GIR Global Investigations Review

United States: fresh legislation targets corporate crime and incentivises compliance

 Michael Diaz, Jr

 Javier D Coronado Diaz

drt DIAZREUS INTERNATIONAL LAW FIRM

13 November 2024

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

Nodus International Bank, a Puerto Rican bank, has been at the centre of a high-profile criminal investigation involving the Department of Justice (DOJ), various federal agencies and Puerto Rican regulators. Nodus entered a liquidation plan under the supervision of Puerto Rico's Commissioner of Financial Institutions Office (OCIF). The bank agreed to cease operations and use its licence solely for liquidating its assets and returning depositors' money. In March 2023, however, OCIF discovered that Nodus had made insider payments to directors, shareholders and affiliated individuals and companies, rather than adhering to the liquidation plan.

The ongoing criminal investigation has led to the freezing of approximately US$80 million in assets located in Miami, Puerto Rico and several Latin American countries. Nodus is also facing multiple lawsuits in the United States from account holders who have lost access to their funds due to the bank's wrongful diversion of payments in violation of the liquidation plan. Many affected account holders had entrusted their money to Nodus, believing it would be safer in an international bank than in a local financial institution.

The situation could deteriorate further because the bank's accounts are not covered by the Federal Deposit Insurance Corporation because it operated as an international banking entity in Puerto Rico, thus excluding it from US federal insurance. Additionally, this is not the first time Nodus may have run afoul of US law. On 18 October 2022, the Office of Foreign Assets Control (OFAC) issued a finding of violation, concluding that Nodus violated US sanctions relating to Venezuela by knowingly transacting with blocked funds without an OFAC licence and failing to maintain relevant records for these transactions.

2 Outline the legal framework for corporate liability in your country.

A state or federal statute will typically provide the legal basis for authorities to investigate and prosecute a corporation, as well as the way in which a corporation's criminal liability should be determined. Additionally, under the common law doctrine of *respondeat superior*, a corporation may be held liable based on the actions of its directors, officers, employees or other agents if those actions were within the scope of the agents' duties and benefited or sought to benefit the corporation.

According to the DOJ's 'Principles of Federal Prosecution of Business Organizations', there are 11 factors that federal prosecutors should consider in deciding whether to criminally charge a corporation:

- the nature and seriousness of the offence;
- the pervasiveness of wrongdoing within the corporation;
- the corporation's history of similar misconduct;
- the corporation's willingness to cooperate;
- the adequacy and effectiveness of the corporation's compliance programme at the time of the

offence, as well as at the time of a charging or resolution decision;
- the corporation's timely and voluntary disclosure of wrongdoing;
- the corporation's remedial actions;
- collateral consequences;
- the adequacy of remedies, such as civil or regulatory enforcement actions;
- the adequacy of the prosecution of individuals responsible for the corporation's malfeasance; and
- the interest of any victims.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Various law enforcement agencies may investigate corporations, each with specific jurisdiction based on the nature of the potential wrongdoing and industry involved in the case. The allocation of the jurisdiction among these authorities is defined by each agency's statutory and regulatory frameworks. These agencies include:

- the DOJ, which includes the US Attorney's Office in each federal district, the Federal Bureau of Investigation and the Drug Enforcement Agency. The DOJ is the primary federal agency responsible for investigating and enforcing federal laws, including criminal laws applicable to corporations;
- the Securities and Exchange Commission, which, through its Enforcement Division, investigates possible violations of federal securities laws and the regulations promulgated thereunder;
- the Federal Trade Commission, which conducts investigations of potential violations of the Federal Trade Commission Act, such as unfair or deceptive acts or practices, fraud, scams, identity theft, false advertising and privacy violations;
- the US Department of the Treasury's Financial Crimes Enforcement Network, which receives, analyses and disseminates financial transactions data for law enforcement purposes;
- the Department of Homeland Security, which, through divisions such as Homeland Security Investigations, US Immigration and Custom Enforcement and US Customs and Border Protection, investigates crimes relating to cross-border criminal activities that threaten the US's security;
- OFAC, which administers and enforces economic sanctions against targeted foreign countries, entities and individuals to further US foreign policy and national security. OFAC enforces sanctions in coordination with other executive branch agencies, such as the US Department of Commerce's Bureau of Industry and Security, as well as various subdivisions within the Department of State and the DOJ; and
- other agencies that investigate financial crime, including the US Secret Service and the Internal Revenue Service's Criminal Investigation.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

An investigation is usually initiated when a government agency receives credible information reporting an activity that violates federal or state laws or regulations. This information may come from a human source (such as the victim, a witness or an informant), a written report (such as a suspicious activity report), a request made by a foreign government, a request made by a US member of Congress or from publicly available sources. A common method to compel information is for the US government to revoke the US visa of the subjects of a criminal investigation, which incentivises the relevant person to come forward and enquire or cooperate with law enforcement authorities.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

The process to challenge a notice or subpoena from an authority is very broad and it can vary depending on the type of authority issuing the notice or subpoena or the civil or criminal nature of the notice or subpoena. One way to challenge the lawfulness or scope of a notice or subpoena is through a motion to quash or modify, suggesting lack of jurisdiction because of the extraterritorial nature of the subpoena. Similarly, a motion to quash or modify a subpoena can be filed before the court with the purpose to challenge legal sufficiency or validity of the subpoena in question.

If a motion to quash or modify is denied, a party may have to comply with the subpoena. However, if compliance with the subpoena might result in the disclosure of sensitive or confidential information, a motion for protective order can be filed with the court to limit the use or disclosure of the information.

6 Does your country make use of cooperative agreements giving immunity or leniency to individuals who assist or cooperate with authorities?

US prosecutors often resolve financial crime cases through non-prosecution agreements and deferred prosecution agreements. Under these agreements, the DOJ may agree to not prosecute the target of the investigation if the target agrees to cooperate with the government and to implement remedial or compliance measures. The defendant's cooperation with the government may also be required under a plea agreement whereby the defendant accepts all or some of the criminal charges in exchange for the government:

- to agree not to bring certain criminal charges;
- to recommend or agree not to oppose the defendant's request that a sentence or sentencing range is appropriate; or
- to agree that a specific sentence or sentencing range is the appropriate disposition of the case.

