GIR Global Investigations Review

The Practitioner's Guide to Global Investigations - Eleventh Edition

United States: sanctions, whistleblowers and AI drive corporate investigations agenda

The Practitioner's Guide to Global Investigations - Eleventh Edition

GIR publishes the eleventh edition of its practical guide for external and in-house counsel, compliance officers and accounting practitioners. All chapters are authored by leading practitioners from around the world and are available free to GIR's readers to view and download.

The chapters in Part I provide in-depth coverage of the broad spectrum of law, practice and procedure applicable to investigations in the United Kingdom and United States.

Part II opens with an overview of emerging trends in corporate investigations across the Asia-Pacific region. Local experts from major jurisdictions across the globe then respond to a common and comprehensive set of questions designed to identify the local nuances of law and practice that practitioners may encounter in responding to a cross-border investigation.

Generated: November 13, 2026

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2026 Law Business Research



Explore on **GIR**

United States: sanctions, whistleblowers and AI drive corporate investigations agenda

Michael Diaz Jr, **Javier D Coronado Diaz** and **Isabela Hernández-Peredo**
Diaz Reus International Law Firm

Summary

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS
CYBER-RELATED ISSUES
CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES
ECONOMIC SANCTIONS ENFORCEMENT
BEFORE AN INTERNAL INVESTIGATION
INFORMATION GATHERING
DAWN RAIDS AND SEARCH WARRANTS
WHISTLEBLOWING AND EMPLOYEE RIGHTS
COMMENCING AN INTERNAL INVESTIGATION
ATTORNEY–CLIENT PRIVILEGE
WITNESS INTERVIEWS
REPORTING TO THE AUTHORITIES
RESPONDING TO THE AUTHORITIES
PROSECUTION AND PENALTIES
RESOLUTION AND SETTLEMENTS SHORT OF TRIAL
PUBLICITY AND REPUTATIONAL ISSUES

DUTY TO THE MARKET

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE

ANTICIPATED DEVELOPMENTS

ACKNOWLEDGEMENTS

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.

Among the highest-profile corporate investigations under way in the United States are matters involving companies and intermediaries that allegedly helped the former Maduro regime and Cuban state entities trade Venezuelan oil and evade US sanctions. US authorities are examining shell companies, opaque payment structures, falsely registered or "shadow fleet" vessels and other mechanisms designed to conceal the origin, ownership or destination of oil and related funds. These investigations have assumed even greater prominence following the arrest and prosecution in the United States of Nicolás Maduro and his wife, as well as enforcement actions against Alex Saab and other individuals associated with Maduro.

The investigations are particularly noteworthy because they extend well beyond traditional white-collar sanctions and enforcement investigations. They combine potential sanctions and export control violations with money laundering, asset forfeiture, corruption and national-security investigations, and US authorities are examining the entire ecosystem through which transactions are structured and executed. This creates substantial compliance and enforcement exposure for companies operating in international energy, shipping and financial markets, particularly where transactions involve opaque beneficial ownership structures, high-risk counterparties or jurisdictions construed as unfriendly to the United States and the national security interest.

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 Department of Justice's (DOJ) "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 PROSECUTE (OR REGULATE) CORPORATIONS? HOW IS JURISDICTION BETWEEN THE AUTHORITIES ALLOCATED? DO THE AUTHORITIES HAVE POLICIES OR PROTOCOLS RELATING TO THE PROSECUTION OF CORPORATIONS?

At the federal level, the primary federal agency responsible for enforcing federal laws, including criminal laws applicable to corporations, is the DOJ, which includes the US Attorney's Office in each federal district.

