measures across a range of issues, including forced labour and child labour within supply chains, employment rights and non-discrimination.

Peruvian Law 30709 prohibits wage discrimination on the basis of gender and protects pregnant or breastfeeding women against dismissal. The Peruvian government, through the Ministry of Labour and Employment and the Ministry of Women and Vulnerable Populations, has promoted and recognised diverse and inclusive companies through schemes like 'Perú Responsable' (Peru Responsible) and 'Sello Empresa Segura' (the Safe Company Seal). Although Peru historically had a poor reputation for the treatment of human rights defenders,[44] the country has also seen further measures to clamp down on sexual discrimination in the workplace including protection for domestic workers and against the victimisation of complainants and 2022 saw the national minimum wage increased for the first time in four years.[45]

However, in 2022, Peru failed to meet the US Department of State standards for the elimination of human trafficking, in part due to lack of government funding and failure to prosecute complicit officials. Support for marginalised groups, including young males and LGBTQ+ individuals, was deemed inadequate. That said, Peru was praised for its overall increase in efforts considering the impact of covid-19, which included more successful convictions of traffickers and the adoption of the National Policy against Human Trafficking.[46]

Practical considerations

Companies assessing performance under the Social Pillar should consider the key risks that could exist across the following categories.

43 Peru National Action Plan on Business and Human Rights, June 2021, https://globalnaps.org/wp-content/uploads/2021/06/plan-nacional-de-accion-sobre-empresas-y-derechos-humanos-2021-2025pdf.pdf.

44 Amnesty International Report on Peru 2021/22, https://www.amnesty.org/en/location/americas/south-america/peru/report-peru/.

45 L&E Global, 'Peru: Summary of Recent Employment Law Developments', https://leglobal.law/2022/04/20/peru-summary-of-recent-employment-law-developments/.

46 US Department of State, '2022 Trafficking in Persons Report: Peru', https://www.state.gov/reports/2022-trafficking-in-persons-report/peru__trashed/.

Employees

Issues to consider here could include the risk of undocumented remuneration; underage workers or children; workers seemingly working without any formal employment contracts in place; employees working long hours without breaks; underpayment or deductions from salaries (e.g., to repay loans); the presence of hazardous materials, dangerous working conditions or a lack of necessary safety equipment; and a general lack of safeguarding policies and training and reporting procedures in place to protect workers (e.g., health and safety policies and incident logs, harassment or discrimination reporting and disciplinary procedures, whistleblower channels and protections, and employee data privacy policies).

Suppliers

In terms of suppliers, companies are increasingly requiring suppliers to have the same safeguarding policies, training and checks in place as are applied to their own businesses. Supply chain audit rights are increasingly utilised as a way to confirm that suppliers adhere to the agreed standards (e.g., organising a periodic inspection of a farm or factory to assess working conditions).

Customers and the community

Related to customers and the community, companies should consider (among other areas) product quality, safety and general fitness for purpose; the manner in which products are labelled, advertised, or otherwise marketed to consumers (e.g., the accuracy or fairness of the product labelling or description, the tone of the marketing materials and advertisements, and the intended audience of the marketing approach); how the company or company website collects and manages personal data from the individuals who interact with it; and general customer and community engagement (e.g., review processes, complaint handling procedures, and participation in wider community events).

Conclusion

ESG has captured the world's attention, and the 'S' in particular has increasingly become a focus for a variety of stakeholders. Given the breadth of this pillar's application, and its significance for companies, tackling and managing the Social Pillar is an involved task. Nonetheless, companies that have taken action to pre-emptively mitigate risk in these areas enjoy an increasing competitive advantage as governments begin imposing requirements on managing and measuring compliance on social issues.

Given these trends, companies in Latin America should start actively assessing the risks and consider what proactive risk mitigation measures can be implemented now as part of the company's broader compliance programme and environment. It is just a matter of time before local law and private initiatives in Latin America start to close the gaps and render serious consequences for non-compliance. While it may be difficult to gain traction in these areas, particularly given the ongoing challenges in the aftermath of the covid-19 pandemic, companies that choose to be more forward-leaning when it comes to ESG compliance will be well served in the long run.

CHAPTER 20

Compliance as the Foundation for ESG Oversight

Martín Sánchez, Gabriel Calvillo, Adriana Morales and Paula Pérez Benítez[1]

The purpose of this chapter is to provide a general overview of certain environmental, social and governance (ESG) matters, risks, regulations and best practices for effective ESG oversight in the Latin American region, with a special focus in Mexico, based on our experience and the challenges that we have faced.

ESG outlook: Mexico

ESG has been on the agenda over the past few years in Mexico's corporate and finance sectors. Emphasising these areas has proven to be helpful in improving companies and keeping them resilient. In recent years, with changing environments due to political and economic instability, climate change, and changes in social dynamics and consumer habits, it has become more evident that companies can no longer be managed based solely on an economic perspective, hence the growing demand from investors to ensure that business models consider ESG factors as one of the main drivers of the company's strategy.

The changing business environment has made the sustainability of companies more complex over time. Certain practices and factors that have emphasised ESG issues in Mexico, and that are driving accelerated changes in business practices, making companies more aware of the manner they operate and the consequences and implications of their business models, include the following:

1 Martín Sánchez is a partner, Gabriel Calvillo and Adriana Morales are of counsel, and Paula Pérez Benítez is a senior associate at Mijares Angoitia Cortés y Fuentes SC.

- the transition of companies to zero emissions to mitigate negative effects on the environment and natural resources in accordance with international conventions;
  greener packaging of products aligned to circular economy tendencies;
  the tendency to produce and consume healthier products;
- pressure from foreign agencies to implement labour and human rights policies related to working conditions, the mental health of employees, gender equality and inclusion at the workplace;
- pressure from the finance and securities market towards more transparent corporate governance structures and compliance oversight frameworks;
- implementation of the Guiding Principles on Business and Human Rights as a result of visits of representatives of the United Nations;[2]
- the implementation of an ESG framework by Mexican pension funds that will require compliance of reporting obligations and to consider ESG factors as part of their investment decisions;
- initiatives from securities and banking regulators to enact ESG reporting regulations; and
- the indirect effects of ESG reporting regulations abroad, in particular in the EU.

Mexico's government sustainability agenda

In September 2015, the Member States of the United Nations, including Mexico, approved the 2030 Agenda for Sustainable Development. The 2030 Agenda for Mexico is a road map that sets a common horizon to guide multisectoral actions in favour of individuals, the preservation of the planet, economic prosperity by reducing inequalities, as well as promoting peace and alliances. This Agenda includes 17 Sustainable Development Goals (SDGs), 169 goals and 230 global indicators.[3]

Presentation of results of the 'Agenda 2030 Initiative' project of the German cooperation agency GIZ in Mexico at the Ministry of Economy took place on 24 January 2023.[4] The Initiative is part of a project that began a couple of years ago, where the German government and the government of Mexico joined efforts to implement practices in the country's states, promoting the governance approach,

2 https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf (last accessed on 7 March 2023).

3 Agenda 2030 | Gobierno | gob.mx (www.gob.mx). Last accessed on 7 March 2023.

4 Presentación de resultados del proyecto 'Iniciativa Agenda 2030' | Agenda 2030 | Gobierno | gob.mx (www.gob.mx). Last accessed on 7 March 2023.

improving the institutional and strategic architecture to accelerate progress. Among the achievements of the project, the following stand out: the accompaniment for the incorporation of the sustainability approach in legislative initiatives, the promotion of the mobilisation of financial resources and the implementation of inclusion measures through innovation for groups in vulnerable situations.

Mexico's Sustainable Taxonomy (the Taxonomy)[5] was presented on 16 March 2023, by the Ministry of Finance and Public Credit, the Taxonomy is a globally unique tool allowing a comprehensive approach to sustainability which includes the corresponding criteria that must be met in order to categorize an economic activity as sustainable, we will present later on this paper a broad analysis on what the Taxonomy represents in terms of ESG compliance.

In terms of environmental matters, the Mexican government has also implemented new environmental regulations; for example, the past administration promoted the use of renewable energy resources. However, there are still enormous challenges on this area, such as air and water pollution, deforestation, climate change mitigation and promoting the use of clean energy. On the social front, the most pressing issues are still inequality and poverty, and to continue the efforts to improve access to education, healthcare and social services. In the area of governance, there has been some improvement in the private sector in terms of transparency and accountability, mostly driven by the pressure of financial institutions and pension funds. However, the Mexican government has come short in the measures taken to address corruption, regulatory oversight in some areas and a standardised implementation of ESG compliance frameworks.

Key ESG risks in the region

As mentioned before, the implementation of ESG factors has taken on special importance during the last couple of years, with an emphasis on a variety of commercial operations, investments, financing and, in general, to the development and management of emerging and operating projects.

In a post-covid-19 pandemic world, where environmental, political, economic and social challenges are becoming more visible, the international efforts of the relevant public and private actors involved in this matter have intensified. All efforts are aimed at achieving a clear goal, to standardise ESG criteria at

5 https://www.gob.mx/shcp/documentos/taxonomia-sostenible-de-mexico?state=published Last accessed on 17 May 2023.

an international level, so that such standards can be applied homogeneously to organisations and projects. The main objective is the recognition and proper management of the ESG risks triggered by projects and the companies' activities.

From an optimistic standpoint, the fact that there is currently no international standards and binding application of ESG criteria has encouraged stakeholders in different countries in North America and Latin America to develop specific tools such as compliance programmes and policies to identify the ESG risks to which investments, financing, business development and companies' operations are subject. However, from another less encouraging point of view, the lack of homogeneity and application of binding international standards has opened the door to increasing green and social washing, which have had negative repercussions for those involved therein, generating lack of trustworthiness in the development of businesses in the medium and long term. A broad reference to green and social washing concerns will be reviewed later on this paper.

According to the Global Risks Report 2023 issued by the World Economic Forum,[6] it is necessary to differentiate the risks we face globally into three types: (1) current risks, (2) risks that are likely to become more serious in two years, and (3) risks that are likely to become more serious in 10 years. The main risks for the next two to 10 years – established in this report – relate to the practicality of mitigating climate change and adapting to it, as well as the loss of biodiversity and natural resources, which directly affect environmental, social and governance factors.

That said, the main risks are those relating to the development and implementation of accurate tools to assess and manage ESG risks, which should be helpful and suitable for each of the involved recipients. Another important risk that must be considered is the impact that ESG risks can have on investors, customers, communities, employees and companies, among others. It has become crucial to identify and address the responsibilities faced by each of the parties involved and the direct and indirect consequences that will be had regarding the recipients of such risks. In the private sector, the special focus on the positions and roles of board members, directors, and managers on ESG risk management and attention, is becoming increasingly visible.

In North America, the obligations of reporting and disclosure of climate, environmental and social risks and impacts of projects have gained relevance. Although in Latin American countries such as Mexico there is no legislation

6 https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf. Last accessed on 23 February 2023.

that requires companies to address ESG matters, in practice, due to reputational, commercial, market and transactional factors, it has become essential to disclose and manage strategies and to implement compliance programmes, policies and other key tools to monitor and manage ESG risks.

Given the increase in relevance of and adaptation to evolving ESG criteria, in recent years ESG risks have been considered as key issues in terms of decision-making for the development of projects in companies. While environmental and climate risks have been the most discussed, other important issues relating to diversity, gender equality and fair policies for employees in companies have also come to the fore.

Supply chain risks in the region

One of the most significant ESG changes is a recent proposal adopted by the European Commission for a directive on Corporate Sustainability Due Diligence (CSDDD) on 23 February 2022.[7] The CSDDD will require in-scope EU and non-EU companies to carry out due diligence on the human rights and environmental impacts of their supply chains, their subsidiaries and those of certain business partners; to prevent, mitigate or avoid adverse impacts; to monitor the effectiveness of their due diligence policies and measures; and to publicly communicate what they are doing on due diligence.

Those changes and additional regulations that are expected to come in the future will undoubtedly have a significant impact on global supply chains and supply agreements, as businesses wishing to retain access to lucrative markets will have to adapt their existing systems and processes to source, validate and provide the necessary information. A significant amount of capacity-building and preparation will be required to comply with these new requirements adopted by the CSDDD, as well as changes to procurement processes and contract terms and the creation of mechanisms to provide effective access to remedy.

For many businesses across the globe, including Latin America and Mexico, this will require main significant changes to the way the operation of the businesses has been managed and reported, as well as considering the way they interact with their business partners.

These new regimes also play into the overarching ESG theme of greater transparency and accountability to enable key stakeholders to make better-informed decisions and is a good illustration of how the social and governance components of ESG are developing into mandatory requirements.

---

7 Corporate sustainability due diligence (europa.eu) Last accessed on 7 March 2023.

ESG in Mexico, taxonomy and examples of other relevant local laws

As mentioned above, Mexican government published an official Taxonomy providing a classification tool to determine the economic sectors and activities including that can be considered as sustainable. The Taxonomy establishes three objectives: mitigation of climate change, gender equality and access to adequate basic services related to sustainable cities. The Taxonomy is directed to six economic sectors:

- agriculture, livestock breeding, forestry and logging;
- generation, transmission, distribution, and commercialisation of electric power and supply of water to the final consumer;
- construction;
- manufacturing industries;
- transportation; and
- waste management and remediation services.