Furthermore, during a criminal investigation, the government may extend an agreement wherein, in exchange for an individual's testimony, it commits to refraining from prosecuting the witness for the offences pertinent to their testimony (transactional immunity). Alternatively, the government may agree not to utilise the witness's testimony against them in a prosecution, except in circumstances involving perjury or the provision of false statements in subsequent proceedings (use immunity).

7 What are the top priorities for your country's law enforcement authorities?

In recent years, the United States has prioritised law enforcement actions targeting the following criminal activity, in no particular order: corruption, sanctions evasion, cybercrime, terrorist financing, fraud, transnational criminal organisation activity, drug trafficking, human trafficking and human smuggling, and proliferation financing.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

Each government agency provides official guidance on what makes an effective compliance programme. There is a heightened push from US law enforcement to evaluate whether a company has used a 'risk-based approach' to design, implement and periodically update compliance programmes. Accordingly, the compliance programme of each organisation should be different and tailored to the company's industry, products and clients, as well as to the risks associated with the jurisdictions in which the company has operations. Nevertheless, US authorities typically expect organisations to develop the following essential and base components of compliance:

- *management commitment*: ensuring senior management commit to the company's compliance with US law;
- *risk assessment*: conducting frequent risk assessments to identify and mitigate specific risks;
- *internal controls*: developing and deploying policies and procedures to identify, interdict, escalate, report and maintain records pertaining to activity prohibited by US law;
- *testing and audit*: identifying and correcting weaknesses and deficiencies; and
- *training*: ensuring all relevant personnel are provided with tailored training on the pertinent US law.

Cyber-related issues

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

The United States regulates cybersecurity through a combination of federal and state laws, as well as industry-specific regulations. For instance, the Cybersecurity Information Sharing Act of 2015 establishes guidelines for sharing cyber information between public and private entities to ensure the protection of personally identifiable information.

Cybersecurity has also been a major concern for the US government over the years. For instance, Executive Order (EO) 13694 focuses on specific harms caused by significant malicious cyber-enabled activities and directs the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to impose sanctions on those persons who are determined to be responsible for, or complicit in, activities leading to harm. On 12 May 2021, the president issued EO 14028, 'Improving the Nation's Cybersecurity', which seeks to remove barriers to sharing threat information between the government and private sector, and implement stronger cybersecurity standards in the federal government.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Yes. For example, after EO 13694 was issued by the president, the Office of Foreign Assets Control (OFAC) implemented a cyber-related sanctions programme to address the threat to US national security, foreign policy and economy caused by the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by, persons located, in whole or in substantial part, outside the United States. OFAC has imposed economic sanctions on a number of individuals and companies for their roles in cyber operations against the United States.

The US government is particularly concerned about cyber-enabled financial crime, ransomware attacks and the misuse of cryptocurrency and other virtual assets for the laundering of illicit proceeds.

Cross-border issues and foreign authorities

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

US criminal laws are primarily intended to apply within the territorial boundaries of the United States. However, there are specific circumstances and offences in which US federal statutes provide for extraterritorial jurisdiction in cases involving terrorism, drug and human trafficking, and foreign corruption. For example, in December 2023, the president signed the Foreign Extortion Prevention Act (FEPA) into law, which directly allows the US government to investigate and prosecute foreign officials that solicit or accept bribes from US entities or individuals.

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Cross-border investigations present a complex array of challenges, particularly when they involve jurisdictions with differing legal systems and enforcement priorities. These challenges vary depending on the countries involved, the nature of the investigation and the level of cooperation between the US and foreign authorities.

Some of the challenges include differences in the appropriate legal response to potential wrongdoing. For instance, while facilitation payments may be exempt from penalties under the Foreign Corrupt Practices Act (FCPA), they could be illegal under the anti-bribery laws of many other countries. Also, while some countries have strong cooperative relationships with US authorities, others may be less willing or unable to cooperate. This can be due to political reasons, lack of resources or differences in legal and enforcement priorities.

Mutual legal assistance treaties (MLATs) are key tools for cooperation in cross-border investigations, allowing countries to request legal assistance from one another. However, some countries may not have MLATs with the United States, or may interpret the treaties narrowly, limiting the scope of cooperation.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The principle of double jeopardy generally does not apply to prevent a corporation from facing criminal exposure after resolving charges on the same core set of facts in another country. The US legal system adheres to the concept of 'separate sovereigns', meaning that different jurisdictions, such as federal, state and foreign governments, can prosecute the same conduct independently without violating double jeopardy protections.

However, the Department of Justice formally recognised the benefits of coordinating multi-jurisdictional resolutions in 2018, when it adopted the 'anti-piling on' policy. This policy encourages coordination between US authorities and foreign regulators to ensure that penalties are proportionate and not duplicative, taking into account penalties already imposed by other jurisdictions.

14 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are becoming increasingly common, especially in complex white-collar investigations involving multinational corporations. For instance, cases involving violations of the FCPA or antitrust laws often require coordination with foreign regulators. Practical considerations when negotiating global settlements include coordination among US and foreign regulators to ensure consistency in the settlement terms and results that are acceptable across all jurisdictions, as well as sharing internal investigation findings and other pertinent data across borders while complying with varying privacy and data protection laws. Additionally, compliance and monitoring obligations need to be harmonised across jurisdictions to ensure efficient implementation and reporting following the global settlement.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

A criminal ruling against a corporation in another country will not necessarily impact an ongoing investigation. However, in practice, a decision by a foreign authority may influence an investigation. For example, if a corporation is found guilty of bribery in a foreign country, US authorities may use the evidence and findings from that case to bolster their own investigation under FEPA or the FCPA. Additionally, the outcome of the foreign case could provide valuable insights or lead to new evidence that impacts the direction and focus of the US investigation.