Various law enforcement agencies may investigate corporations in coordination with the DOJ, 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 Federal Bureau of Investigation (FBI), which investigates a wide range of criminal, counterintelligence and national security matters;
- the Drug Enforcement Administration, which investigates violations of US controlled substances laws;
- the Securities and Exchange Commission (SEC), which, through its Enforcement Division, investigates possible violations of federal securities laws and the regulations promulgated thereunder;
- the Federal Trade Commission (FTC), which conducts investigations of potential violations of the FTC Act of 1914, 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 (FinCEN), 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 Customs Enforcement and Customs and Border Protection, investigates crimes relating to cross-border criminal activities that threaten US national security;
- the Office of Foreign Assets Control (OFAC), which administers and enforces economic sanctions against targeted foreign countries, entities and individuals to further US foreign policy and national security; and
- other agencies that investigate financial crime, including the US Secret Service and the Internal Revenue Service's (IRS) Criminal Investigation.

At the federal level, corporations may be subject to regulation by different agencies depending on their industry, business activities and the laws that apply to them. Regulatory bodies include, but are not limited to, the SEC for securities markets and public company disclosures, the Commodity Futures Trading Commission (CFTC) for derivatives, FinCEN and federal banking regulators such as the Office of the Comptroller of the Currency and the Federal Reserve for financial compliance, the FTC for consumer protection and competition, the Consumer Financial Protection Bureau for financial products and services,

the Department of Labor and Occupational Safety and Health Administration (OSHA) for workplace standards and the IRS for tax compliance.

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 or a US member of Congress, or 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 for challenging a notice or subpoena from an authority is very broad and can vary depending on the issuing authority 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 of challenging 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 may result in the disclosure of sensitive or confidential information, a motion for a 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 (NPAs) and deferred prosecution agreements (DPAs). Under these agreements, the DOJ may agree not to 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's:

- agreement not to bring certain criminal charges;
- recommendation or agreement not to oppose the defendant's request that a sentence or sentencing range is appropriate; or
- agreement 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?

According to the DOJ memorandum on 13 August 2026 setting out the National Fraud Enforcement Division's (the Fraud Division) enforcement priorities, the Fraud Division will concentrate its resources on fraud schemes that pose the greatest threats to the health, safety, security and prosperity of US citizens, with particular attention to vulnerable populations. The memorandum identifies five principal areas of focus: public trust and financial integrity, healthcare, internal revenue, global trade and commerce, and corporate misconduct. It also emphasises a more coordinated and data-driven enforcement model, including expanded staffing, greater use of analytics and technology, and closer collaboration with US Attorney's Offices, federal agencies and state and local partners.

Additionally, cases involving significant victim impact, senior-level culpable actors, demonstrable loss, obstruction of justice or links to cartels, terrorist groups, drug money laundering or sanctions evasion receive the highest priority, and prosecutors are directed to seize criminal proceeds and, where authorised, use forfeited assets to compensate victims.

These priorities align with broader US national security efforts. On 20 January 2025, President Trump issued Executive Order (EO) 14157, "Designating Cartels and Other Organizations as Foreign Terrorist Organizations and Specially Designated Global Terrorists". EO 14157 authorises the designation of international cartels and other entities as foreign terrorist organisations (FTOs) and specially designated global terrorists (SDGTs), recognising that they present "an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States", and sets US policy to ensure their total elimination. Since February 2025, the United States has designated eight Mexican cartels, a Central American cartel (Mara Salvatrucha) and two Venezuelan cartels (Tren de Aragua and Cartel de los Soles), and the Brazilian organisations Primeiro Comando da Capital and Commando Vermelho under these authorities.

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 CONSTITUTES 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 its 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. Overall, US authorities expect organisations to develop the following essential and basic 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.

Key US authorities have issued guidance on what constitutes an effective compliance programme, including, but not limited to the following:

- US Sentencing Guidelines §8B2.1, which outline seven core elements of an effective compliance and ethics programme, including risk assessment, policies and procedures, due diligence in delegation of authority, training, monitoring and auditing, enforcement and continuous improvement;
- the DOJ, through its Evaluation of Corporate Compliance Programs and Principles of Federal Prosecution of Business Organizations, provides prosecutors with factors to assess a programme's design, application and effectiveness in practice;
- the Federal Financial Institutions Examination Council publishes manuals and guidance for banks and other financial institutions on compliance risk management, including compliance programmes concerning the Bank Secrecy Act of 1970 (BSA) and anti-money laundering (AML); and
- OFAC, through its Framework for OFAC Compliance Commitments, sets out essential components of a sanctions compliance programme, emphasising senior management commitment, risk assessment, internal controls, testing and auditing, and training.