To align the 124 activities comprehended in such economic sectors, the following aspects must be met: eligible activities must be included in the Taxonomy, such activities must be classified under various metrics and thresholds, Non-Significant Harm (NSH) criteria must be met, and activities have to maintain minimum safeguards.

The use of the Taxonomy will require an ethical behaviour from organisations that intend to communicate to their stakeholders that their economic activity is sustainable, according to criteria of legitimacy and based on science, and therefore it seeks to reduce the risks of green and social washing. Notwithstanding that the Taxonomy has no direct regulatory objectives, which means it is beyond compliance regarding environmental regulation and legislation protecting human rights, it will provide certainty and transparency to financial markets and investment in sustainable activities. The Taxonomy also establishes cross-guidelines to identify activities to ensure compliance with gender equality. Below, we describe examples of other Mexican regulations involved with ESG aspects.

Governance aspects

The board of directors, consistent with its duty of loyalty, must take ESG factors into account, implementing and monitoring systems to identify material risks and address risks once identified, to preserve and protect the value of the company in the long term. It is imperative that companies monitor and address these ESG risks, as such risks can damage and alter strategies, business positioning, operations, and relationships with relevant parties in the company, being essential to guarantee its long-term sustainability.

Under Mexican law, the mains aspects of corporate governance in charge of regulating integration of the board of directors, vigilance, shareholders' rights and obligations, minority rights are outlined in the General Law of Commercial Companies. For public companies, specific regulations are in place, such as the Stock Exchange Law and soft law such as the Best Corporate Practices Code and principally the general provisions applicable to issuers of securities and other participants of the securities' market, where they are obliged to publish an annual report disclosing environmental policies, certificates, projects, relevant impacts and explain whether their activities represent a potential risk.[8]

It is worth mentioning that many Mexican public companies, such as Grupo Femsa, Grupo Bimbo, Grupo Modelo and Cemex, are already being consistent with its duty of loyalty on sustainability to generate the appropriate social, environmental, and economic conditions to operate and continue to grow and leading different actions for change.[9] Many of such public companies are signatories to the United Nations Global Compact and are adhered to its 10 principles to protect human rights, maintain ethical labour practices, preserve the environment and combat corruption. For such purposes, there is a tendency in public companies to create specific committees (sustainability, inclusion or diversity committees) to continue strengthening the company's strategies regarding ESG matters, among other objectives to contribute on increasing customer satisfaction, operational continuity and reducing costs.

Corporate bribery, money laundering, corruption, lobbying and donations regulations are overseen by the (1) Federal Law to Prevent and Identify Transactions with Illegal Funds, (2) the General Law of the National Anticorruption System, (3) the General Administrative Liabilities Act, (4) Local and Federal Criminal Laws (5) the Securities' Exchange Law and (6) the Investments Fund Act, among others.

Tax and fiscal planning are overseen in the Fiscal Code of the Federation and local codes.

One relevant topic worth mentioning is that there is a working team comprising authorities and participants of the Mexican stock market who are working on the most recent amendment project to the Securities Market Law. Within this project, a new section is being considered that would grant the

8 Grupo BMV Regulations issued by the authorities and other entities. Last accessed on 7 March 2023.

9 *4 empresas mexicanas y sus acciones a favor del medio ambiente* (forbes.com.mx). Last accessed on 7 March 2023.

Ministry of Finance, prior opinion of the Securities and Banking Commission and the Mexican Central Bank, authority to establish general provisions regarding sustainable and equitable development. These provisions are expected to apply to securities issuers, brokerage firms, stock exchanges, rating agencies and other participants in the Mexican market.

Finally, in terms of ESG regulations, the National Commission of the Retirement Savings System (CONSAR) currently has a regulation on ESG investments and, therefore, the 10 Retirement Fund Administrators (AFORES) have been incorporating these aspects into their strategies as of 1 April 2022, and must include in the analysis of characteristics and risks inherent to the investments they make, an analysis of the adherence of the issuers to ESG standards.[10]

CONSAR also published on 27 September 2022 a regulation establishing that the AFORES already have the obligation to have a continuous training programme for its personnel related to ESG principles.[11]

The Mexican AFORES worked together on 2022 with the AMAFORE, which is the Mexican Association of AFORES, in the standardisation of an ESG questionnaire for public companies, which is expected to be disclosed and implemented by mid 2023.[12]

Environmental aspects

From an environmental standpoint, Mexico has enacted diverse regulations in which ESG aspects have been addressed. Environmental regulations derived from the human right to a healthy environment that is set forth in the Mexican Political Constitution, for purposes of national development the Constitution provides that social, public and private sectors must concur.

Mexican environmental laws relevant to ESG aspects are: (1) the General Law of Ecological Equilibrium and Environmental Protection, (2) the General Law of Prevention and Comprehensive Management of Waste, (3) the General Climate Change Law, and (4) the Federal Environmental Liability Law.[13]

Federal environmental regulations establish diverse principles in which environmental policies must be based, the principles related with ESG aspects recognise jointly accountability between public and private sectors regarding the

10 Inversiones ASG benefician a AFORE de Trabajadores | PENSIONISSSTE | Gobierno | gob.mx (www.gob.mx). Last accessed on 7 March 2023.

11 CUF_20220927.pdf (www.gob.mx). Last accessed on 7 March 2023.

12 Amafore | Asociación Mexicana de Afores. Last accessed on 7 March 2023.

13 Leyes y Normas del Sector Medio Ambiente | Secretaría de Medio Ambiente y Recursos Naturales | Gobierno | gob.mx (www.gob.mx). Last accessed on 7 March 2023.

protection of the natural resources towards the achievement of ecological balance. Moreover, they state that the subjects of ecological consensus are not only individuals, but also social groups and organisations, being the main purpose of concerting ecological actions to reorient the relation between society and nature.

Finally, it is important to mention that the Federal Environmental Liability Law provides certain aspects relevant to sustainability compliance under ESG matters, this becomes relevant due to such law recognises the minimum requirements to elaborate an environmental compliance system under Mexican law. In addition, local jurisdictions, such as, the Environmental Liability Law of the State of Coahuila have implemented environmental compliance elements establishing an environmental risk compliance.

Social aspects

From a social standpoint, relevant matters such as human rights, prohibition of discrimination and child labour issues are found in the Mexican Political Constitution, with specific laws, to name a few: (1) the National Human Rights Commission Law, (2) the National Security Law, (3) the General Law on Victims, (4) the Federal Act for the Prevention and Elimination of Discrimination, (5) The Federal Labor Law, and (6) the Federal Regulations on Health and Safety at Work. In addition, there are certain state regulations enacted to prevent and eradicate human trafficking.[14,15]

The Federal Labor Law addresses working conditions and employer-employee relations, including the right of unionisation, and striking. Likewise, the Federal Regulations on Health and Safety at Work, outline the minimum environmental, health and safety conditions that must be observed at the workplace.

Best practices for effective ESG oversight

An organisation's ESG commitment is first and foremost an ethical commitment. Understood as corporate action motivated by a deep understanding of the negative impacts that human behaviour has had on human rights and the environment, ESG strategies reflect a movement towards organisational ethics and correctness.

In November 2022, the 27th Conference of the Parties to the United Nations Framework Convention on Climate Change (COP27), that took place in Egypt concluded with several historic decisions, public pronouncements and documents

14 Marco Normativo | Comisión Nacional de los Derechos Humanos – México (cndh.org.mx). Last accessed on 7 March 2023.

15 Orden Jurídico Nacional (ordenjuridico.gob.mx). Last accessed on 7 March 2023.

with ethical implications. Among the latter, the Report from the High-Level Expert Group on the Net Zero Emissions Commitments of Non-State Entities entitled Integrity Matters: Net Zero Commitments by Businesses, Financial Institutions, Cities and Regions (the Report),[16] comprises an important message regarding ethical behaviour in sustainability. The Report addresses green- and social-washing concerns raised by citizens, environmentalist, investors and consumers, and emphasises the need to prevent dishonest actions in sustainability efforts. It also contains strong recommendations to effectively tackle unethical, misleading and even deceptive information disseminated by organisations with the purpose to present an environmentally responsible public image.

In our opinion, the COP27 greenwashing prevention actions can also be applied to social washing deterrence and unethical governance behaviour. ESG commitments and disclosures ought to be accurate, reliable and subject to ethical controls. The Report recommends increased transparency and accountability actions in financial and non-financial institutions that should seek independent evaluation of metrics and targets, internal controls, the establishment of a process to receive and review public complaints, and internal mechanisms to ensure that their governance avoid conflicts of interest. All of this represents a call for ESG compliance.

Corporate ethical compliance is rapidly becoming an essential part of business environmental and socially responsible operations in the region. In the context of the environmental and human rights litigation that has followed the implementation of the Regional Agreement on Access to Information, Public Participation and Justice in Environmental Matters in Latin America and the Caribbean,[17] also known as the Escazú Agreement, ESG's three pillars of environmental, social and governance have the potential to become targets of concern and potential detonators for conflict and litigation. One example of an ESG landmark case that revealed unethical corporate behaviour and misleading and deceptive dissemination of ESG relevant information is the well known international diesel emissions fraud that had local effects in Latin America. In Mexico, the effect of this reflected on several car manufacturers that were penalised for commercialising vehicles without environmental emissions certificates despite the corporate commitment with the protection of environmental human rights.

16 https://www.un.org/sites/un2.un.org/files/high-level_expert_group_n7b.pdf. Last accessed on 2 March 2023.

17 https://treaties.un.org/doc/Treaties/2018/03/20180312%2003-04%20PM/CTC-XXVII-18.pdf. Last accessed on 2 March 2023.

These sorts of cases encourage social suspicion and increase the concerns of communities, investors, regulators and other corporate interest groups that need to be addressed by ESG compliance.

In Mexico, due to the publication of the Taxonomy, ESG compliance shall be implemented for ensuring that companies, organisations, or entities use the criteria, metrics and thresholds provided in such Taxonomy ethically and in accordance with applicable laws, regulations, standards and practices. This is a relevant issue for compliance officers, who must identify the inherent risk scenarios that green and social washing will generate for the company, as well as to adjust the control environment to ensure the application of Non-Significant Harm principles and promote the transparency that allows the financial sector and different stakeholder groups of organisations to have confidence in the classification and sustainability rating of business activities.

CSO and ESG ethical oversight

ESG has brought new roles within companies and their organisational structures. The emerging figure of the chief sustainability officer (CSO) who joins the C-suite is a clear example of the recent development in the corporate organisational design that responds to the need of assigning duties of coordinating the organisation's sustainability efforts to a dedicated professional. Tracking sustainability performance, reporting and ensuring compliance with ESG frameworks and standards are day-to-day tasks that should be carried out within the control and supervision ethics environment of the organisation.

The interaction of the ethics compliance officer and the CSO in a day-to-day basis is seen as a rapidly emerging compliance best practice in Latin America. The new relationship of the ESG function implies its role as first line of defense against green- and social-washing. The ethical compliance work will remain as the second line of defence needed to prevent ESG conflicts and litigation that can arise from social concern, operational incidents and the perception of unethical, misleading, or deceptive ESG information dissemination by the organisation. The above has led to a deeper understanding of the role of compliance as a basic tool for ESG oversight, being the cornerstone for any company to supervise compliance with the applicable regulatory framework and the ESG commitments assumed with the company's stakeholders (lenders, investors, clients and authorities).

Building on existing compliance infrastructure

An ethical ESG function should be constructed upon the existing organisations' control environment. Sustainability commitments should be accompanied with a pledge for transparency and accountability within the organisation's code of ethics.

Companies should welcome ESG-related public complaints that can and should be process through current ethical channels. The ESG function should also be subject to compliance controls and independent evaluation of metrics and targets assigned to internal or external audit. Persons that report unethical and otherwise incorrect conducts associated to the organisation ESG commitments should be awarded protection under international recognised standards and regulations such as the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.[18]

ESG risk identification

One important process required to build ESG accountability and transparency is ESG risk identification. This requires mapping the ESG function and CSO day-to-day activities that include obtaining and reporting sustainability information, identifying ethical vulnerabilities and evaluating the probability of an event that could result in dissemination of false or incorrect information to the public or to the organisation interest groups.

ESG risk evaluation requires a working understanding of the concept of ESG materiality and considering materiality assessments when determining the organisation's vulnerability to fraudulent corporate behaviour.

Finally, compliance ESG impact risk assessments should incorporate the adverse economic, reputational and operational effects that can result from green- and social-washing and from the conflicts and litigation that can be initiated as a result by enforcement agencies, communities, non-governmental organisations and investors.

Corporate liability considerations

In countries that have incorporated corporate criminal liability into their legal systems, such as Mexico, compliance officers should consider the exposure that could arise from investigations associated to financial fraud.

An example of such exposure can be found in the Mexican Securities Market Law, that provides severe penalties for companies that disclose false information on financial, administrative, economic, or legal condition of an issuer, through any prospectuses, supplements, brochures, reports, disclosure of relevant events

18 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1937. Last accessed on 2 March 2023.

and other informative documents and, in general, of any mass media. A provision that can be used in green- and social-washing enforcement by the Department of Justice.