Economic sanctions enforcement

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Generally, Office of Foreign Assets Control (OFAC) sanctions require US persons to block assets or restrict financial or trade-related activities with the target of these sanctions. Notably, OFAC may enforce two types of sanctions involving a country: comprehensive sanctions (also known as embargoes), which prohibit all transactions between the designated country and US persons, and non-comprehensive sanctions, which limit certain transactions involving the country as specified by laws enacted by Congress, executive orders or OFAC regulations and guidelines.

US law imposes both civil and criminal penalties on individuals found in violation of OFAC sanctions, encompassing acts of violation, attempted violation, conspiracy to violate or causation of a violation. Foreign entities may also be subject to civil or criminal actions if they conspire to violate or cause a violation of OFAC sanctions. Additionally, certain sanctions programmes authorise OFAC to block foreign persons that directly or indirectly violate OFAC sanctions.

Currently, OFAC administers 38 sanctions programmes in an effort to deter various threats to US foreign policy and national security.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Regarding sanctions targeting individuals and organisations, OFAC publishes and continually updates a series of lists, including the Specially Designated Nationals and Blocked Persons List (the SDN List).

Unless authorised by a general or specific licence issued by OFAC, US persons are prohibited from engaging in transactions with any listed individual or entity, or with any entity in which they have, directly or indirectly, 50 per cent or greater ownership interest. Additionally, all of the listed individual's or entity's property or interest in property within or transiting any US jurisdiction are blocked.

The SDN List contains over 9,400 names, and OFAC designations have steadily increased since 2000.

18 Do the authorities responsible for sanctions compliance and enforcement in your country cooperate with their counterparts in other countries for the purposes of enforcement?

The US government cooperates with agencies in the European Union and with countries such as the United Kingdom, Canada and Australia. For example, the United States and its allies established a multilateral Russian Elites, Proxies and Oligarchs Task Force to collaborate on the enforcement of economic sanctions related to Russia.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

No.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Not applicable in this jurisdiction.

Before an internal investigation

21 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct generally come to light through regulatory reporting requirements, internal audits and investigations that result in voluntary self-disclosures, whistleblower complaints, customer or supplier complaints, media reports or parallel civil litigation that exposes potential crimes related to money laundering or terrorist financing activities, corporate fraud, violations of US anti-corruption statutes, insider trading, sanctions evasion or cryptocurrency-related crimes.

Information gathering

22 Does your country have a data protection regime?

The United States does not have a comprehensive data protection regime. However, it relies on a combination of federal and state laws that focus on specific aspects of data protection and privacy. Federal laws include the following:

- the Health Insurance Portability and Accountability Act, which establishes national standards to protect sensitive patient health;
- the Gramm-Leach-Bliley Act, which establishes data protection standards concerning consumers' personal financial information for financial institutions;
- the Children's Online Privacy Protection Act, which imposes specific requirements on operators of websites or online services that are directed towards children;
- the Fair Credit Reporting Act, which regulates the collection, dissemination and use of consumer information;
- the Federal Trade Commission Act (the FTC Act), which empowers the Federal Trade Commission (FTC) to take action against unfair or deceptive practices related to the privacy and security of personal data; and
- the Electronic Communications Privacy Act, which has provisions protecting the privacy of electronic communications.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

Because there is no comprehensive data protection regime, the consequences of a data breach vary depending on the federal statute or regulation at issue. For example, the FTC Act empowers the FTC to take action against unfair or deceptive practices related to the privacy and security of personal data by seeking court orders to stop companies from engaging in these practices, imposing monetary penalties on companies or pursuing refunds or compensation for consumers who have been harmed by a company's unfair or deceptive practices.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

While the United States does not have a comprehensive federal data protection law, there are still several data protection issues that can cause concern during internal investigations, particularly in the context of white-collar crime. For example, industries such as healthcare and finance are subject to regulations that impose data protection obligations. Similarly, pursuant to the Federal Rules of Procedure and Evidence, companies must have clear policies regarding the retention and deletion of

data relevant to the investigation to avoid potential claims of evidence spoliation or obstruction of justice. Additionally, employers must navigate any state laws that protect employee privacy, especially concerning personal communications and data stored on personal devices.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

There is no comprehensive data protection regime and there is no right to privacy in an office or company-issued device. However, the United States regulates interception of employees' personal communications through federal and state laws. As an example, the Electronic Communications Privacy Act prohibits intentional actual or attempted interception, use, disclosure or procurement of any other person to intercept or endeavour to intercept any wire, oral or electronic communication from an employee's personal device. Accordingly, employers generally need at least one party's consent to intercept communications from personal devices; however, some states have stricter rules and require both parties to consent.

Dawn raids and search warrants

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

US law enforcement generally uses subpoenas to obtain documents and other material from companies. However, law enforcement may also use search warrants for these purposes. To obtain a search warrant, the authorities must show that probable cause exists to believe that a crime has been committed and that the evidence is likely to be found at the specified location. Once obtained, the warrant allows the authorities to enter the premises, and search for and seize evidence. If the authorities do not adhere to the terms of a search warrant or were not truthful in obtaining it, a court may exclude any improperly seized documents from being used as evidence in legal proceedings. Additionally, if law enforcement obtains other evidence derived from the illegally seized evidence, courts may also exclude that derivative evidence.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

To lawfully protect privileged material from seizure during a dawn raid or in response to a search warrant, the organisations must assert privilege claims in real time and request that the documents be sealed and reviewed by a court before any examination by investigators. Accordingly, organisations should maintain logs that clearly identify privileged documents and communications so they can quickly identify and argue against the seizure of the material. Having legal counsel present during the search could also be advantageous, and cooperation with authorities can be beneficial. Government agencies may agree to protocols for handling potentially privileged information.

Following the seizure, motions can be filed with a federal court for the return of unlawfully seized privileged materials and property.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

At the federal level, when the government requires the testimony of a person in connection with an ongoing criminal investigation, it may seek a grand jury subpoena compelling that person's declaration. This subpoena may also be used to order the person to produce material for the criminal investigation. States provide for similar legal avenues for law enforcement to compel the appearance of a person for interview.