9 WHAT IMPACT IS AI HAVING IN INVESTIGATIONS? DESCRIBE ANY RELEVANT GUIDANCE, REGULATORY EXPECTATIONS AND CASE LAW CONCERNING THE USE OF AI IN INVESTIGATIONS.

In September 2024, the DOJ updated its Evaluation of Corporate Compliance Programs (ECCP) policy document, which requires prosecutors to evaluate whether a company's compliance programme includes safeguards to ensure that its deployment of new technologies, including AI, will not result in "deliberate or reckless misuse" that violates criminal laws or the company's Code of Conduct.

In December 2024, the DOJ published a report in response to Executive Order 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" (EO 14110), addressing the use of AI in the criminal justice system. The report identifies areas where AI can enhance law enforcement efficiency and accuracy, consistent with protections for privacy, civil rights and civil liberties, and recommends best practices for law enforcement agencies, including safeguards and appropriate use limits for AI.

According to the 2024 ECCP, prosecutors may consider management of emerging risks to ensure compliance with applicable law. For example:

- Is the management of risks related to the use of AI and other new technologies integrated into broader enterprise risk management strategies?
-

What is the company's approach to governance regarding the use of new technologies such as AI in its commercial business and in its compliance programme?

- How is the company mitigating the potential for deliberate or reckless misuse of technologies, including by company insiders?
- To the extent that the company uses AI and similar technologies in its business or as part of its compliance programme, are controls in place to monitor and ensure its trustworthiness, reliability and use in compliance with applicable law and the company's code of conduct?
- How is accountability over use of AI monitored and enforced?
- How does the company train its employees on the use of emerging technologies such as AI?

CYBER-RELATED ISSUES

10 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 requirements. The Cybersecurity Information Sharing Act of 2015, currently extended to 30 September 2026, continues to govern the sharing of threat indicators between public and private entities with safeguards for personal information. EO 14028, issued in May 2021, remains a key directive for strengthening federal cybersecurity, enhancing threat information sharing and setting higher security standards for government systems. More recently, EOs 14144 and 14306 expanded federal efforts to secure software supply chains and strengthen vendor oversight.

The US government also continues to work on the implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), with the Cybersecurity and Infrastructure Security Agency (CISA) requiring most covered entities to report qualifying cyber incidents within 72 hours and ransom payments within 24 hours. However, multiple funding lapses have impacted CISA's ability to conduct rulemaking activity for CIRCIA. CISA continues to work on the final rule. The SEC now requires public companies to disclose material cyber incidents and describe risk management and governance practices in annual reports. Other regulators, such as the New York Department of Financial Services and the FTC, have updated their own cybersecurity rules to impose stricter controls and breach notification obligations. Agencies including the DOJ, FBI, FTC, SEC and the Office for Civil Rights investigate and enforce cybersecurity failings, often focusing on inadequate controls, misleading statements and delayed reporting.

11 DOES YOUR COUNTRY PROSECUTE CYBERCRIME? WHAT IS THE APPROACH OF LAW ENFORCEMENT AUTHORITIES IN YOUR COUNTRY TO CYBERCRIME?

Yes. The DOJ prosecutes cybercrime through federal laws such as the Computer Fraud and Abuse Act of 1986, as well as wire fraud laws, bank fraud laws and money laundering laws. In these prosecutions, federal authorities utilise a combination of criminal charges, asset seizures, arrests and economic sanctions, and have targeted prominent ransomware groups and criminal infrastructures in coordinated operations. For example, the United States, along with international partners, recently disrupted the LockBit ransomware enterprise, brought charges against a suspected LockBit developer and dismantled the 911 S5 botnet that

facilitated widespread fraud. The FBI's Internet Crime Complaint Center reported losses exceeding US$20.9 billion in 2025, reflecting sustained growth in cyber-enabled fraud.