Criminal liability can also arise from the concealment or failure to disclose any relevant information or events that, in terms of this legal statute, must be disclosed to the public or to other shareholders or securities holders.

Use of digital tools for ESG synergy and oversight

The challenges caused by the synergy between ESG matters and compliance controls can be efficiently addressed in the near future through the use of digital tools. Online platforms make possible to create task forces to address and manage risks and incidents in companies' operations, which are relevant to their ethical environment and ESG commitments. In addition, the use of these tools will make easier for the compliance officer and the CSO to link risk analysis and ESG materiality assessments.

Governance commitment in the ESG strategy should include associating the operational and day-to-day functions of the company. In the case of medium, large and transnational organisations that operate in Latin America, governance and controls in anti-corruption, environmental, human rights protection and tax compliance, among others, may facilitate the collaborative environment applicable to multiple assets and business units deployed in different geographical areas. The above-mentioned could be limited on its effectiveness and efficiency in the cases where ESG strategies continue on being limited to analogous tools.

The future of ESG compliance

Certainly, environmental and human rights litigation will continue growing in the following years around the world. In the case of Latin America, with the progress and implementation of international human rights commitments such as the Escazú Agreement, it is foreseeable that such actions will raise awareness as well as concerns towards the corporate commitment to protect human rights and the environment.

In addition to the above, the regional incorporation of the recommendations established in the COP27 Report regarding the adoption of governance best practices and processes for accountability relevant to ESG, will continue to raise the necessity for organisational controls and ethics compliance in the near future.

In this context, ESG compliance will serve as a solid foundation for environmental, social and governance oversight, transparency and accountability.

CHAPTER 21

Rapidly Expanding Fintech Industry Brings Unique Compliance Challenges To Mexico

Ana Sofía Ríos, Valentín Ibarra and Alejandra Pacheco[1]

Corporate compliance overview

Mexico's financial sector has undergone significant transformations in recent years, with the rise of fintech companies disrupting traditional financial services through technological innovation. While this has brought about new opportunities, it has also posed challenges for regulatory compliance, particularly given the constantly evolving regulatory landscape. In this chapter, we will examine the importance of compliance for fintech companies in Mexico, challenges they face, and strategies they can employ to ensure compliance.

As we have seen over the past few years, fintech companies have grown in Latin America thanks to several factors, including poor access to traditional banking and obtainment of credit. This growth has had an impact on the size of the economies in Latin America, which is led by Brazil, followed by Mexico, Colombia, Argentina and Chile. According to calculations made by the Interamerican Development Bank, at the end of 2021 the number of fintech companies in Latin America and the Caribbean was estimated to be more than 2,300, an increase of more than 85 per cent since 2017.

The primary goal of fostering a culture of compliance in Mexico is to mitigate legal risks for businesses, executives, shareholders, officers, representatives and employees. Furthermore, compliance is crucial for improving a company's

1 Ana Sofía Ríos and Valentín Ibarra are partners, and Alejandra Pacheco is a senior associate at Chevez, Ruiz, Zamarripa y Cía.

competitive edge and worth in comparison to both national and international competitors. The Organisation for Economic Co-operation and Development (OECD) has been integrating corporate governance practices into its policies, emphasising that 'good corporate governance contributes to financial market stability, investment, and economic growth'. To develop strong corporate governance, businesses must satisfy key criteria, such as employing honest management, defining roles and responsibilities within various company divisions, ensuring the efficient, transparent and continuous information flow internally, safeguarding the rights of shareholders, and managing relations among diverse stakeholders.

The fintech industry is rapidly expanding in Mexico and disrupting traditional financial services. Fintech firms operate at the intersection of finance and technology, making them subject to strict regulation and oversight by authorities. Ensuring compliance with relevant laws, regulations and best practices is essential to maintain the trust of customers, investors and regulators alike. This, in turn, fosters a stable and secure environment for the industry to thrive. However, fintech companies face unique compliance challenges compared to traditional financial institutions, as they operate in a constantly evolving technological landscape with new products and services being introduced regularly.

Fintech companies must prioritise establishing robust internal compliance frameworks, staying current on evolving regulations, and fostering a culture of transparency and accountability. Given that fintech companies are relatively new players in the financial landscape, they have garnered significant attention from supervisory authorities, which are keen to monitor their activities and mitigate potential risks.

Noncompliance with regulations can result in severe consequences, such as fines, reputational damage or even the suspension of operations. Fintech entities must prioritise creating effective compliance programmes that are specifically tailored to their business models and products. Conducting a thorough risk assessment to identify and then mitigate potential risks associated with their unique operations and regulatory environment is crucial. Fintech firms should develop targeted policies and procedures to address the intersection of finance and technology, ensuring compliance with stringent regulations and oversight by authorities.

This risk-based approach should be complemented by fostering a strong culture of compliance throughout the organisation, starting with a clear commitment from senior management and the board of directors. Regular training and education for employees, robust monitoring and reporting systems, and encouraging open communication and feedback are crucial components for maintaining compliance and facilitating continuous improvement within the fintech industry.

Fintech companies in Mexico need to navigate a complex regulatory landscape to ensure compliance. Thus reguatory landscape is led by the Financial Technology Institutions Law (the Fintech Law), followed by several regulations issued by the National Securities and Banking Commission, applicable to different types of fintech entities (electronic payment companies, crowdfunding companies or sandboxes), anti-money laundering compliance, programing interfaces, external auditing services providers, among others, as well as the regulations issued by Banco de México in connection with cryptocurrencies. However, fintech companies that prioritise compliance can build a reputation for trustworthiness and reliability, while also fostering a stable and secure environment for the industry to thrive.

Embracing technology

As the fintech sector continues to grow and evolve, it is vital for companies to embrace technology to enhance their corporate compliance efforts. The incorporation of cutting-edge technological solutions, such as artificial intelligence (AI),[2] machine learning, and blockchain, can greatly improve the efficiency and effectiveness of compliance programmes. These technologies can be employed in various aspects of compliance management, such as monitoring transactions, identifying risks, and ensuring adherence to regulations. By leveraging advanced technologies, fintech companies can proactively identify and mitigate potential risks, reduce manual errors and streamline compliance processes, ultimately fostering transparency and accountability in the organisation.

The integration of technology in compliance management also enables fintech companies to stay ahead of the constantly evolving regulatory landscape. For example, implementing automation and data analytics tools can help fintech entities to monitor effectively large volumes of data, identify patterns and trends, and detect unusual activities that may signal noncompliance. By embracing technology and harnessing its potential in the realm of corporate compliance, fintech companies can maintain a competitive edge and ensure that they remain in line with the highest standards of regulatory adherence, thus safeguarding their reputation and promoting the overall growth and stability of the industry.

2 See 'Why Fresh Perspectives on Tech Solutions are Key to Evolving Data-Driven Compliance Monitoring' by Gabriela Paredes, Dheeraj Thimmaiah, Jaime Muñoz and John Sardar.

Financial technology regulation in Mexico

Mexico's fintech sector has grown in the past decade given legislative advances that have made Mexico an appealing location for start-up creation and development. Investors have been able to expand their businesses and enter new regional markets. On 9 March 2018, Mexico's Congress enacted the Fintech Law to regulate financial services using innovative technology. This law provides a framework for regulatory sandboxes, APIs, crowdfunding and electronic payment fund institutions (collectively known as 'ITF' in Spanish), making Mexico a leader in the Latin American region for governing the fintech industry.

With the enactment of the Fintech Law, ITFs must adhere to strict regulatory compliance measures. Specifically, they must establish necessary supervisory and internal control structures and disclose procedures and documents to customers and authorities, including in the ITF's agreements and webpages. Additionally, upon receiving authorisation, ITFs face challenges in implementing and maintaining good corporate practices, such as internal control, anti-money laundering (AML) compliance and external auditing. As a result, it is crucial for fintech companies in Mexico to prioritise the establishment of compliance programmes to navigate the complex regulatory landscape and ensure long-term success in the industry.

On 8 March 2019, the Mexican Central Bank issued Circular 4/2019, which significantly limited the use of cryptocurrencies by ITFs and banking institutions. Under this regulation, such entities can use cryptocurrencies only for internal operations and are prohibited from conducting consumer transactions involving these assets. In Mexico, only cryptocurrency operations conducted by crowdfunding firms, electronic money institutions and banking institutions are regulated under the Fintech Law, its secondary regulations and Circular 4/2019. Transactions between other individuals and entities are not covered by these regulations and instead fall under regular commercial and civil legal provisions.

Compliance provisions in the Fintech Law

The Fintech Law in Mexico includes several articles that address the compliance requirements of ITFs, ensuring that they operate within the bounds of the established regulations. One of the key articles in this regard is Article 39, which outlines the requirements necessary for ITFs to obtain authorisation from the National Banking and Securities Commission (CNBV) to operate. These requirements include:

- Developing and implementing risk disclosure policies, as well as defining responsibilities for the conduct of operations. ITFs are also required to disclose warnings related to the use of interfaces, websites or electronic communication means on their respective platforms.
- Establishing measures and policies for operational risk control and information security. This includes implementing confidentiality policies and ensuring that they are supported by secure, reliable and accurate technological infrastructure.
- Creating policies to address and resolve potential conflicts of interest that may arise during the performance of the ITFs' activities.
- Implementing fraud prevention policies, as well as measures to prevent operations involving resources of illicit origin and the financing of terrorism.

These regulations highlight the importance of due diligence in the fintech sector. Failure to comply with any of these provisions can result in sanctions, including the cancellation of an ITF's authorisation to operate. This underscores the need for ITFs to have a comprehensive compliance programme in place to avoid potential penalties and maintain a trustworthy reputation.

Article 48 of the Fintech Law further emphasises the importance of compliance by requiring regulated entities to maintain the stability and proper functioning of their internal control mechanisms and risk management systems. The CNBV and the Mexican Central Bank have been granted the authority to issue specific regulations related to these matters.

To ensure compliance with the Fintech Law and its provisions, ITFs should prioritise the establishment of comprehensive compliance programmes that cover every aspect of their operations. This includes regular reviews and updates of internal policies and procedures to remain current with any changes to the regulatory landscape. Moreover, ITFs should invest in employee training and education to promote a culture of compliance, ensuring that all team members understand the importance of adhering to these regulations and the consequences of noncompliance.

The Fintech Law also contains key provisions relating to the following.

Financial statements and external auditors.

Articles 49 to 52 focus on the financial statements of ITFs and compliance requirements, which include:

- an annual financial statement audit by an external auditor, appointed by the board of directors (external auditor);

- regulations set by the CNBV defining the characteristics and qualifications of external auditors and the contents of their reports;
- the CNBV's authority to supervise and examine external auditors, including information requests, supervision visits, appearance requests for auditors, and issuance of audit rules and procedures;
- external auditors must retain information and documents related to the evaluation and issuance of their opinions on financial statements for a minimum of five years. Technological or automated means may be utilised for storage purposes;
- external auditors must share relevant information supporting their opinions, evaluations, and conclusions with the CNBV;
- if irregularities that threaten the ITF's operation and functioning are discovered during or as a result of an audit, external auditors must report their concerns to the audit committee or company commissioner and the CNBV, or the Mexican Central Bank, as appropriate; and
- external auditors may be held liable under certain circumstances specified in the Fintech Law and applicable regulations.

Anti-Money Laundering

ITFs must adhere to specific compliance requirements concerning anti-money laundering (AML) and combating the financing of terrorism (CFT), including:

- establishing measures and procedures to prevent and detect acts, omissions, or operations linked to terrorist financing or money laundering – ITFs should develop a risk assessment methodology based on the products, services, practices and technologies used in their operations;
- submitting reports to the Ministry of Finance regarding transactions or services with clients, between clients, and carried out by ITFs' board members, executives, employees, or attorneys that may be related to terrorist financing or money laundering;
- adequately understanding clients' backgrounds, specific conditions, economic and professional activities, and geographic locations where they conduct business;
- aafeguarding and ensuring the security of client identification information and documents;
- establishing a communications and control committee; and
- appointing a certified compliance officer.

Board of directors and a managing director

ITFs must appoint a managing director and maintain a board of directors comprising no more than nine members, with at least 20 per cent deemed independent. Article 60 of the Fintech Law outlines the specific requirements for board members, while Article 61 defines independent members.

Audit Committee

Depending on their activities, ITFs may need an audit committee to support the board of directors.

These provisions emphasise the importance of ITFs establishing robust compliance programmes that address a wide range of regulatory requirements. By focusing on comprehensive compliance management, ITFs can mitigate risks associated with financial statement audits, AML and CFT measures, governance structures, and audit committees.

Information security

On 28 January 2021, the CNBV and the Mexican Central Bank issued the Regulations applicable to Electronic Payment Institutions in connection with information security, as established in Articles 48, Paragraphs 54 and 56 of the Fintech Law (Information Security Regulations), which have the purpose of setting principles of financial inclusion and innovation, promotion of competition, protection of consumers, financial stability and technological neutrality. The Information Security Regulations provide a unified, systematic, coherent and clear regulatory framework that grants legal certainty to the participants of the financial technology market, promotes the growth of electronic payment institutions and safeguards the interests of their customers and the financial system as a whole.