However, under the Fifth Amendment, an individual cannot be forced to provide self-incriminating testimony. Any testimony that is improperly compelled cannot be used against the individual in court. This privilege does not extend to companies, which cannot refuse to provide testimony even if it might be incriminating.

Whistleblowing and employee rights

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

The United States has a number of federal programmes that incentivise whistleblowers and protect them from retaliation. For example, on 1 August 2024, the Department of Justice's Criminal Division launched a Corporate Whistleblower Awards Pilot Program to uncover and prosecute corporate crime. Whistleblowers may be eligible for an award pursuant to this programme when they provide original, truthful information about certain types of criminal misconduct, where that information leads to forfeitures exceeding US$1 million in net proceeds. As described in more detail in the programme guidance, the information must relate to: (1) certain crimes involving financial institutions, from traditional banks to cryptocurrency businesses; (2) foreign corruption involving misconduct by companies; (3) domestic corruption involving misconduct by companies; or (4) healthcare fraud schemes involving private insurance plans.

The Securities and Exchange Commission, the Commodity Futures Trading Commission and the US Department of the Treasury's Financial Crimes Enforcement Network have also established whistleblower programmes to encourage the reporting of potential misconduct under their purview.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

There is no US federal employment law specifying an employee's rights during an investigation. However, employees who report misconduct or cooperate with investigations as whistleblowers may be protected from retaliation under statutes such as the Sarbanes-Oxley Act of 2002 and the Dodd-Frank Act of 2010. Retaliation practices that are forbidden by US federal law include retaliating against employees who file complaints or participate in investigations into discrimination based on race, colour, religion, sex or national origin.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Unless whistleblower or anti-retaliation protections are in place under federal law, a company may freely impose disciplinary measures on an employee involved in misconduct, such as suspension, termination, demotion, written warning or reprimand, and probation. Suspension is recommended when the alleged misconduct could pose a risk to the company or other employees if the employee remains at work.

Additionally, organisations may be required to act upon learning of an employee's misconduct to prevent negative legal consequences. For instance, if an organisation fails to suspend an employee who is under investigation for serious misconduct, it could be exposed to legal actions for breach of fiduciary duties.

32 Can an employee be dismissed for refusing to participate in an internal investigation?

Most employees are employed at will, meaning their employment can be terminated at any time unless specific protections apply. Accordingly, failure to cooperate in an internal investigation can lead to dismissal.

Commencing an internal investigation

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

Internal investigations often rely on a detailed investigation or work plan that sets out the person or persons who will conduct the investigation, the scope of the investigation, an estimate of the timing to complete the investigation, the persons or entities to be investigated and a process for document and interview collection and review. Ordinarily, the plan should also specify how the results of the investigation are to be reported.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

There are generally no internal steps that a company is legally or ethically required to take when an issue comes to light. If a company discovers misconduct, its best course of action is to immediately draft an investigation or work plan and begin an internal investigation to gather all material facts regarding the misconduct. After completing an investigation, the company will be best suited to decide on its next steps, such as whether to disclose its findings to the government.

If a company chooses to undergo an internal investigation, it should ensure that its investigation complies with the requirements of *Upjohn v. United States* to enjoy the benefits of the attorney–client privilege and the work-product doctrine. Pursuant to *Upjohn*, a lawyer must disclose their role as corporate counsel to a witness in case the witness's interests may be adverse to the company or if the witness is mistaken as to the lawyer's role. The *Upjohn* warning also helps to avoid a potential conflict of interest as an interviewing lawyer may inadvertently create an implied attorney–client relationship with the witness.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Upon receiving a notice or subpoena, the company should issue a litigation hold to its employees requiring them to preserve any relevant information. Then, the company should identify all custodians of potential responsive documents and instruct its employees on how to find and collect further information. The company must then oversee the collection process and monitor document preservation efforts to ensure they comply with the notice or subpoena. Finally, the company should review all collected information, separate out privileged information and submit all collected non-privileged information to the requesting authorities in compliance with the subpoena's requirements.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Companies are generally not required to publicly disclose the existence of an internal investigation or contact from law enforcement authorities. However, under the Securities and Exchange Commission's Regulation S-K, a company must publicly disclose the existence of an internal investigation or contact from a law enforcement authority when the matter becomes material to investors and could influence their decisions. An investigation or inquiry is deemed material if it could have a significant impact on the company's financial condition or operating results, or if it raises substantial legal or regulatory risks that could affect the company's business operations. Additionally, if a company is involved in a government investigation or legal proceedings that are likely to result in a significant financial impact or affect its operations, this must be disclosed to ensure transparency for investors and to comply with the broader principles of fair and accurate financial reporting.

For other matters, a company may choose to file a voluntary self-disclosure with the Department of Justice (DOJ) or the relevant government agency for strategic reasons, such as mitigation of penalties. However, a company must consider several practical factors in deciding whether to make a disclosure, including the potential for favourable treatment from the government, the amount of time that has lapsed since the company discovered the potential misconduct, the risk of further or greater government scrutiny and the risk of exposing confidential information.

37 How are internal investigations viewed by local enforcement bodies in your country?

Internal investigations are encouraged by the DOJ and other federal agencies as they help a company to identify potential misconduct and take remedial action. In fact, companies that conduct these investigations and voluntarily disclose wrongdoing may avoid enforcement actions or earn cooperation credit.

Companies are generally free to control the conduct or format of their own internal investigations provided that the investigation is timely, comprehensive and candid, and that the findings and remedial actions of the company are well documented. However, if a company is subject to a subpoena or a parallel governmental investigation, the company would be best advised to conform its internal investigation to the requirements of the subpoena or the government's expectations in an ongoing investigation.

Attorney–client privilege

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Yes. In *Upjohn v. United States*, the US Supreme Court held that communications between all corporate employees and the company's counsel may be protected by the attorney–client privilege. Under this privilege, any confidential communications between a lawyer and a client for the purpose of obtaining or rendering legal advice are protected. However, pursuant to *Upjohn*, lawyers conducting an internal investigation should provide an *Upjohn* warning (see question 34). Moreover, a company in the United States should consider retaining outside counsel to conduct the investigation to minimise the risk of waiving the privilege due to in-house counsel's dual nature as a business and legal adviser.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

The basic elements of the attorney–client privilege are that it concerns a confidential communication between a lawyer and a client for the purpose of obtaining or rendering legal advice. Accordingly, the attorney–client privilege in the United States operates to preclude an opposing party's discovery of a client's confidential communications to a lawyer.