Additionally, OFAC has implemented a cyber-related sanctions programme to address the threat to US national security and the US economy caused by the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by, persons located outside of the United States. OFAC has also imposed economic sanctions on a number of individuals and companies for their roles in cyber operations against the United States. The United States' current approach to cybercrime specifically prioritises ransomware, cyber-enabled financial crime and misuse of cryptocurrency and other virtual assets.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

12 DOES LOCAL CRIMINAL LAW HAVE GENERAL EXTRATERRITORIAL EFFECT? TO THE EXTENT THAT EXTRATERRITORIAL EFFECT IS LIMITED TO SPECIFIC OFFENCES, GIVE DETAILS.

US criminal law does not have general extraterritorial effect; it ordinarily applies only to conduct within US territory. However, certain federal statutes extend jurisdiction to conduct abroad, particularly in cases involving terrorism, drug and human trafficking, and foreign corruption. For example, in 2025, President Trump issued EO 14157 authorising the designation of drug cartels as FTOs or SDGTs. Since then, the State Department has designated about 20 cartels and other transnational criminal organisations (TCOs) as FTOs, bringing them within the scope of the extraterritorial "material support" statutes (18 United States Code (USC) sections 2339A to 2339B), which criminalise providing funds, goods or other forms of assistance to FTOs even when relevant conduct occurs outside the United States.

13 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 United States 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 of 1977 (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.

14 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 prevent a corporation from facing criminal exposure in the United States after resolving charges on the same core facts in another country. Under the US "separate sovereigns" doctrine, different jurisdictions – federal, state and foreign – may prosecute the same conduct independently without violating double jeopardy protections. However, in 2018, the DOJ adopted its "anti-piling on" policy, encouraging coordination with other US and foreign authorities to avoid unnecessary and duplicative corporate penalties.

On 5 June 2025, the Head of the DOJ's Criminal Division, Matthew R Galeotti, reaffirmed this policy in a memorandum titled "Guidance on Coordinating Corporate Resolution Penalties in Parallel Criminal, Civil, Regulatory, and Administrative Proceedings". The updated guidance largely echoes the 2018 framework but introduces a significant caveat: coordination may not come at the expense of victim compensation. Galeotti instructed prosecutors to prioritise restitution and other victim recoveries when coordinating with domestic or foreign authorities, even if that limits the extent to which penalties imposed elsewhere are credited against DOJ resolutions. In effect, while the DOJ remains committed to avoiding duplicative penalties through inter-jurisdictional cooperation, corporate defendants must demonstrate proactive, meaningful coordination early in the process and cannot expect penalty offsets that would reduce or eliminate compensation to victims.

15 ARE "GLOBAL" SETTLEMENTS COMMON IN YOUR COUNTRY? WHAT ARE THE PRACTICAL CONSIDERATIONS?

Global settlements are 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.

16 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 US 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 the FCPA, which criminalises the bribery of foreign officials by US persons and companies, as well as foreign companies listed on US exchanges, or under the Foreign Extortion Prevention Act of 2023, which criminalises the demand or acceptance of a bribe by a foreign official from a US person or company. 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. Strategically, foreign persons facing similar crimes in both their home

jurisdiction and the United States may prefer to defend the local proceedings first, thereby delaying extradition to the United States in the hope of a more favourable US enforcement climate with a change of policy or administration in the United States.

ECONOMIC SANCTIONS ENFORCEMENT

17 DESCRIBE YOUR COUNTRY'S SANCTIONS PROGRAMME AND ANY RECENT SANCTIONS IMPOSED BY YOUR JURISDICTION.

The United States administers and enforces economic sanctions primarily through OFAC, a division of the US Department of the Treasury. OFAC sanctions target foreign countries, geographic regions, entities and individuals to advance US foreign policy and national security interests.