Specifically, the Information Security Regulations contain provisions on security of the information, including confidentiality policies, and account registries, use of electronic, optic or any other technological means, automated systems of data processing and telecommunications.

Data Privacy Protection.

By the very nature of its business, the fintech sector collects and operates with personal data. Fintech companies therefore must ensure compliance with data protection laws, specifically the Federal Law on Protection of Personal Data Held by Private Parties (Mexican Data Privacy Law).

The Mexican Data Privacy Law is the main data protection law in Mexico, regulating the collection, processing, storage and transfer of personal data by private parties. It aims to protect the fundamental right to privacy of individuals and provides guidelines for the processing of personal data by private parties, including fintech companies. Failure to comply with the Mexican Data Privacy Law can result in significant fines and reputational damage for fintech companies.

Fintech companies operating in Mexico must adhere to the requirements set out in the Mexican Data Privacy Law, including obtaining the explicit consent of individuals for the collection and processing of their personal data, limiting the use of personal data to the specific purposes for which it was collected, implementing appropriate technical and organisational measures to protect personal data, and ensuring the accuracy and completeness of personal data. It is crucial for fintech companies to be transparent about their data collection practices and provide individuals with clear and concise information about the purposes for which their personal data will be used.

Additionally, fintech companies must ensure that they have the necessary technical and organisational measures in place to protect personal data. This includes implementing appropriate security measures to prevent unauthorised access, disclosure, alteration, or destruction of personal data. Fintech companies must also ensure that their employees are adequately trained on data protection and security measures and have access to policies and procedures that govern the handling of personal data.

The Mexican Data Privacy Law also requires fintech companies to establish internal procedures for handling individuals' requests to access, modify or delete their personal data. These procedures must be simple, accessible, and timely. Fintech companies must also provide individuals with access to their personal data upon request, as well as information about the origin, use and third-party recipients of their data.

Furthermore, the Mexican Data Privacy Law requires fintech companies to have agreements in place with any third parties that may have access to personal data. These agreements must outline the specific purposes for which the third party is permitted to use the personal data and include appropriate technical and organisational measures to protect the data.

It is essential for fintech companies to keep current with changes in the regulatory landscape to ensure ongoing compliance with data protection laws. In recent years, Mexico has seen significant developments in data protection laws, including the enactment of the General Data Protection Regulation (GDPR) in

the European Union. As many fintech companies operate globally, compliance with the GDPR is essential, as it imposes strict requirements on the processing of personal data of individuals in the EU.

Benefits of having good corporate compliance practices

Having a robust corporate compliance programme can offer several advantages to fintech entities and other companies, such as to:

- pursue a long-term vision to achieve an unbiased benefit for all participants within and outside the company, including employees, managers, administrators, investors and the investing public;
- establish a firm framework to perform accurate, clear and useful regular evaluations, including an analysis of potential risk factors within and beyond the regular course of business, alternatives to mitigate the impact of different events on the company and its financial situation, as well as efficient management of capital, cash and liquidity;
- cultivate a culture of review and control of the company's documentation and information, enabling regular and transparent communication between the company and its stakeholders;
- ensure accountability, equity and transparency at every level and group within the company;
- enhance operational growth with coordinated and transparent systems that attract investment from the investing public;
- create a culture of collaboration with established protocols to prevent conflicts between shareholders and related parties;
- enhance the company's reputation with the investing public and international markets, positioning it in competitive places nationally and internationally, thereby improving access to financing and capital sources; and
- in the event of a possible sale, the price rises and there is a higher bargaining power due to the entity's internal regulations.

Challenges going forward

Mexico's fintech sector has experienced significant growth and transformation in recent years, largely due to regulatory advancements that have made the country an attractive destination for startups and investors. The enactment of the Fintech Law and other regulatory measures has created a complex landscape that fintech companies must navigate to ensure compliance and long-term success.

Challenges for fintech companies in Mexico include establishing robust internal compliance frameworks, staying up to date on evolving regulations, and fostering a culture of transparency and accountability. Fintech entities must

prioritise the implementation of compliance programmes that are tailored to their specific business models and products, while also addressing the unique intersection of finance and technology.

Adherence to strict regulatory compliance measures, such as data protection and anti-money laundering, is crucial for mitigating legal risks, improving a company's competitive edge, and maintaining trust among customers, investors and regulators. A successful compliance programme can also enhance the value of a fintech entity, making it an attractive acquisition target for larger national and multinational groups in the industry.

Going forward, fintech companies in Mexico must continue to adapt to the ever-evolving regulatory landscape and technological advancements while maintaining a strong commitment to compliance, transparency and accountability. By doing so, they can foster a stable and secure environment for the industry to thrive, benefiting all stakeholders and contributing to the country's overall economic growth.

Additionally, as the global financial landscape continues to evolve, international cooperation and coordination among regulators will become increasingly important. Fintech companies in Mexico must stay informed about international regulatory developments and be prepared to adapt their compliance strategies accordingly. By maintaining a proactive approach to regulatory compliance and actively engaging with regulatory authorities both domestically and internationally, Mexican fintech companies can ensure their continued success in a rapidly changing industry while bolstering their reputation as trusted and reliable financial service providers.

APPENDIX 1

About the Authors

Elissa N Baur

McGuireWoods LLP

Elissa focuses her practice on white-collar and antitrust criminal defence matters, including internal investigations, litigation and regulatory enforcement actions. She has defended clients in numerous government investigations before the Department of Justice, United States Office of Special Counsel, Securities & Exchange Commission, Department of Treasury's Financial Crimes Enforcement Network (FinCEN), Office of the Comptroller of Currency and Federal Reserve Board, among others.

Elissa is a member of the McGuireWoods' government investigations and white collar litigation department, which was recognised by Law360 as a Practice Group of the Year. She has particular experience conducting internal investigations and advising clients on compliance with the US Foreign Corrupt Practices Act (FCPA) and other anti-corruption laws. Her practice also includes representing companies and financial institutions in connection with regulatory, civil, and criminal enforcement actions arising from US anti-money laundering (AML) laws and regulations. She speaks Spanish and Portuguese and uses her language skills regularly in her practice.

Julie Bédard

Skadden, Arps, Slate, Meagher & Flom LLP

Julie Bédard is head of Skadden's international litigation and arbitration group for the Americas. Fluent in French, Spanish and Portuguese, she practises in four languages in complex international litigation and arbitration matters. Ms Bédard regularly counsels management and supervisory boards in corporate governance, internal investigations and US Foreign Corrupt Practices Act matters. She frequently assists with internal investigations and related corporate governance advice, including remedial measures and the implementation of corporate

compliance programmes. She also is experienced in conflict of laws and has represented clients in connection with litigation and arbitration proceedings throughout the world. Ms Bédard has been listed repeatedly in *Chambers USA*, *Chambers Global*, Law Business Research's *Who's Who Legal: Arbitration*, *Chambers Latin America* and *The Best Lawyers in America*. Additionally, Ms Bédard has been named repeatedly by *Latinvex* magazine as one of Latin America's 'Top 100 Lawyers for Arbitration and Litigation', and as one of its 'Top Female Lawyers' in Latin America. She was named *Latin Lawyer* 2023 International Lawyer of the Year.

Paula Pérez Benítez
Mijares Angoitia Cortés y Fuentes SC

Paula specialises in environmental law with more than 17 years of experience in that practice. She has a comprehensive vision of environmental, administrative and regulatory law as she has worked in both the public and private sectors.

Paula has specialised in providing advice on compliance with legal obligations regarding environmental impact and risk, water, waste management, soil contamination and its remediation, federal maritime land zone, forestry and soil changes, hydrocarbons, among others. Within regulatory matters, she has a particular focus on health law, as well as emerging regulations on cannabis and its derivatives.

She has participated in multiple environmental audits for clients from different industries, such as renewable energies, the hydrocarbons, food and beverage, forestry, paper, chemical, real estate, tourism, product manufacturing, tobacco and pharmaceutical sectors, laboratories, among others. Likewise, she has experience in environmental litigation and administrative procedures against acts of environmental and regulatory authorities in the three levels of government. Paula has worked particularly with the system of environmental responsibility, remediation and compensation of environmental damage, based on the regulations established in the Federal Law of Environmental Responsibility.

As part of the ESG specialisation, Paula has focused on designing tools for the development and implementation of regulatory management and environmental compliance systems, as key tools in clients' ESG strategies.

María González Calvet
Ropes & Gray

María González Calvet serves as co-chair of the firm's award-winning global anti-corruption and international risk practice and Latin America initiative, and is a former US federal prosecutor and former in-house executive counsel of a Fortune 500 company. With a practice that spans two decades, María is

recognised for her significant experience in anti-corruption and other investigative matters in Asia, Africa, Latin America and Europe, and in every significant business sector. María is widely recognised as a thought leader in anti-corruption, particularly on anti-corruption risks and enforcement trends in Latin America. As one client noted to *The Legal 500*, 'María is super experienced when it comes to performing internal investigations, speaks perfect Portuguese and Spanish and understands the Latin culture.' María is quoted frequently in the press for her expert commentary on anti-corruption issues and publishes a number of articles for well-known publications, including Law360, *The Anti-Corruption Report* and *Latinvex*. Notably, María is a contributor to GIR's 2021 Latin America chapter of *The Practitioner's Guide to Global Investigations*. María also developed Ropes & Gray's Anti-Corruption Legislation in Latin America Reference Guide, which highlights the firm's depth of knowledge in the Latin America region.

Gabriel Calvillo
Mijares Angoitia Cortés y Fuentes SC

Gabriel focuses his practice on compliance, corporate criminal liability, white-collar crime and environmental litigation. His experience comes from the practice of criminal law, both in the private and public sectors.

Gabriel has been criminal counsel in corporate criminal matters for more than 10 years, as well as head of the Environmental Crimes Unit of the Attorney General's Office in matters particularly close to corporate activity, such as crimes against the environment, corporate homicide and industrial related offences. He specialises in complex corporate criminal liability cases and criminal compliance.

In his environmental practice, Gabriel regularly represents corporations in complex litigations cases, as well as buyers and sellers in environmental and compliance due diligence. He worked as general counsel for the Federal Environmental Enforcement Agency (PROFEPA), litigation director general at the Environmental and Natural Resources Ministry, as well as the head of the Environmental Crimes Division of the Federal Department of Justice. In private practice he represented corporations for more than 10 years in complex environmental damage and toxic torts cases. Gabriel has a long history in the regulatory, law enforcement and compliance field in environmental and human rights matters, which allows him to incorporate real procedural criteria and experiences into the prevention, risk analysis and compliance models of Mijares Angoitia Cortés y Fuentes SC.

Gabriel oversaw the design and implementation of the Federal Law on Environmental Responsibility, which addresses central issues of compliance, climate responsibility and ESG litigation, as well as a litigator and prosecutor specialising in business crimes that expose people to criminal liability due to failures in control, surveillance and good governance.

Isabel Costa Carvalho
Hogan Lovells

Isabel Costa Carvalho is a managing partner at Hogan Lovells. She advises and speaks extensively on anti-bribery laws, corporate governance and data privacy issues in Brazil. She has been at the forefront of the implementation of Brazil's new General Data Privacy Law, supporting some of the country's most prominent entities with data risk management concerns. She routinely assists clients in setting up compliance programmes to fit their unique needs, industries, and risks, and guides them in solving problems when they arise, including leading crossborder investigations and dealing with relevant US and Brazilian authorities.

Isabel began her career in London, where she spent six years with a major international firm then moved to Brazil to assist with the opening of the firm's new office. She later joined Hogan Lovells to lead its São Paulo office with a focus on corporate, compliance, and investigations in Brazil. Her diverse practice gives her the chance to assist clients from many industry sectors, including financial institutions, energy, infrastructure and logistics, technology, retail, and real estate. Fluent in English, Portuguese and Spanish, she is able to help clients of different cultures all around the world.

Brendan P Cullen
Sullivan & Cromwell LLP

Brendan Cullen is a partner in Sullivan & Cromwell LLP's litigation group. He is based in the firm's Palo Alto office. Mr Cullen has litigated a broad range of matters, including complex securities, commercial, intellectual property and competition litigation, frequently with a substantial technological element. He has advised and represented clients in arbitrations, in cases in state and federal trial courts and on appeals before state and federal appellate courts, including the US Supreme Court. He also has conducted numerous confidential internal investigations, including investigations relating to issues of corporate governance, securities matters and Foreign Corrupt Practices Act compliance, and involving numerous countries throughout Asia, Europe, the Middle East and Latin America.

Maximiliano D'Auro
Beccar Varela

Maximiliano D'Auro is a partner at Beccar Varela. He joined the firm in 2000 and is a member of the executive committee and heads the anti-corruption and compliance department.

He has broad experience in banking and financial law, advising both foreign and local financial institutions not only on structuring complex financial transactions but also on specific regulatory matters. He provides legal advice to national and multinational companies on all aspects of anti-corruption laws, regulations and compliance. His expertise relates specifically to the prevention aspects of the anti-corruption legal framework and the implementation of codes of ethics and compliance programmes.