As it relates to corporations, federal law extends the privilege to communications that an attorney receives from a member of the corporation's control group, such as an officer. In *Upjohn*, the US Supreme Court also extended the privilege to employees when the communication:

- concerns a matter within the employee's corporate duties;
- is made at the direction of a corporate superior;
- is made and directed for the purpose of obtaining legal advice for the corporation; and
- is not communicated to others who need not know of its contents.

Because the company is the client, it holds the privilege.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

No. Because of the nature of in-house counsel, an in-house lawyer is subject to stricter requirements to acquire and maintain the attorney–client privilege.

First, an in-house lawyer is only protected if the lawyer's communication involves legal advice, as opposed to business advice. In the case of mixed communications, US federal courts apply a 'predominant purpose' test to determine whether the overall communication is for legal or business advice. Second, an in-house lawyer is only protected if they are actually involved in a matter and the involvement is not illusory. Third, an in-house lawyer is only protected if their communication remains confidential. In the corporate context, a communication remains confidential as long as its disclosure is confined to a group of people that 'need to know' of it.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

Yes. US federal law makes no distinction over the domestic or foreign nature of the lawyer from whom legal advice is sought.

42 To what extent is waiver of the attorney–client privilege regarded as a cooperative step in your country? Are there any contexts where privilege waiver is mandatory or required?

A voluntary waiver of the attorney–client privilege may help in obtaining a more favourable resolution to a government investigation. The Department of Justice's prosecutorial guidelines direct that a company's eligibility for cooperation credit should not be conditioned on a waiver of the attorney–client privilege or work-product protection. Other government agencies, such as the Securities and Exchange Commission, have followed suit. Nevertheless, to receive cooperation credit, government agencies require companies to disclose all facts relevant to the misconduct being investigated. Moreover, in practice, federal agencies may treat a company's willingness to waive privileges as indicative of its willingness to cooperate with the investigation.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

The Federal Rules of Evidence allow a federal court to order that disclosing privileged information in a current litigation does not waive the privilege in that case or any other federal or state proceeding. These Rules also provide that any agreement between parties on the effect of a disclosure in a federal case is binding only on those parties unless it is included in a court order.

However, federal agencies have increasingly defined cooperation with an investigation as a way that a party may require or risk full waiver of the attorney–client privilege or the work-product doctrine. Despite ceasing to require companies to waive their privilege for them to obtain cooperation credit in a pending investigation, federal agencies continue to require that companies disclose all facts relevant to the potential misconduct. And because these facts are often recorded in privileged material created from an internal investigation, a company may be required to disclose privileged material.

In this context, a company must take great care in disclosing privileged information to the government in a way that does not waive protection, or should seek an agreement or court order to maintain the privilege despite the disclosure. Failure to do so may result in a court finding that previously privileged material is no longer protected.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Federal Rule of Evidence 502(c) states that if privileged information is disclosed in a state proceeding without a state court order on waiver, the disclosure does not waive the privilege in a federal proceeding if it either would not be considered a waiver under federal rules or is not a waiver under the laws of the state where it occurred. However, it is unclear whether this Rule applies to disclosures made in other countries.

Federal courts tend to apply the law that is most protective of the attorney–client privilege and work product. Thus, if privilege has been waived on a limited basis in another country, a federal court may find that the waiver remains limited in the United States, which is a separate sovereign.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

In the United States, the common interest privilege protects communications between one group of clients and their counsel and another group of clients and their own counsel to encourage honest communication between negotiating parties.

The common interest privilege requires the same elements of the attorney–client privilege. However, the common interest privilege also requires the existence of a 'common' interest between the communicating parties. US courts vary on what constitutes a sufficiently common interest, with some holding that the parties must have identical interests, while others hold that the parties may even have some adverse interests.

The common interest privilege also requires that each separate communicating client group be represented by its own counsel. Thus, if a represented client group communicates with an unrepresented client group, that unrepresented client group constitutes a third party and the privilege is waived in their communications. Similarly, most US courts require that only each group's lawyers communicate with each other.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

Yes, especially if the third parties could benefit or facilitate attorney–client communications. Courts vary on whether communications made in the presence of the lawyer's employees or staff is privileged, but the ultimate decision tends to rest on the circumstances of the communication and whether the communication is intended to be confidential.

Witness interviews

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

Yes, provided that the lawyers conducting a witness interview of an employee provide an *Upjohn* warning (see question 34).

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

The lawyer conducting the interview should provide an *Upjohn* warning prior to the interview so the company's attorney–client privilege is maintained. This warning also serves to comply with the applicable rules of professional conduct, which normally require US lawyers to disclose their role as corporate counsel if the witness's interests may be adverse to the company or if the witness is mistaken as to the lawyer's role. Similarly, the *Upjohn* warning also helps to avoid a potential conflict of interest as an interviewing lawyer may inadvertently create an implied attorney–client relationship with the witness if the witness reasonably believes the lawyer represents the witness.

To protect the company's privilege, the company and its counsel should take steps to maintain the confidentiality of interviews, as well as ensuring that witnesses do not disclose the contents of the interviews to third parties. To protect the witness, the company and its counsel should also inform the witness that the interview is confidential and whether the company intends to disclose its contents to a third party.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Generally, the internal interview process begins with a notice to the witness that should include a reminder that the matter is confidential. Once the interview begins, the lawyer or agent of the lawyer conducting the interview should give the witness the *Upjohn* warning. Once the witness confirms that they understand the warning, the interview may proceed.