Currently, OFAC administers 37 sanctions programmes addressing threats such as hostile foreign governments, transnational crime, human rights abuses, corruption and narcotics trafficking. 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 only certain transactions involving the country as specified by laws enacted by US Congress, EOs and OFAC regulations and guidelines.

Most recently, on 20 January 2025, President Trump issued EO 14157, authorising the designation of cartels and other entities as FTOs. Following this Order, on 20 February 2025, the US Department of State designated eight organisations as FTOs and SDGTs. OFAC implemented these designations by adding or updating entries on the Specially Designated Nationals and Blocked Persons (SDN) List.

All property and interests in property of the FTOs or SDGTs in the United States or under the control of US persons are blocked. US persons are generally prohibited from transacting with the FTOs or SDGTs unless authorised. Non-US persons may also face exposure if they seek to evade US sanctions or if their conduct causes a US person to engage in a prohibited transaction.

18 WHAT IS YOUR COUNTRY'S APPROACH TO SANCTIONS ENFORCEMENT? HAS THERE BEEN AN INCREASE IN SANCTIONS ENFORCEMENT ACTIVITY IN RECENT YEARS, FOR EXAMPLE?

Violations of sanctions – including attempted violations, conspiracies or causing a violation – can lead to both civil and criminal penalties under US law. Foreign entities may also be subject to enforcement if they conspire to violate or cause a violation of OFAC sanctions. Additionally, OFAC can designate foreign persons to its SDN List if they directly or indirectly violate sanctions. There are exceptions in the form of general licences (broad authorisations for certain classes of transactions) and specific licences (which permit a particular prohibited transaction upon OFAC approval), typically when deemed consistent with US foreign policy.

In 2025, the United States sharply reduced the overall volume of financial sanctions while reorienting their focus, easing pressure on Russia, intensifying "maximum pressure" on Iran and increasingly targeting China and transnational criminal networks.

19 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 Mexico, the United Kingdom, Canada and Australia. For example, OFAC and the DOJ cooperate with Mexican counterparts like the Financial Intelligence Unit to coordinate cross-border financial and sanctions enforcement actions.

20 HAS YOUR COUNTRY ENACTED ANY BLOCKING LEGISLATION IN RELATION TO THE SANCTIONS MEASURES OF THIRD COUNTRIES? DESCRIBE HOW SUCH LEGISLATION OPERATES.

No.

21 TO THE EXTENT THAT YOUR COUNTRY HAS ENACTED ANY SANCTIONS BLOCKING LEGISLATION, HOW IS COMPLIANCE ENFORCED BY LOCAL AUTHORITIES IN PRACTICE?

This is not applicable in this jurisdiction.

BEFORE AN INTERNAL INVESTIGATION

22 HOW DO ALLEGATIONS OF MISCONDUCT MOST OFTEN COME TO LIGHT IN COMPANIES IN YOUR COUNTRY?

In the United States, allegations of corporate misconduct typically surface through a combination of pathways:

- *Whistleblowers:* US law, including the Dodd-Frank Act of 2010 and the Sarbanes-Oxley Act of 2002, provides strong anti-retaliation protections and, in certain cases, monetary incentives. This framework was recently reinforced by the DOJ's 12 May 2025 memorandum regarding the Criminal Division's Corporate Whistleblower Awards Pilot Program, which has been expanded to prioritise tips that lead to forfeiture in high-impact areas, including corporate sanctions offences, trade and customs fraud, money laundering linked to international cartels or TCOs, corporate procurement fraud and material support of terrorism.
- *Standard screening processes:* Customer due diligence, vendor vetting and transaction screening under AML, anti-bribery and corruption, and sanctions compliance programmes often flag anomalies that, upon escalation, reveal misconduct, especially in high-risk jurisdictions or involving politically exposed persons.
- *Suspicious activity reports:* In financial institutions, suspicious activity flagged internally and reported to FinCEN under the BSA frequently initiates law enforcement inquiries. Suspicious activity reports can also prompt internal remediation and, in some cases, voluntary disclosure to other agencies.
- *Audits and other reviews:* Risk-based internal audits, independent external audits and targeted compliance reviews – whether internally initiated or regulator-mandated – are key mechanisms for detecting misconduct. These processes can uncover control weaknesses, transactional irregularities or systemic compliance gaps, including in areas such as trade finance, third-party relationships and cryptoasset transactions. Red flags may point to fraud, sanctions breaches or books-and-records violations. Under section 10A of the Securities Exchange Act of 1934, external auditors have specific obligations to report certain illegal acts to the company's board and, if unaddressed, to the SEC. Findings from any of these reviews are typically escalated