Maximiliano obtained his law degree from National University of Mar del Plata (1997) and his LLM from the London School of Economics (2000).

He is a member of the Buenos Aires Bar Association, secretary of the Comité de Abogados de Bancos de la República Argentina and a past president of the compliance committee of the Colegio de Abogados de la Ciudad de Buenos Aires. He is a member of the International Bar Association, Conference Quality Officer of its Anticorruption Committee, and the Argentine contributor for its Anti-Money Laundering Forum. He is also an honorary member of the International Association of Young Lawyers.

Diego Durán de la Vega
Hughes Hubbard & Reed LLP

Diego Durán de la Vega is a partner of Hughes Hubbard based in Washington, DC and co-chair of the Latin American disputes practice group. His practice focuses on international disputes, including white-collar defence matters, internal investigations, commercial litigation and international arbitration cases – including investor-state arbitration. He also has experience in compliance, where he assesses exposure, designs and implements programmes, and provides training.

Diego mainly advises and represents non-US clients in US litigation, and US clients that are facing litigation abroad. Among Diego's clients are government agencies, international corporations and high-profile individuals.

Diego has appeared before international arbitration tribunals, federal and state courts in the United States, and all levels of the Mexican judiciary, including the Mexican Supreme Court. He has also participated in cases before the Inter-American Commission on Human Rights and its Court of Justice.

In the area of international arbitration, Diego has represented clients in the following industries: renewable energy, oil and gas, maritime services, engineering and construction, health, casino, and food franchising. He conducted such representations before the following international arbitration institutions: ICC, AAA/ICDR, JAMS and ICSID. He also has experience with ad hoc cases. In addition, Diego has experience as an arbitrator: he currently serves as an arbitrator in two ICC commercial arbitrations, is included in the AAA's roster of Consumer Arbitrators and the Mexican Arbitration Center National Roster of Arbitrators.

In the areas of white-collar criminal defence, internal investigations and compliance, Diego has represented and advised clients in various investigations and proceedings related to DOJ, SEC, OFAC and FinCEN, as well as federal prosecutors' offices in different states of the United States. He has also represented clients in connection with extradition proceedings. In addition, he has participated in several internal investigations related to FCPA, money laundering, tax evasion and economic sanctions, among others.

Diego's experience as a litigator in Mexico and the US, his academic work in Europe, Mexico and the United States, and his cultural capabilities enable him to easily navigate complex cross-border legal issues. He has ample experience coordinating international legal teams and local counsel in different jurisdictions.

Because Diego's native language is Spanish, and he is fluent in English, he is able to handle cases in both languages. Furthermore, Diego is licensed to practise law in both Mexico and the US (New York and District of Columbia). He is the only attorney at the firm licensed to practice in both countries. This places Diego in a unique position to understand and navigate both civil and common law systems.

Diego is also experienced in Mexican criminal, constitutional and amparo law. Prior to Hughes Hubbard and Quinn Emanuel, he was a successful litigator at one of the top criminal law boutiques in Mexico, where he defended and helped prosecute dozens of cases.

Palmina M Fava
Vinson & Elkins LLP

Palmina M Fava is a partner with Vinson & Elkins LLP, based in New York. She has over 20 years of experience. She represents clients in internal and government investigations, litigation and corporate governance counselling, with a principal focus on matters involving the Foreign Corrupt Practices Act (FCPA), international anti-corruption, anti-money laundering and anti-bribery laws,

accounting irregularities, bid rigging and unfair trade practices, off-label pharmaceutical marketing, misappropriation of trade secrets, fraud, cyber breaches and data privacy.

Palmina regularly represents companies in matters before the United States Department of Justice, the Securities and Exchange Commission, other federal and state agencies, and international regulatory bodies. She leads teams in investigations in Latin America, Europe, Asia, Africa, Australia and the Middle East. Relying on her extensive language skills, she is capable of assisting clients in Spanish, Portuguese, Italian and English. She also designs and implements comprehensive, practical and user-friendly corporate compliance programmes tailored to a client's particular risks and growth strategies.

She provides employee and third-party training; conducts proactive reviews of a client's high-risk business areas; structures commercial arrangements to protect against compliance risks; and handles due diligence of agents, joint venture partners, and targets in mergers and acquisitions or other investment transactions. Palmina's litigation practice focuses on commercial, business tort, and intellectual property disputes. She has served as lead litigation and trial counsel in matters involving breaches of fiduciary duty, breaches of contract, fraud, negligence, misappropriation of trade secrets and insurance coverage. She has tried and defended cases in federal and state courts, and before arbitration panels, and represented clients in appellate arguments, mediations and negotiations, including before the US Supreme Court.

Ryan Fayhee
Hughes Hubbard & Reed

Ryan Fayhee leads the sanctions, export controls and anti-money laundering practice group at Hughes Hubbard and is a former senior prosecutor and national security official with the US Department of Justice (DOJ). Ryan's practice focuses on government and congressional investigations, crisis management, cross-border compliance, corporate governance and white-collar criminal defence.

Ryan draws upon a multi-disciplinary skillset to assist corporations, boards of directors, audit committees, and senior executives facing high-profile reputational risks and incident response, often involving US and foreign regulators and enforcement authorities, political stakeholders, and the media. He also advises clients on strategic opportunities, governance and compliance best practices, acquisition due diligence, and national security reviews before the Committee on Foreign Investment in the United States (CFIUS).

An experienced trial lawyer, Ryan has successfully tried several cases to verdict, with the unique ability to handle deeply regulatory matters and seamlessly transition to high profile enforcement actions involving the DOJ as well as regulators at the Office of Foreign Assets Control (OFAC), Financial Crimes Enforcement Network (FinCEN), Bureau of Industry and Security (BIS), and the Directorate of Defense Trade Controls (DDTC).

Ryan is on *Global Investigations Review*'s elite list of the most respected sanctions lawyers in Washington, DC. *The Legal 500* has recognised Ryan for 'excel[ing] at leading and conducting investigatory work as a result of the "wealth of experience and insights" he gained in his former position as a DOJ national security prosecutor.'

Ryan's clients come from varied industries, including financial services, private equity, technology, aerospace and defence, telecommunications, energy, mining, construction materials, logistics, pharmaceuticals and consumer goods.

Ryan maintains an active pro bono practice and, in particular, has extensive experience representing current and former hostages of foreign governments and transnational criminal organisations, as well as the unlawfully detained, with a focus on advocating for victim families, securing release, and ensuring long term reintegration.

Raimundo Gálvez
Carey

Raimundo Gálvez is an associate at Carey and a member of the antitrust and regulated markets group. His practice focuses on antitrust, litigation and mergers and acquisitions. He has been a teaching assistant in civil law and antitrust law at the University of Chile. Before becoming associate, he worked as a law clerk at the National Economic Prosecutor's Office (FNE). He graduated summa cum laude from the University of Chile.

Antonio Gesteira
FTI Consulting

Antonio Gesteira is a senior managing director, based in Brazil, at FTI Consulting. He is a seasoned e-discovery and forensic technology expert with more than 20 years of experience in supporting complex investigations and litigations.

Mr Gesteira has delivered more than 400 projects spanning emerging technology, data services, information security, data protection, and internal and external audit support across a variety of industries. He has led large investigations and risk management efforts in Brazil and internationally. As the technology

segment's leader for the Latin American market, Mr Gesteira works with clients to address a broad range of corporate risk and respond to high-stakes legal and regulatory matters.

Prior to joining FTI Consulting's technology segment, Mr Gesteira was managing director of the forensic practice at Big 4s in Brazil, where he served as a leader for computer forensic investigations, e-discovery vendor management, cyber response services and data services. In that role, he grew the practice through the creation of new capabilities and extending the team's reach to clients in previously unaddressed industry segments.

Baldemar Gonzalez
Ropes & Gray

Baldemar Gonzalez joined Ropes & Gray's litigation and enforcement group in 2019. As an associate, he focuses his practice on white-collar criminal defence, governmental and internal investigations, and related civil litigation. His experience includes representing companies in matters involving the False Claims Act and Foreign Corrupt Practices Act, government enforcement actions, internal investigations, and complex commercial litigation. Baldemar also maintains an active pro bono practice that includes representing asylum seekers. During law school, Baldemar served as a managing editor of the Columbia Law Review and was named a Harlan Fiske Stone Scholar. Baldemar has experience mediating disputes in New York City courts.

Erich O Grosz
Debevoise & Plimpton LLP

Erich Grosz is a litigation counsel at Debevoise & Plimpton LLP and focuses his practice on white-collar and regulatory defence, internal investigations and compliance-related advice. Mr Grosz has represented companies and individuals in investigations and enforcement proceedings involving allegations, among others, of violations of the US Foreign Corrupt Practices Act, securities and accounting fraud, and employee misconduct. He also regularly advises companies on compliance matters and on risk mitigation in connection with potential transactions. He received his JD from Stanford Law School and his BA from Princeton University.

Tyler Grove
Hughes Hubbard & Reed

Tyler Grove is a counsel in the Washington, DC office of Hughes Hubbard & Reed. As part of the international trade group, Tyler has experience in advising domestic and international clients on economic trade sanctions compliance and enforcement; advising companies in cross-border acquisitions on trade-related contractual provisions, due diligence, and filings with the Committee on Foreign Investment in the United States (CFIUS); investigating and drafting complex voluntary disclosures submitted to the Commerce, State, and Treasury Departments; conducting product classifications and de minimis analyses; and preparing Commodity Jurisdiction and Commodity Classification Automated Tracking System (CCATS) requests.

As part of the litigation group, Tyler has experience in complex litigation, fact investigation and discovery in various government facing matters, including those involving professional liability, securities, antitrust and trade issues.

Anna Hamati
Hughes Hubbard & Reed LLP

Anna Hamati is an associate in Hughes Hubbard's Washington, DC office. She is a member of the firm's sanctions, export controls and anti-money laundering practice group.

As part of the firm's sanctions, export controls and anti-money laundering practice group, Anna assists clients with matters related to export controls and economic trade sanctions.

Prior to joining Hughes Hubbard & Reed, Anna was a senior sanctions policy advisor at the US Department of Treasury in the Office of Foreign Assets Control. She was also an assistant vice president at Citibank in both the global sanctions compliance and the anti-money laundering units.

Valentin Ibarra
Chevez, Ruiz, Zamarripa y Cía

Valentin Ibarra joined Chevez Ruiz Zamarripa in 2004. His professional practice is mainly concentrated on advisory and litigation in the tax, administrative and fintech areas in a wide range of sectors and transactions, representing domestic and international clients. He litigates complex matters before federal and state administrative and tax courts and carries out constitutional actions at the level of the Supreme Court of Justice of Mexico.

He is highly experienced in alternative dispute resolution proceedings and has handled complex tax cases before the tax authorities and the Mexican Tax Ombudsman (PRODECON).

Valentin also leads the firm's fintech law practice and teaches fintech law at the Universidad Panamericana (UP) and Universidad Iberoamericana (UIA) in Mexico City. Additionally, he has lectured on tax and fintech law in the private and public sectors, including the Ministry of Finance.

He is the author of several articles on tax matters published in Mexican and overseas media specialised in taxation and fintech law.

Hayley Ichilcik
Morrison & Foerster LLP

Hayley leads the firm's global ethics and compliance regional practice in Europe, and her practice focuses on white-collar criminal litigation defence, financial crime investigations, and compliance reviews. She represents both corporates and individuals in criminal litigation and regularly conducts internal investigations. Hayley specialises in anti-bribery and corruption, anti-money laundering, anti-tax evasion, trade and financial sanctions, as well as the UK Modern Slavery Act and whistle-blowing regulations. She advises clients across a range of sectors, including technology, financial services, oil and gas, healthcare and mining.

Prior to joining Morrison & Foerster, Hayley was seconded to the UK Serious Fraud Office for 20 months, where she was part of the team that secured the SFO's first deferred prosecution agreement and was awarded Prosecution Team of the Year by the UK Attorney General.

Christopher James
Vinson & Elkins LLP

Christopher James is a partner at Vinson & Elkins LLP's San Francisco office. Chris's practice focuses on government and internal investigations, white-collar criminal defence, commercial litigation, and corporate risk and compliance. He works with a variety of individuals and private and public companies in technology, finance and banking, and energy sectors. Chris regularly represents clients in matters before the United States Department of Justice, the Securities and Exchange Commission, and other federal and state agencies. He also conducts compliance risk assessments and provides counselling on internal controls, employee and third-party training, and transactional diligence. Chris has been designated a Certified Information Privacy Professional (CIPP/US) by the International Association of Privacy Professionals (IAPP).

Andrew B Jánszky
Andrew B Jánszky

Andrew Jánszky has more than 40 years' experience in international capital markets, mergers and acquisitions, corporate governance and compliance as a partner at Shearman & Sterling and Milbank. At Shearman, he was head of its global capital markets group and its Latin America practice. He opened and headed Shearman's São Paulo office. He then joined Milbank in 2010 to open and run its São Paulo office and lead its Latin America practice. Since retiring from the practice of law, Andrew has been a member of the board of two NYSE-listed companies, was part of several investigative committees appointed by boards of Brazilian companies to look into corruption allegations, and has served as a consultant to various boards on compliance issues.