During the interview, the interviewer may ask the witness questions and show evidence to the witness. To reduce the risk of inadvertent waiver of a privilege, evidence provided to witnesses should be limited to evidence that the witness has accessed in the ordinary course of their duties. As the interview ends, the interviewer should ask the witness if they would like any clarification on discussed matters and whether the witness would like to add any further information or clarification. The interviewer should conclude the interview with a reminder to the witness of the interview's confidentiality and a request for the witness to provide further information should they recall relevant information after the interview. Afterwards, the interviewer should memorialise the contents of the interview in a separate document to ensure protection under the attorney–client privilege and the work-product doctrine.

An employee witness is not required to have their own counsel present during an interview, although a witness may request to have counsel present.

Reporting to the authorities

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

US law does not generally require disclosures of corporate misconduct to law enforcement authorities. Nevertheless, some mandatory disclosure obligations do originate from certain statutes or regulations, such as:

- the Sarbanes-Oxley Act of 2002, which requires disclosure of all information with a material financial impact on a public company with periodic financial reports;
- the Bank Secrecy Act of 1970, which requires financial institutions to disclose suspicious transactions; and
- state-level laws requiring companies to disclose data breaches of individuals' personal information.

Additionally, government agencies encourage companies and individuals to voluntarily disclose misconduct in exchange for cooperation credit when pursuing enforcement actions. For example, on 14 April 2024, the Department of Justice (DOJ) launched a pilot programme for voluntary self-disclosures by individuals involved in corporate misconduct. This programme allows individuals to receive a non-prosecution agreement from the government in exchange for self-disclosing, freely cooperating with law enforcement and paying any applicable penalty to disgorge the profits of the misconduct.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Self-reporting to law enforcement is generally recommended, as it can result in reduced fines and a more favourable overall resolution. Based on the DOJ's 'Principles of Federal Prosecution of Business Organizations', a company's willingness to self-disclose, cooperate and remedy misconduct can carry significant weight with law enforcement's choices on whether to prosecute a company. If a company is forced to self-report in a foreign jurisdiction, it should consider also reporting the misconduct to US authorities to prevent duplicative enforcement actions or because foreign authorities will likely share incriminating information with US authorities.

However, it may be premature to self-report if: the evidence of misconduct is not concrete or is based on speculation; protections such as privilege apply; the misconduct is isolated and does not significantly violate US laws or regulations; or there is a lack of clear guidance on how the authorities might react.

53 What are the practical steps needed to self-report to law enforcement in your country?

The DOJ generally awards the greatest amount of cooperation credit for self-reporting if a company takes the following actions:

- discloses all facts relevant to the wrongdoing at issue in a timely manner;
- attributes facts to specific sources, rather than a general narrative;
- proactively, rather than reactively, cooperates with the authorities;
- identifies all individuals involved in or responsible for the misconduct at issue;
- voluntarily preserves, collects and discloses relevant documents and information in a timely manner;
- deconflicts witness interviews and other investigative steps that a corporation takes as part of its internal investigation; and
- makes corporate officers and employees who possess relevant information available for interviews by the authorities.

Other government agencies follow similar approaches towards granting cooperation credit.

Responding to the authorities

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Upon receiving a notice or subpoena, a company should identify and preserve any possible responsive documents. The company should review all collected information, separate out privileged information and submit all collected non-privileged information to the requesting authorities in compliance with the subpoena's requirements. If the company has questions or concerns about the scope of the subpoena, it can discuss these with the issuing authority before or after criminal charges are brought.

The company may choose to resist the notice or subpoena by serving written objections, moving to quash or modify the notice or subpoena or moving for an order protecting confidential, proprietary or private information. The company may also consider contacting the party whose interests are adverse to the issuer of the notice or subpoena so that the other party can oppose the subpoena.

55 Are ongoing authority investigations subject to challenge before the courts?

Yes. If a company believes government authorities are overstepping their boundaries, it may turn to the courts to seek relief. For instance, the company may seek a protective order limiting the availability or disclosure of evidence sought by a subpoena or similar request. The company moving for a protective order must show that the requested disclosure would be unduly annoying, embarrassing, burdensome, expensive or oppressive.

Similarly, the company may move to quash a subpoena when it can show that the subpoena does not allow the company enough time to comply; requires uncompensated travel beyond a certain permitted distance; requires the disclosure of privileged or confidential information; or is otherwise an undue burden to the company.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

A company receiving separate notices or subpoenas should address each one independently to ensure compliance with each requesting authority's requirements, especially if the notices or subpoenas differ.

US law imposes some limits on foreign governments seeking to access US-held information. The Stored Communications Act of 1986 (SCA), for example, blocks foreign government access to US-held stored communications. Specifically, it protects the privacy of stored electronic communications, as well as any other records service providers maintain about their subscribers. Communication providers therefore cannot comply with production orders from other countries if the order seeks communication data located in the United States or held by a US company. Thus, foreign authorities would have a more limited reach when it comes to a company's US-held information.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for and produce material in other countries to satisfy the request? What are the difficulties in that regard?

The recipient of a notice or subpoena in the United States is required to produce all responsive documents within its possession, custody or control. There is no exception for documents located outside the United States, and courts have routinely compelled recipients of subpoenas to produce documents held in other countries. Accordingly, if a subpoena seeks a document located in another country, and that document is within the subpoena recipient's possession, custody or control, the recipient must produce that document.

Some difficulties in complying with a subpoena that seeks material located abroad include the possibility that producing documents held in a foreign jurisdiction may be illegal under that jurisdiction's laws. Despite this possibility, US federal courts tend not to make exceptions and still require disclosure.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for cooperation with foreign authorities?

To avoid the slow and unreliable diplomatic process under letters rogatory, the United States has established a framework of mutual legal assistance treaties (MLATs) between it and other countries. Each treaty has the force of law and defines the countries' obligation to provide assistance, the scope of the assistance and the contents of a request under the treaty. Because each treaty is unique to a particular country, each one contains different standards and requirements. In addition to MLATs, some extradition treaties and tax treaties also contain mutual legal assistance provisions.