to compliance, legal or the board's audit committee for further investigation and remediation.

- *Tax reporting:* Discrepancies in tax filings or disclosures to the IRS may reveal schemes involving transfer pricing manipulation, unreported offshore accounts or fraudulent deductions.
- *Media reports:* Investigative journalism can prompt both regulatory inquiries and internal investigations, particularly when reports link a company to prohibited transactions, sanctioned counterparties or politically exposed persons.
- *Private litigation:* Civil or commercial suits – particularly those filed by former employees, competitors or contractual counterparties – may contain factual allegations that attract the attention of enforcement agencies and lead to parallel criminal or regulatory proceedings.

From a US enforcement perspective, matters surfacing through these channels can escalate rapidly, especially when accompanied by aggravating factors such as senior management involvement, cross-border elements or conduct touching on national security priorities (eg, sanctions, export controls or terrorist financing).

INFORMATION GATHERING

23 DOES YOUR COUNTRY HAVE A DATA PROTECTION REGIME?

The United States does not have a comprehensive data protection regime; instead, 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 of 1996 (HIPAA), which establishes national standards to protect sensitive patient health information;
- the Gramm-Leach-Bliley Act of 1999 (GLBA), which establishes data protection standards concerning consumers' personal financial information for financial institutions;
- the Children's Online Privacy Protection Act of 1998, which imposes specific requirements on operators of websites or online services that are directed towards children;
- the Fair Credit Reporting Act of 1970, which regulates the collection, dissemination and use of consumer information;
- the FTC Act, which empowers the FTC to take action against unfair or deceptive practices relating to the privacy and security of personal data; and
- the Electronic Communications Privacy Act of 1986, which contains provisions protecting the privacy of electronic communications.

Several states have also enacted broad privacy laws. For example, California's Consumer Privacy Act of 2018 and Privacy Rights Act of 2020 and Washington's My Health My Data Act of 2023 impose significant requirements for certain types of sensitive data. Other new state laws in Tennessee, Maryland, Delaware, New Jersey, Minnesota, New Hampshire, Iowa and Nebraska also establish consumer rights and business obligations concerning sensitive data.

24 TO THE EXTENT NOT DEALT WITH ABOVE AT QUESTION 10, 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 relating 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.

Additionally, the Department of Health and Human Services' Office for Civil Rights enforces the HIPAA through investigations, corrective action plans and monetary settlements. The SEC enforces its cybersecurity disclosure and controls requirements for public companies. State authorities, including the California Privacy Protection Agency and attorneys general in states with privacy statutes, investigate violations and bring enforcement actions, sometimes coordinating with federal authorities.

25 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 such as the HIPAA and the GLBA, which 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.

The DOJ's 2024 update to its ECCP states that prosecutors will scrutinise whether companies can access and retain business communications, including those on third-party or bring-your-own-device channels, and whether these policies deter the use of channels that cannot be preserved.

26 DOES YOUR COUNTRY REGULATE OR OTHERWISE RESTRICT THE INTERCEPTION OF EMPLOYEES' COMMUNICATIONS? WHAT ARE ITS FEATURES AND HOW IS THE REGIME ENFORCED?

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 attempt 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. Generally, there is no right to privacy in an office or company-issued device.