Daniel S Kahn
Davis Polk & Wardwell LLP

Daniel S Kahn represents companies and individuals in criminal and regulatory enforcement matters and in conducting internal investigations involving violations of the anti-bribery laws, money laundering and securities, commodities, and financial fraud, as well as on compliance matters. A former prosecutor, he served for 11 years in senior roles at the Department of Justice.

The Wall Street Journal described Dan as the DOJ's 'most recognizable expert on the Foreign Corrupt Practices Act'. At the DOJ, Dan was acting Deputy Assistant Attorney General of the Criminal Division and, earlier, head of the Fraud Section and FCPA Unit. He supervised matters involving FCPA violations, money laundering, and fraud related to digital currency, fintechs, commodities, securities, healthcare and procurement.

At the DOJ, Dan played a central role in developing enforcement policies on the FCPA, corporate investigations and resolutions, compliance and monitors. He worked with enforcement authorities in the US, Europe, Asia and Latin America. Dan teaches Corporate Criminal Investigations at Harvard Law School and Global Anti-Corruption at Georgetown Law Center, and sits on the board of the NYU Program on Corporate Compliance and Enforcement.

Jordan Rae Kelly
FTI Consulting

Jordan Rae Kelly is a senior managing director and the head of cybersecurity for the Americas at FTI Consulting. Ms Kelly has more than 15 years of experience coordinating incident response and managing cyber policy planning.

At FTI Consulting, Ms Kelly advises clients on a broad range of cybersecurity and data privacy matters involving breaches, insider threats, intellectual property, crisis communications, vendor management, compliance, regulation, risk management and forensic investigations.

Prior to joining FTI Consulting, Ms Kelly served as the director for Cyber Incident Response on the National Security Council at the White House. During her tenure there, she was responsible for both national incident response coordination, as well as management of the US government's process for managing zero-day exploits. She was also a chief author of the National Cyber Strategy, the first of its kind in the United States in 15 years.

Before joining the National Security Council in 2017, Ms Kelly served as Chief of Staff and Chief of Strategic Initiatives in the FBI Cyber Division, where she managed daily operations and strategic and policy planning for the FBI's national cyber programme.

James M Koukios
Morrison & Foerster LLP

James Koukios is a partner in Morrison & Foerster's Washington, DC office, and serves as global co-head of the FCPA and anti-corruption practice. Mr Koukios represents companies and individuals in high-stakes government enforcement actions and complex internal investigations. An experienced trial attorney and former federal prosecutor, Mr Koukios has tried over 20 federal jury cases, including serving as the lead prosecutor in two landmark FCPA-related trials: *United States v. Esquenazi* and *United States v. Duperval*. James has been ranked by Chambers & Partners in their US guide for Nationwide FCPA.

Prior to joining Morrison & Foerster, James served as the senior deputy chief of the fraud section in the criminal division of the DOJ. In that role, he supervised investigations, prosecutions and resolutions in the fraud section's FCPA, healthcare fraud, and securities and financial fraud units. He was also a key contributor in drafting the DOJ and SEC joint publication, 'A Resource Guide to the US Foreign Corrupt Practices Act', which followed a series of consultations with business and compliance leaders. Along with his role as senior deputy chief, James has also held numerous government positions, including assistant chief in the fraud section's FCPA unit, special counsel to former FBI director Robert S Mueller III, and as an Assistant US Attorney in the Southern District of Florida.

Andrew M Levine
Debevoise & Plimpton LLP

Andrew Levine is a litigation partner at Debevoise & Plimpton, based in New York, and a member of the firm's white-collar and regulatory defence group. He serves as co-head of the firm's Latin America practice and as a co-leader of its Environmental, Social and Governance (ESG) group. Mr Levine is well recognised in the region and elsewhere for defending companies and individuals in criminal, civil and regulatory enforcement matters and for conducting internal investigations. He serves as a trusted adviser to numerous leading global companies and has represented many clients on corruption-related matters in Latin America, including the *Lava Jato*, *Zelotes*, *Carne Fraca* and *FIFA* scandals. Mr Levine has led important representations in Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Guatemala, Mexico, Peru, Uruguay and Venezuela, among other countries. In addition to an active defence and investigations practice, he frequently advises clients on a broad array of compliance and ESG matters, including conducting risk assessments, enhancing compliance programmes and mitigating risks presented by potential corporate transactions. His practice also encompasses complex litigation and other commercial disputes, often with an enforcement or investigative connection.

Mr Levine is ranked as one of the two top lawyers for corporate crime and investigations in Latin America by *Chambers Latin America* and as a leading lawyer for FCPA by *Chambers USA*. Clients in these directories have described him as 'a massive name in the region for this kind of work', 'a leading expert in providing sophisticated compliance advice to large multinationals' and 'a reassuring presence in tumultuous times' with 'a very business-oriented way of finding and presenting solutions'. Mr Levine has also been praised as 'an amazing lawyer who is extremely practical, to the point and very responsive' and for possessing a 'global view when representing clients'. *The Legal 500 Latin America* quotes one client who asserts: 'Andrew Levine is a superstar. He has a wealth of experience and is passionate about his area of practice'.

In 2020, Latin Lawyer named Mr Levine as 'International Lawyer of the Year', based on 'his profile in the market and the vast amount of work he has done to shape the development of anti-corruption and investigations work in Latin America'. Mr Levine actively advances the anti-corruption dialogue in Latin America, including as a thought leader in organising conferences and by publishing widely on related topics. Since 2013, he has co-chaired annually 'Latin Lawyer and GIR Live Anti-Corruption & Investigations Brazil' and, since 2019, the edition of this conference in Mexico.

Before joining Debevoise, Mr Levine served as deputy counsel to the Independent Inquiry Committee into the United Nations Oil-for-Food Programme. He received his JD from Yale Law School and his BA *summa cum laude* and Phi Beta Kappa from Yale College.

Anthony J Lewis
Sullivan & Cromwell LLP

Anthony Lewis is a partner in Sullivan & Cromwell LLP's litigation group. He is based in the firm's Los Angeles office, and his practice involves complex government investigations. Mr Lewis has represented clients in matters involving the US Department of Justice, the US Securities and Exchange Commission and the Commodities Futures Trading Commission, as well as in internal investigations. Mr Lewis has been a federal prosecutor for more than 10 years in the United States Attorney's Office for the Central District of California, where he was Deputy Chief of the Terrorism and Export Crimes Section. He prosecuted sophisticated cybercrimes, financial frauds and criminal tax cases, as well as various domestic and international counter-intelligence and counter-terrorism matters. He has conducted and supervised investigations and prosecutions involving OFAC-administered sanctions, the Export Administration Regulations and the International Traffic in Arms Regulations. Mr Lewis's experience has also involved significant dealings with technology and technology companies. He has tried a variety of cases and briefed and argued appeals before the Ninth Circuit.

Nelson Luis
Deloitte

Nelson Luis serves as Deloitte's forensic services practice leader for the Spanish Latin America region. He also serves on Deloitte's global forensics executive committee as the Americas Forensics Leader. He has extensive global experience advising clients on complex domestic and cross-border forensic and litigation support matters. He assists clients on issues related to disputes, forensic accounting, and fraud investigations, including matters involving allegations of bribery and corruption, financial reporting irregularities and occupational fraud.

Leveraging his experience abroad and fluency in English and Spanish, Nelson has expertise in cross-cultural business norms to assist in effectively conducting internal investigations, cross-border disputes and mitigate compliance risks. He has managed over 150 cross-border investigations in Latin America, Asia-Pacific and Africa.

Nelson supports private equity and multinational clients perform due diligence efforts around proposed transactions, business interruption or fidelity insurance claims, and compliance assessments to recover underreported revenues. He has led in-country Foreign Corrupt Practices Act (FCPA) investigations and compliance assessments in over 40 countries; and assists clients in developing and assessing anti-fraud and anti-corruption compliance programmes. Nelson has served clients as an independent arbitrator and expert. His dispute-related responsibilities include managing the preparation of financial models, economic projections and sensitivity analyses used in the determination of financial damages; supporting on purchase price disputes and working capital adjustments; and preparation of evidentiary materials for trial.

Adrián Magallanes Pérez

Von Wobeser y Sierra, SC

Adrián Magallanes Pérez is admitted to practise in Mexico and New York. He has 18 years of experience, working in Washington, DC and Beijing. He frequently appears before Mexican courts, where his experience includes several class action cases, transnational litigation, constitutional law trials (amparos), FCPA investigations and due diligence cases. His practice also extends to commercial and administrative litigation. Adrián Magallanes has acted as counsel in ad hoc and institutional arbitrations (ICC, LCIA, ICSID, AAA, ICDR, UNCITRAL, CAM, CANACO) in the commercial, infrastructure, energy, oil and gas, and investor-state sectors. He has also acted as arbitrator in commercial and construction cases, and has acted as expert on Mexican law before different courts and agencies.

Reynaldo Manzanarez Radilla

Incode Technologies Inc.

Reynaldo Manzanarez is a senior corporate attorney and compliance professional with substantial experience in providing advice to international operations, including Fortune 500 companies; helping organisations in building and optimising processes and mitigating risks to comply with internal policies and applicable laws and taking actions to protect corporate interests and maintain reputable profitable businesses.

Reynaldo is a strategic leader and function-builder with more than 20 years of experience, who can operationalise and manage the legal and compliance function on an international scale and assist in overseeing and supporting day-to-day operations, including corporate governance, M&A, ethics and compliance, strategic negotiations and general corporate matters and commercial law, among many others. He currently leads the legal affairs and compliance department at Incode

Technologies, managing a group of professionals who support the business on a global scale. Reynaldo and his team are responsible for driving and coordinating all legal aspects, managing and mitigating risks by designing and implementing company policies and procedures, as well as ensuring compliance with the laws and regulations that apply to the business and its products and service offerings and promoting legal, compliance and risk management best practices throughout the organisation.

He currently heads the legal affairs and compliance department at Incode Technologies (a worldwide service provider of identity solutions that facilitate human authentication and ID verification); previously, he worked for many years at different companies serving the IT and wireless industries in the Americas, such as Brightstar Corp (now Likewize), Cisco Systems, Microsoft and Oracle. He also worked at GE Capital and, before serving as in-house counsel, he acquired corporate experience working at major well-recognised firms.

Reynaldo holds a JD, has studied telecommunications law and intellectual property and he has participated as speaker in seminars and conferences across the LatAm region providing knowledge on various matters such as anti-corruption and data privacy regulations.

Tatiana R Martins
Davis Polk & Wardwell LLP

Tatiana R Martins represents companies and individuals in white-collar defence and regulatory enforcement matters, and in conducting internal investigations involving violations of the anti-bribery laws, money laundering and financial frauds. She also advises on compliance matters.

An experienced trial lawyer, Tatiana has tried multiple cases to jury verdict. As an Assistant US Attorney for the SDNY, she tried high-profile cases including that of former New York Assembly Speaker Sheldon Silver. As chief of the SDNY Public Corruption Unit, she oversaw major investigations and prosecutions, including cases against Michael D Cohen, NCAA basketball coaches and high-level UN officials.

Tatiana is recognised for her white-collar work by Chambers USA, where sources say she 'has excellent judgment' and 'always produces excellent legal analysis without losing sight of the practical and strategic implications'. In 2021 and 2022, Tatiana was recognised in *Latinvex*'s 2022 'Latin America: Top 100 Female Lawyers'.

Tatiana was born in Recife, Brazil and is a native speaker of Portuguese. She is also fluent in Spanish.

Tatiana is on the boards of the Office of the Appellate Defender and the Tinker Foundation.

Maria Cruz Melendez
Skadden, Arps, Slate, Meagher & Flom LLP

Maria Cruz Melendez is a partner in Skadden's white-collar defence and investigations team based in New York. She formerly served as a federal prosecutor for the US Attorney's Office for the Eastern District of New York. She was the deputy chief of the Public Integrity Section, the EDNY's corruption section, and most recently served as deputy chief of the civil rights section. Ms Cruz Melendez counsels on domestic and cross-border investigations and civil and administrative proceedings conducted by the Department of Justice, the Securities and Exchange Commission and the Office of Foreign Asset Control in connection with US securities laws, the Foreign Corrupt Practices Act and other domestic and international regulatory enforcement matters. She also advises corporations on prevention, oversight and compliance programmes designed to address sexual harassment in the workplace; issues concerning civil rights; diversity, equity and inclusion; and related matters. In recognition of her work, Ms Cruz Melendez was included on Lawdragon's inaugural list of 500 Leading Litigators in America in 2022.

Adriana Morales
Mijares Angoitia Cortés y Fuentes SC

Adriana has collaborated with Mijares Angoitia Cortés y Fuentes SC since 1998.

Currently, Adriana is part of the firm's ESG practice and has advised various clients for several years on corporate governance structures. The clients' board of directors plays a key role, particularly in adopting policies to address and mitigate ESG risks, which encompass a wide range of issues. These issues can include employee relations, human rights, climate change and supply chain management within a business society.

As part of her ESG specialisation, Adriana has focused on designing tools for the development and implementation of regulatory and compliance management systems. These tools are essential in our clients' ESG strategies, helping to mitigate corporate liability for control failures, oversight and good governance.