Additionally, 18 USC Section 3512, often referred to as the Foreign Evidence Request Efficiency Act, provides a legal framework for US federal courts to assist in gathering evidence for use in foreign criminal proceedings. Under this statute, US district courts have the authority to issue orders necessary to execute requests from foreign authorities. This can include orders to compel testimony, produce documents or conduct searches and seizures.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

To comply with the US Privacy Act, federal law enforcement should not disseminate personal information and must take precautions to keep that information confidential. The Privacy Act, however, does not protect information acquired from 'non-record' sources, such as observation, emails and the rumour mill.

Also, privileged material disclosed pursuant to a subpoena remains protected and cannot be disclosed by law enforcement authorities in most circumstances. The disclosing party must contact the recipient and notify it of the claim of privilege or protection, as well as the basis for that claim. The recipient, after being notified, must take steps to promptly return, sequester or destroy the information and its copies, and may not disclose or use the information until the claim of privilege is resolved. If the recipient disclosed the information prior to being notified, it must take reasonable steps to retrieve it and promptly present it under seal to the court.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

Generally speaking, a company in this situation should first identify if the solicited documents or information even exist, and whether their mere possession under foreign law requires their immediate destruction such that the evidence no longer exists and can no longer be compelled. Otherwise, a company may file written objections to the subpoena or move to quash or modify the subpoena. Courts have held that violation of a foreign law is an insufficient reason for failing to comply with an otherwise valid subpoena issued by a US court. This leaves the party receiving a subpoena requesting a foreign document with a difficult choice between facing contempt of court or other sanctions for failing to comply with the subpoena, or facing penalties in a foreign jurisdiction for illegally producing a document.

US courts consider several factors when deciding whether to compel compliance with a subpoena for documents located abroad. These factors include the importance of the documents to the investigation or litigation, the specificity of the request, whether the information originated in the United States, the availability of alternative ways to obtain the information and whether non-compliance would harm US interests or compliance would harm the interests of the country in which the information is located.

In this context, US courts often require the recipient of the subpoena to make a good-faith effort to obtain permission from the foreign authorities to disclose the document. If the recipient fails to produce the requested document despite a good-faith effort to obtain permission, courts will generally not impose sanctions or other penalties.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

US law may establish limits on foreign governments seeking to access US-held information. The SCA, for example, blocks foreign government access to US-held stored communications. Communication providers therefore cannot comply with production orders from other countries if the order seeks communication content data located in the United States or held by a US company. Likewise, warrants issued pursuant to the SCA can only reach communications located in the United States.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Confidentiality generally attaches to compelled disclosures as long as the disclosing party makes a claim of privilege. Similarly, companies may request that their information remains confidential under the Freedom of Information Act. However, companies should assume that all information provided to the government will likely become public and discoverable at some point. Once made public, third parties may freely discover the information. Accordingly, companies seeking to protect particularly sensitive information should attempt to obtain a protective order or a confidentiality agreement with the government to minimise the risk of future disclosure.

Prosecution and penalties

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Companies and their directors, officers or employees may face significant penalties in the form of fines, disgorgement, restitution, forfeiture and suspension or debarment. Individuals may also be subject to prison time depending on the nature of the misconduct. Companies and individuals involved in corporate misconduct may also be exposed to civil liability in addition to governmental fines and criminal penalties.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Suspension or debarment results in a company temporarily losing the right to conduct business with the federal government and government contractors. While there is no restriction for a company facing suspension or debarment to relocate to another country, the company's name will remain published as

ineligible on the US General Services Administration's System for Award Management website. Also, the company's ties to other entities doing business with the federal government will be closely scrutinised and could be impaired, even if the company moves abroad.

A company seeking to move abroad when there is a risk of suspension, debarment or other restrictions should attempt to voluntarily self-disclose its potential misconduct, or settle or otherwise resolve its issues with US authorities prior to relocating. Failing to do so could result in US authorities sharing information with foreign authorities or the foreign authorities' independent discovery of the company's misconduct. This could lead to negative legal consequences in the country to which the company wishes to relocate.

65 What do the authorities in your country take into account when fixing penalties?

At the federal level, courts determine criminal penalties based on the Federal Sentencing Guidelines, which are non-binding rules established by the US Sentencing Commission in an attempt to unify sentencing policy and calibrate sentences depending upon factors relating both to the subjective guilt of the defendant and to the actual harm caused by the crime. While the Guidelines are not mandatory, federal judges must consider them when deciding a criminal defendant's sentence. Accordingly, when a judge determines within their discretion to depart from the Guidelines, they must explain what factors warranted the increased or decreased sentence.

According to an April 2024 report by Good Jobs First, penalties for corporate misconduct in the United States have been rapidly increasing from approximately US$7 billion per year in the 2000s to more than US$50 billion per year in the 2020s, constituting a 300 per cent increase when adjusted for inflation. Toxic securities, mortgage abuses and the opioid crisis have seen the most penalties by far, followed by price-fixing, emissions cheating, sanctions violations and foreign bribery.

Resolution and settlements short of trial

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Formal and informal non-prosecution agreements (NPAs) and deferred prosecution agreements (DPAs) exist in the United States. In exchange for the government's agreement not to prosecute, or to delay prosecution, both NPAs and DPAs generally require companies to undertake a number of measures, including disgorging funds, paying a penalty, waiving a statute of limitations, cooperating with government actions, admitting to the relevant facts and initiating remedial efforts (which sometimes includes a corporate compliance monitor).

In the case of NPAs, which are not filed in court, the government agrees not to criminally charge a company. If a company breaches the terms of an NPA, the prosecutor may charge the company and initiate prosecution as normal. Under a DPA, the government files a charging document with the court and simultaneously requests that the prosecution be postponed for the purpose of allowing the target of the investigation to demonstrate good conduct. If the defendant complies with the DPA, the government moves to dismiss the criminal charges or civil enforcement action.