In 2008, Adriana established and led the corporate services area of the firm until June 2022. The corporate services area focuses on providing daily corporate services related to the corporate maintenance of commercial and civil entities, both Mexican and foreign. The client base includes specialised companies in entertainment, telecommunications, energy and the financial system, among others.

Adriana also specialises in anti-money laundering (AML) and supervises and advises various clients in the financial and non-financial sectors to ensure compliance with the obligations imposed by Mexican legislation in this area. Adriana obtained the certification in AML/CFT issued by the National Banking and Securities Commission in December 2019.

Jaime Muñoz
Anheuser-Busch InBev

Jaime Muñoz is the global director of ethics and compliance for AB InBev responsible for Latin America. He studied economic-social studies at the Sorbonne University (France), as well as law at the Catholic University in Bolivia, and has a master's in strategic business management from the University of Leon in Spain.

Before working at AB InBev, he worked for LBC - Zurich Financial Services and Citibank for almost 15 years as legal director and country manager, respectively.

He is a Latin American speaker in forums, workshops and seminars with a focus on ethics and compliance.

Lauren Navarro
Morrison & Foerster LLP

Lauren Navarro is a partner in the firm's investigations and white-collar criminal defence group and a member of the FCPA + Global Anti-Corruption practice. Lauren's practice focuses on complex white-collar criminal matters, including defending clients facing US Department of Justice (DOJ) and US Securities and Exchange Commission (SEC) enforcement proceedings and conducting internal investigations with and without parallel government investigations. Lauren also regularly advises clients on compliance issues including anti-corruption, global risk assessments, training, third-party due diligence, and the development of effective, risk-based compliance programmes. Lauren also has experience in-house after working for six months as an investigator in the ethics and integrity group at a large, multinational software company. Additionally, she was selected by *LatinVex* as one of 'Latin America's Top 25 Rising Legal Stars in 2022'. Lauren has also worked on commercial litigation matters and has experience taking depositions, drafting discovery-related pleadings and motions, and managing document reviews and productions. In addition, Lauren is an active member of the firm's pro bono practice.

Lauren received her JD with pro bono distinction from Stanford Law School, where she was an advanced clinical student in the Stanford Community Law Clinic. While at Stanford, she was also an associate editor of the *Stanford Journal of Law, Business and Finance*, and the co-Vice President of Community Service

and Social Justice for the Women of Stanford Law. She received her BA in international development studies, with a minor in political science, *cum laude* and Phi Beta Kappa from the University of California, Los Angeles. While in law school, Lauren was a legal intern for the US Attorney's Office in the Southern District of New York.

Ben O'Neil
McGuireWoods LLP

Ben is a member of McGuireWoods' nationally ranked government investigations and white-collar litigation department. A former federal prosecutor, he is as skilled in the courtroom as he is in handling clients' most sensitive, high-profile internal matters. He regularly advises corporate entities, boards of directors, audit and special committees, and individuals on their most difficult legal challenges. Ben has particular expertise in criminal and civil fraud matters, with a focus on cross-border Foreign Corrupt Practices Act (FCPA) and Office of Foreign Assets Control (OFAC) sanctions investigations and litigation, as well as significant experience with congressional investigations and crisis situations.

Over the past several years, Ben has been at the forefront of several groundbreaking, global resolutions for corporate entities facing criminal and civil exposure arising from the same conduct in multiple jurisdictions. His experience in navigating the process of cooperation and resolution with regulators spread throughout the world simultaneously has made him uniquely qualified to manage these special situations. He is among only a handful of US lawyers who have achieved these types of global results and is at the forefront of this emerging trend of international criminal law.

Alejandra Pacheco
Chevez, Ruiz, Zamarripa y Cía

Alejandra has advised clients in fintech law matters, including the obtaining of authorisation from the relevant authorities and analysis of the scope of their activities, as permitted under fintech law.

Her professional practice focuses on corporate, financial and capital markets law. She has participated in public and private debt and equity issuances and acquisition offers as well as financing structures with and without collateral.

She has also provided advice to Mexican and foreign entities regarding corporate restructures, including mergers, spin-offs, and purchase and sale of shares and assets, among others, as well as analysis of options and execution of estate planning.

Gustavo Papeschi
Beccar Varela

Gustavo Papeschi is a partner at Beccar Varela, having joined the firm in 2007.

Gustavo specialises in corporate advice, banking and financial institutions, anti-corruption and compliance. He also has extensive experience in advising on distribution and franchising agreements, and on private international law matters.

He obtained his law degree from University of Belgrano in Buenos Aires (first in class Academic Merit Recognition, 2006) and his master of laws (LLM) in international and comparative law from Southern Methodist University, Dedman School of Law (Dallas, Texas, 2013). He worked as a foreign associate at Haynes and Boone, LLP (Dallas, Texas, 2013) and at Holland and Knight, LLP (Miami, Florida, 2014).

He is a member of the Buenos Aires Bar Association, the International Bar Association and, following approval of the New York Bar Exam (2015), he is admitted to practise before the New York State Bar.

Gustavo has been awarded an Excellence Award granted by the City of Buenos Aires Bar Association (2005).

José Pardo
Carey

José Pardo is partner at Carey and co-head of the firm's antitrust and regulated markets group. His main practice includes antitrust, regulation, administrative law and litigation.

He has been recognised in competition and antitrust by international publications such as *Chambers Latin America*, *The Legal 500* and *Best Lawyers*. He is a member of the Litigation Commission of Libertades Públicas AG and a teaching assistant at the University of Chile. He worked as a foreign associate in the antitrust and competition group at Freshfields Bruckhaus Deringer in Brussels (2016–2017).

José is co-author of a book and several articles for national and national publications. He graduated *summa cum laude* from the University of Chile. He also holds an LLM from the University of Chicago and a degree in administrative law from the Catholic University of Chile.

Gabriela Paredes
Anheuser-Busch InBev

Gabriela Paredes is the compliance manager for AB InBev responsible for Ecuador. Gabriela joined AB InBev's ethics and compliance Latin American team in 2021, where she focuses on data privacy and compliance. She has a Master of

Laws (LLM) in international legal studies from NYU and is certified to practise law in Ecuador and the state of New York. She is a board member of the World Compliance Association, Ecuadorian Chapter and has more than seven years of experience in the private sector, practising as a corporate lawyer.

Lorena Pavic
Carey

Lorena Pavic is partner at Carey and co-head of the firm's antitrust and regulated markets, public law, and corporate, mergers and acquisitions groups.

She received the Women in Antitrust award from *Global Competition Review* and was recognised as one of the 100 female leaders in Chile by *El Mercurio* newspaper, both in 2017. She has been widely recognised by international publications, including *Chambers Latin America*, *The Legal 500*, *Latin Lawyer* and *Best Lawyers*, among others.

She is founder and mentor of Carey's mentorship programme for young female lawyers, Learning to Lead, postgraduate professor in many universities and a member of several entities, such as the Chilean Trade Association, the Antitrust Committee of the Chilean Bar Association, the Centre for Antitrust Studies of the Catholic University of Chile, the Women's Competition Network and others.

Lorena graduated *summa cum laude* from the University of Chile and holds a degree in regulation and competition from the same university, and a degree in public law from the Catholic University of Valparaíso.

Martin Pereyra
Vinson & Elkins LLP

Martin Pereyra is an attorney at Vinson & Elkins' New York office. His principal practice area is complex commercial litigation.

Fernando Peyretti
Deloitte

Fernando Peyretti is a partner in Deloitte's forensic services practice in Mexico City, with more than 16 years of consulting experience in projects related to anti-corruption investigations, including investigations with disclosure to the DOJ and the SEC; corporate fraud investigations, including litigation support; integrity due diligence; remedial actions after breaches of the compliance programmes; implementation and audit of anti-corruption compliance programmes; change management and training, risk management; and internal and external audits.

Fernando is the director of the Corporate Fraud Committee of the Argentine Association of Ethics and Compliance, one of the most prestigious non-government organisations in Latin America in this area. Fernando is also a professor in several executive educational programmes including the University of CEMA and other prestigious institutions. Prior to joining Deloitte, Fernando was the forensic practice leader in Argentina for a leading global middle-market accounting firm.

Stephanie Pong
Morrison & Foerster LLP

Stephanie Pong is an associate based in the London office of Morrison & Foerster and is a member of the litigation group. She focuses on advising clients on commercial litigation and complex dispute resolution matters, including cross-border commercial contracts disputes, white-collar crime and internal corporate investigations involving government enforcement agencies. She has experience advising multinational organisations in relation to compliance and regulatory matters, such as anti-money laundering, bribery, anti-corruption and sanctions.

Stephanie received a bachelor of science in chemistry at Imperial College London with a first-class honours and subsequently completed her graduate diploma in law at bpp university and legal practice course at the University of Law with distinctions.

Adriana Prado
FTI Consulting

Adriana Prado is a managing director, based in Brazil, at FTI Consulting. She has over 15 years of experience in major PR firms and media outlets. Ms Prado specialises in the intersection between communications, cybersecurity, data protection and privacy. She frequently presents at tier 1 events in Brazil and conducts workshops in partnerships with key players in this field.

Prior to joining FTI Consulting, Ms Prado was a director at the global communications consulting firm Brunswick Group, where she worked for nearly seven years and participated in major crisis, M&A, litigation and profile-raising projects. She co-led Brunswick's cybersecurity, data protection and privacy offer in Brazil. Ms Prado has also worked for some of the major Brazilian media outlets, such as *O Globo* and *Extra* newspapers, the all-news radio station CBN, and *IstoÉ* magazine. In the corporate communications field, she was part of the FSB PR agency's social media team.

Fluent in English and with intermediate knowledge of Spanish and Italian, she contributed to the Knight Center for Journalism in the Americas at the University of Texas at Austin for almost three years. She graduated in journalism from the Pontifical Catholic University of Rio de Janeiro and took a post-graduate in communications, marketing and information technology at FIA in São Paulo.

Ana Sofía Ríos

Chevez, Ruiz, Zamarripa y Cía

Ana Sofía's legal practice focuses on corporate law, banking and finance, including mergers and acquisitions, private equity, as well as advising clients and family offices on wealth management matters. In addition, Ana Sofia advises by public and private companies on corporate governance and regulatory compliance matters.

She has represented, among others, domestic and foreign issuers, underwriters, investors, purchasers, sellers, lenders and borrowers in securities offerings, stock and asset acquisitions, financing transactions, reorganisations and restructurings.

Ana Sofía has also focused on fintech law, advising technology companies, start-ups and investors across the sector. She has participated in advising technology companies in regulatory and financial matters. Ana Sofia has also advised domestic and foreign entrepreneurs and participated in financing new ventures and start-ups.

Raúl Saccani

Deloitte

Raúl Saccani has more than 20 years of international experience in compliance and financial crimes prevention. Raul is a Deloitte partner leading the anti-corruption and financial crime function within Spanish Latin American countries. President of the Integrity and Compliance Commission at the Economic Science Professional's Council in Buenos Aires. Raul is a lecturer and director of the Governance and Transparency Centre at IAE Business School.

Raúl provided expert testimony at the World Bank (ICSID) and the ICC international arbitrations. Co-Director of the Compliance Treatise (Thomson Reuters, 2018) and author of the Forensic Audit Treatise (Thomson Reuters, 2012).

Martín Sánchez

Mijares Angoitia Cortés y Fuentes SC

Martín has experience in capital markets, mergers and acquisitions and corporate finance.

He regularly represents issuers and underwriters in equity issuances, structured equity transactions (FIBRA, CERPI and CKD), multiple offering programmes, corporate and labeled or sustainable debt issuances, equity and debt takeover bids and complex multi-financing structures involving the issuance of structured or project bonds in Mexico and international markets. He also advises issuers on regulatory and compliance matters and procedures related to regulatory authorities.

In relation to the above, Martín advises issuers and companies in regulated sectors in the adoption of ESG standards, in the implementation of compliance programs aligned with the ESG strategy of companies and leads the firm's ESG and compliance practice.

John Sardar

Anheuser-Busch InBev

John Sardar joined AB InBev as global head of compliance in July 2022. He has over two decades of global legal and compliance experience in private and in-house practice and working for the US government. Before AB InBev, he served as chief ethics and compliance officer for two publicly traded companies, including working in the highly regulated oil and gas industry. John earned a bachelor's degree in economics from California State University at Long Beach and a law degree from St. Louis University. John frequently speaks at domestic and international conferences addressing legal and regulatory compliance issues.

Diego Sierra Laris

Von Wobeser y Sierra, SC

Diego Sierra Laris is admitted to practise law in Mexico and New York, and has working experience in New York. He concentrates his practice in in anti-corruption and compliance matters. He has more than 16 years of experience and frequently acts as counsel in complex commercial litigation. Diego Sierra has advised companies and financial institutions in the United States and Mexico in FCPA investigations and due diligence matters. In addition, he has acted as an expert on Mexican law before different courts and agencies.

Gabriel Silva

Vinson & Elkins LLP

Gabriel Silva is a partner at Vinson & Elkins LLP's New York office. Gabriel's principal area of practice is corporate finance. He works with a variety of public and private companies as well as private equity investors and their portfolio companies in connection with mergers, acquisitions, dispositions and securities offerings. His

practice has a global reach, spanning Latin America, the United States, Europe and Asia, and involves extensive experience advising a multinational client base of leading corporations and financial sponsors on complex, cross-border transactions. In particular, Gabriel has significant experience in transactions in the digital infrastructure sector, such as telecoms towers, data centres and fiber.

Jordan Leigh Smith
Davis Polk & Wardwell LLP

Jordan Leigh Smith advises clients on compliance and anti-corruption matters, including providing advice on civil, criminal and internal investigations relating to alleged violations of the Foreign Corrupt Practices Act (FCPA), fraud and other financial crimes. Her significant experience in compliance includes serving as acting chief compliance officer for a global industrial company.

She assesses compliance programmes, advises on remediation steps and implementation of effective compliance programmes, engages in risk assessments, and advises on corporate governance issues. She conducts due diligence and provides strategic, structural, contractual and risk mitigation advice in connection with M&A, joint ventures, investments and third-party engagements.

Clients also turn to Jordan for practical advice on day-to-day compliance issues, including in connection with contractual negotiations, reviewing policies and procedures, enhancing internal systems and controls, training and disciplinary issues.

Ruti Smithline
Morrison & Foerster LLP

Ruti Smithline is a partner in the securities litigation, enforcement and white-collar criminal defence group. Her practice focuses on complex litigation, with an emphasis on white-collar criminal defence, SEC enforcement, securities litigation and corporate internal investigations.

Ruti is a member of Morrison & Foerster's FCPA and anti-corruption task force, as well as the co-chair of the firm's investigations and white-collar defence practice and Latin America desk. She regularly advises clients on cross-border investigations, global compliance programmes and anti-corruption due diligence for acquisitions, joint ventures and private equity transactions. Ruti has represented individual and corporate defendants in cross-border criminal investigations, SEC enforcement matters and other regulatory proceedings, including matters related to trade sanctions and anti-money laundering. She has experience conducting corporate internal investigations both domestically and internationally, often advising clients on remedial measures responsive to the issues investigated.

Ruti was born and raised in Colombia and is fluent in Spanish. She has conducted investigations, seminars and anti-corruption training in Spanish throughout Central and South America.

Ruti is regularly recognised by leading industry publications such as *Chambers & Partners* in their Latin America guide for corporate crime and investigations – international counsel and in their US guide for nationwide FCPA. Additionally, *Global Investigations Review* named Ruti in its prestigious list of top 2018 women in investigations and she was also selected by *LatinVex* as one of 'Latin America's Top 100 Lawyers: FCPA & Fraud' for 2021.

Peter Spivack
Hogan Lovells

Peter Spivack is a partner at Hogan Lovells. He is one of the most experienced members of the investigations, white collar and fraud practice area and served as the global co-leader of the practice for six years. His experience in the criminal arena includes antitrust, environmental, Foreign Corrupt Practices Act (FCPA), government contract, and healthcare matters. According to Chambers and Partners, where he is ranked in both the White Collar and FCPA practice areas, clients call him 'fantastic' and say that he 'is very insightful and a very good communicator'. Peter has been named as one of the world's top FCPA practitioners by Global Investigations Review.

Peter has three decades of experience working with multi-jurisdictional investigation. He has represented companies and individuals in investigations brought by multilateral institutions such as the World Bank and Inter-American Development Bank. Peter also has considerable experience in representing entities and individuals in criminal and civil enforcement matters involving health care, government contracts, competition and antitrust issues.

Peter frequently writes and speaks on federal criminal issues. He plays an active role in the bar, currently serving as a co-chair of the Health Care Fraud Subcommittee for the ABA White Collar Crime Committee and as a past co-chair of the Criminal Law and Individual Rights Committee for the DC Bar.

Mayra Suárez
Skadden, Arps, Slate, Meagher & Flom LLP

Mayra Suárez is a counsel in the firm's litigation and government enforcement and white-collar crime groups. She has conducted internal investigations on behalf of US and foreign corporations, audit committees and individuals in the United States, Europe, Africa and Latin America. She also has defended clients in connection with investigations by the US Department of Justice and

the Securities and Exchange Commission, including those relating to the US Foreign Corrupt Practices Act. She regularly advises clients on improvements to their compliance policies and procedures.

G Zachary Terwilliger
Vinson & Elkins LLP

G Zachary Terwilliger is a partner at Vinson & Elkins LLP based in Washington, DC. Zach advises corporate clients and individuals who are subject to criminal investigations and civil enforcement actions. Additionally, he handles uniquely Washington problems related to congressional inquiries and interfacing with leadership at the highest levels of the Department of Justice.

Prior to joining Vinson and Elkins, Zach served for 14 years at the Department of Justice. His most recent position was as the presidentially appointed and Senate confirmed United States Attorney for the Eastern District of Virginia – home to some of the most complex and high-profile cases in the country. Zach also served as an Associate Deputy Attorney General in the Office of the Deputy Attorney General with responsibility for criminal matters.

Zach also spent over a decade as an Assistant United States Attorney in the Eastern District of Virginia. Just prior to becoming an AUSA, Zach served as law clerk to the Hon. K. Michael Moore, who serves as the Chief Judge of the United States District Court for the Southern District of Florida. Zach graduated with highest honours from William & Mary School of Law. He obtained his undergraduate degree at the University of Virginia.

Dheeraj Thimmaiah
Anheuser-Busch InBev

Dheeraj Thimmaiah is the global head of compliance analytics for AB InBev. Dheeraj joined AB InBev's global ethics and compliance team in 2019, where he serves as a global director with a focus in analytics and legal technologies.

Before joining AB InBev, Dheeraj was a senior manager in EY's forensics practice in NY, serving clients with a focus in designing, developing and operationalising enterprise compliance solutions focusing on fraud, corruption and monitoring controls and policies.

He is recognised as a leader in the application of data analytics to demystify compliance problems, streamline compliance systems and processes enabled by technology.

Benjamín Torres
Carey

Benjamín Torres is an associate at Carey and a member of the antitrust and regulated markets group. His practice focuses on antitrust, litigation and mergers and acquisitions.

He has been a teaching assistant in procedural law, civil law and Roman law at the University of Chile. Before becoming associate, he worked as a law clerk for the same group at Carey. He graduated *summa cum laude* from the University of Chile.

Krystal Vazquez
Ropes & Gray

Krystal Anali Vazquez joined Ropes & Gray's litigation and enforcement group in 2019. As an associate, she focuses her practice on governmental and internal investigations, white-collar criminal defence, and anti-corruption matters. Her experience includes representing companies in matters involving the Foreign Corrupt Practices Act, government enforcement actions, internal investigations, and complex commercial litigation. Krystal also maintains an active pro bono practice.

APPENDIX 2

Contributors' Contact Details

Andrew B Jánszky
Tel: +1 917 873 7322 /
+55 11 99939 0363
a@janszky.com.br

Anheuser-Busch InBev
250 Park Avenue, 2nd Floor
New York, NY 10017
United States
Tel: +1 212 573 8800
dheeraj.thimmaiah@ab-inbev.com
jaime.munoz2@co.ab-inbev.com
john.sardar@ab-inbev.com
gabriela.paredes@ab-inbev.com
www.ab-inbev.com

Beccar Varela
Edificio República
Tucumán 1, 3rd floor
Buenos Aires
Argentina
Tel: +54 11 4379 6800/4700
mdauro@beccarvarela.com
gpapeschi@beccarvarela.com
www.beccarvarela.com

Carey y Cía
Isidora Goyenechea 2800
43rd floor
Las Condes
Santiago
Chile
Tel: +56 2 2928 2200
Fax: +56 2 2928 2228
lpavic@carey.cl
jpardo@carey.cl
btorres@carey.cl
rgalvez@carey.cl
www.carey.cl

Chevez, Ruiz, Zamarripa y Cía
Vasco de Quiroga 2121
4th floor, Peña Blanca Santa Fe
Mexico City C.P 01210
Mexico
Tel: + 52 55 5257 7000
asrios@chevez.com.mx
vibarra@chevez.com.mx
apacheco@chevez.com.mx
www.chevez.com

Davis Polk & Wardwell LLP
450 Lexington Avenue
New York NY 10017
United States
Tel: +1 212 450 4000
daniel.kahn@davispolk.com
tatiana.martins@davispolk.com
jordan.smith@davispolk.com
www.davispolk.com

Debevoise & Plimpton LLP
66 Hudson Boulevard
New York, NY 10001
United States
Tel: +1 212 909 6000
Fax: +1 212 909 6836
amlevine@debevoise.com
eogrosz@debevoise.com
www.debevoise.com

Deloitte
Deloitte
1700 Market Street
Suite 2700
Philadelphia PA 19103
United States
Tel: +1 786 488 2434
neluis@deloitte.com

Paseo de la Reforma 505, piso 28
Colonia Cuauhtémoc,
06500, Ciudad de México
México
Tel: +52 55 5080 6046
fpeyretti@deloittemx.com

Florida 234 Piso 5°
CABA, Buenos Aires
C1005AAF
Buenos Aires, Argentina
Tel: +54 (011) 4320 2700
rsaccani@deloitte.com

www.deloitte.com

FTI Consulting
555 12th Street NW Suite 700
Washington, DC 20004
United States
Tel: +1 202 312 9100
jordan.kelly@fticonsulting.com
antonio.gesteira@fticonsulting.com
adriana.prado@fticonsulting.com
www.fticonsulting.com

Hogan Lovells
555 Thirteenth Street, NW
Washington, DC 20004
United States
Tel: +1 202 637 5631
peter.spivack@hoganlovells.com

Edifício Plaza JK
Av. Pres. Juscelino Kubitschek, 1700,
14th floor
Itaim Bibi
São Paulo, SP 04543-000
Brazil
Tel: +55 11 3074 3501
isabel.carvalho@hoganlovells.com

www.hoganlovells.com

Hughes Hubbard & Reed
1775 I Street, NW
Washington, DC, 20006-2401
United States
Tel: +1 202 721 4600
ryan.fayhee@hugheshubbard.com
diego.duran@hugheshubbard.com
tyler.grove@hugheshubbard.com
anna.hamati@hugheshubbard.com
www.hugheshubbard.com

Incode Technologies Inc.
221 Main St. Suite 520
San Francisco, CA 94105
United States
Tel: +1 650 446 3444
reynaldo.manzanarez@incode.com
www.incode.com

McGuireWoods LLP
888 16th Street NW, Suite 500
Black Lives Matter Plaza
Washington, DC 20006
Tel: +1 202 857 1700
boneil@mcguirewoods.com
ebaur@mcguirewoods.com
www.mcguirewoods.com

Mijares Angoitia Cortés y Fuentes SC
Javier Barros Sierra 540, 4th floor
Park Plaza I, Colonia Santa Fe
Alc. Álvaro Obregón
Mexico City 01210
Mexico
Tel: +52 55 5201 7400
msanchez@macf.com.mx
gcalvillo@macf.com.mx
mamorales@macf.com.mx
pxperez@macf.com.mx
www.macf.com.mx
https://macf.com.mx/esging

Morrison & Foerster LLP
250 West 55th Street
New York, NY 10019-9601
United States
Tel: +1 212 468 8000
hichilcik@mofo.com
jkoukios@mofo.com
lnavarro@mofo.com
rsmithline@mofo.com
spong@mofo.com
gkinsella@mofo.com
www.mofo.com

Ropes & Gray
1211 Avenue of the Americas
New York, NY 10036-8704
United States
Tel: +1 212 596 9000

2099 Pennsylvania Avenue
NW Washington, DC 20006-6807
United States
Tel: +1 202 508 4600

baldemar.gonzalez@ropesgray.com
krystal.vazquez@ropesgray.com
maria.calvet@ropesgray.com
www.ropesgray.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001-8602
United States
Tel: +1 212 735 3000
julie.bedard@skadden.com
maria.cruzmelendez@skadden.com

1440 New York Avenue, NW
Washington, DC 20005
United States
Tel: +1 202 371 7000
mayra.suarez@skadden.com

www.skadden.com

Sullivan & Cromwell LLP
125 Broad Street
New York, NY 10004-2498
United States
Tel: +1 212 558 4000
Fax: +1 212 558 3588

1870 Embarcadero Road
Palo Alto, California 94303-3308
United States
Tel: +1 650 461 5600

1888 Century Park East
Los Angeles, California 90067-1725
United States
Tel: +1 310 712 6600

cullenb@sullcrom.com
lewisan@sullcrom.com
www.sullcrom.com

Vinson & Elkins LLP
1114 Avenue of the Americas
32nd Floor
New York, NY 10036
United States
Tel: +1 212 237 0000
pfava@velaw.com
zterwilliger@velaw.com
gsilva@velaw.com
cjames@velaw.com
mpereyra@velaw.com
www.velaw.com

Von Wobeser y Sierra, SC
Paseo de los Tamarindos, 60
Bosques de las Lomas
Cuajimalpa de Morelos
Mexico City 05120
Mexico
Tel: +52 55 5258 1000
amagallanes@vwys.com.mx
dsierra@vwys.com.mx
www.vonwobeser.com