In general, NPAs and DPAs are frequently used in the United States, with their use increasing in proportion to the rise in enforcement actions against corporations. These agreements are advantageous because they are more efficient than litigation, offer the parties greater flexibility in resolving complex issues and are generally preferred by corporations over criminal prosecution, which can potentially lead to a company's downfall. However, these agreements are also criticised for being too lenient on criminal behaviour.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

NPAs are not public unless the prosecutor wishes to make the results of the investigation public or the company subject to the NPA is required to disclose the agreement. On the other hand, DPAs are filed with a court so they are usually public and do not provide a company with anonymity. Nevertheless, prosecutors tend to acknowledge that reports generated during the term of an NPA or DPA will likely include confidential business information, public disclosure of which could discourage the company from cooperating with the government.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Settling with a law enforcement agency will usually result in a public announcement of the settlement and its terms. Moreover, while a company may settle with US authorities, its misconduct may extend beyond the borders of the United States. Accordingly, as a result of the settlement with the federal government, foreign authorities may discover the company's misconduct and seek to prosecute the company independently. State governments and private parties are not bound by a settlement, which may expose the company to further legal actions. Furthermore, a settlement is often not without consequences for the company or its officers, and it may still result in significant penalties, including fines, suspension and debarment.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

US authorities often rely on corporate compliance monitorship to ensure compliance with government requirements. Companies entering into NPAs, DPAs and other settlement agreements have increasingly been required to incorporate an external compliance monitor to oversee their probationary period. While originally used primarily by the Securities and Exchange Commission and the Department of Justice, many other government agencies have adopted the use of compliance monitors, including the Federal Trade Commission, the Environmental Protection Agency and the Food and Drug Administration.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Parallel actions are generally allowed in the United States, and civil cases are often filed and carried out simultaneously with the government's criminal prosecution of the same defendant. However, criminal cases usually take priority over parallel civil cases, and a court may order a stay of the parallel civil case if necessary.

Private plaintiffs may not gain access to the authorities' files directly, but they may gain access to some materials indirectly by using subpoenas against the defendant company, looking through the public docket of the criminal case or filing a freedom of information request with the government.

Publicity and reputational issues

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

At the investigatory stage, publicity of the criminal case may be limited as a matter occurring before a grand jury. The unauthorised disclosure of grand jury information may be punished pursuant to a district court's contempt powers. If an individual discloses grand jury material with the intent to obstruct an ongoing investigation, they may be prosecuted for obstruction of justice. In addition, an individual who improperly disseminates grand jury materials may be prosecuted for the theft of government property.

Once a case is before a court, proceedings are generally public. However, certain court filings that include confidential information must be redacted or made under seal. Also, lawyers on both sides of the case must generally refrain from commenting on the case in a manner likely to prejudice the proceeding. A district court may partially limit the public's access to the case if the court determines that a party is likely to suffer irreparable injury if access to the proceedings is not limited.

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

US companies often use public relations firms to address corporate crises. However, it is advisable for a company to have its legal counsel review and approve its communications prior to publication to ensure it complies with applicable law and does not expose itself to potential civil or criminal liability. A company should also put in place strict communication guidelines to ensure communications limit potential liability as much as possible.

73 How is publicity managed when there are ongoing related proceedings?

The same restrictions outlined above with respect to publicity of criminal cases apply. Accordingly, publicity of the case should be kept to a minimum when there is an ongoing legal proceeding against the company or its members. If there is a need for publicity, the company's legal counsel should review and approve all communications to ensure compliance with court and ethics rules.

Duty to the market

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

US law generally does not require that a company disclose settlements. However, the securities laws may require disclosure for certain issuers when the settlement is material to investors and could influence their decisions or it could impact the company's financial condition or operating results.

Environmental, social and corporate governance

75 Does your country regulate environmental, social and governance matters?

On 6 March 2024, the Securities and Exchange Commission (SEC) published the Enhancement and Standardization of Climate-Related Disclosures for Investors rule, requiring certain companies to disclose climate-related information, including their greenhouse gas emissions and other climate risks. However, as a result of multiple parties challenging the SEC's authority to issue the rule in the Fifth Circuit, the SEC issued an order staying the rule on 4 April 2024 until completion of litigation in the federal courts.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address environmental, social and governance matters?

Given that the SEC's rule containing certain regulations concerning environmental, social and governance (ESG) was challenged in court almost immediately after its publication, it is unlikely that any key regulatory or legislative changes relating to ESG will emerge in the next year or so. Promoters of ESG-related regulation will likely closely monitor the outcome of the case disputing the SEC's new rule before attempting to introduce any further ESG regulations to avoid duplicative litigation.

77 Has there been an increase in related litigation, investigations or enforcement activity in recent years in your country?

The increased global focus on ESG matters has naturally led to litigation against companies that fell short of their sustainability commitments or that misled investors and other stakeholders in this regard. For instance, the SEC has brought several high-profile enforcement actions against corporate entities such as Vale SA, BNY Mellon Investment Adviser and DWS Investment Management Americas, Inc, for ESG-related violations, including making false and misleading statements to their investors.

Anticipated developments

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

On 1 January 2024, the Corporate Transparency Act (CTA) came into effect. As a result, by 1 January 2025 companies created or doing business in the United States are expected to file a report with the US Department of the Treasury's Financial Crimes Enforcement Network identifying and setting out specified information about their beneficial owners. The complex nature of the CTA's requirements and the sensitive information it requires will likely lead to legal challenges and further regulatory or legislative changes in the near future.

On 17 June 2024, the Internal Revenue Service (IRS) announced a tax regulation initiative to close a loophole utilised by large partnerships called 'partnership basis shifting transactions'. The IRS's proposed rules under this initiative would prevent large partnerships from abusing their relationships with related business entities to maximise tax deductions and minimise their taxable income.

Finally, because transnational criminal organisations are increasingly finding willing participants in the corporate world, especially within financial institutions, greater emphasis is likely to be placed on legislation and enforcement to curb this misconduct.

Acknowledgements

The authors wish to thank Isabela Hernández-Peredo and Gabor Gazso von Klingspor for their contributions to the chapter.

Michael Diaz, Jr

Global Managing Partner
Diaz Reus International Law Firm
mdiaz@diazreus.com

View full biography

Javier D Coronado Diaz

Partner
Diaz Reus International Law Firm
jcoronado@diazreus.com

View full biography