Enforcement of privacy protections has also come indirectly through securities laws. For example, the SEC brought various "off-channel communications" cases in late 2024 and again in early 2025, resulting in substantial financial penalties for failures to preserve business communications sent on personal devices and unapproved apps. Those cases reinforce that employers subject to SEC regulation must maintain clear policies, obtain

appropriate employee acknowledgments and ensure that any business communications occur on systems that can be supervised and retained.

DAWN RAIDS AND SEARCH WARRANTS

27 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.

28 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 to enable them to 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.

29 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

30 DESCRIBE THE WHISTLEBLOWING FRAMEWORK IN YOUR COUNTRY. WHAT FINANCIAL INCENTIVE SCHEMES, IF ANY, EXIST FOR WHISTLEBLOWERS? WHAT LEGAL PROTECTIONS ARE IN PLACE FOR WHISTLEBLOWERS?

The United States has several federal programmes that incentivise whistleblowers and protect them from retaliation. For example, the DOJ's Criminal Division administers a Corporate Whistleblower Awards Pilot Program to uncover and prosecute corporate crime. Under this programme, whistleblowers may be eligible for an award when they provide original, truthful information about certain types of criminal misconduct that leads to forfeitures exceeding US$1 million in net proceeds. As announced in a memorandum from Matthew R Galeotti, Head of the DOJ's Criminal Division, on 12 May 2025, the programme's scope has been expanded to prioritise tips involving:

- violations by corporations relating to international cartels or TCOs, including money laundering, narcotics and other Controlled Substances Act of 1970 offences;
- violations of federal immigration law;
- corporate conduct involving material support of terrorism;
- corporate sanctions offences;
- trade, tariff and customs fraud; and
- corporate procurement fraud.

The SEC, CFTC, OSHA and FinCEN have also established whistleblower programmes to encourage the reporting of potential misconduct under their purview. Additionally, the AI Whistleblower Protection Act was proposed to provide protections to those developing and deploying AI. The law concerns AI companies' restrictive severance agreements and non-disclosure agreements, which can deter willing current and former employees from making whistleblower disclosures to federal authorities. However, as at the time of writing, it has not yet been enacted. Furthermore, on 1 April 2026, FinCEN published a Notice of Proposed Rulemaking on Whistleblower Incentives and Protections. The proposed Whistleblower Program is intended to encourage tips concerning AML, sanctions and other violations. If a whistleblower qualifies for an award, the proposed rule will provide for an award of 10% to 30% of collected monetary sanctions, with a maximum award presumption if 30% of the collected monetary sanctions is, in aggregate, US$15 million or less.

31 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 federal laws such as the Sarbanes-Oxley Act and the Dodd-Frank Act. 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.

Additionally, union-represented employees have the right to request representation during interviews that may lead to disciplinary proceedings. These protections generally apply regardless of whether the individual is an officer, director or employee. Distinctions arise more from the individual's fiduciary duties or corporate governance requirements rather than from employment law itself.

32 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 OR SHOULD TAKE WHEN AN EMPLOYEE IS IMPLICATED IN OR SUSPECTED OF MISCONDUCT, SUCH AS SUSPENSION OR IN RELATION TO COMPENSATION?

Unless whistleblower or anti-retaliation protections are implicated under federal law, a company may freely impose disciplinary measures on an employee involved in misconduct, such as suspension, termination, demotion, a 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, companies may be required to act upon learning of an employee's misconduct to prevent negative legal consequences. For instance, if a company fails to suspend an employee who is under investigation for serious misconduct, it could be exposed to legal actions for breach of fiduciary duties. Companies should take steps that protect the workplace and the integrity of the investigation, which can include placing an employee on short-term leave when their access or presence poses a risk, conducting documented interviews, implementing clear evidence-handling protocols and applying rules consistently.

33 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. However, companies must account for anti-retaliation laws in situations where the employee's refusal is tied to protected activity or legal rights, and companies should apply consistent processes that align with written policies to reduce the risk of claims of wrongful termination or interference with whistleblowing being raised.

COMMENCING AN INTERNAL INVESTIGATION

34 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 identifies 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.

35 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 REQUIRED TO TAKE OR SHOULD CONSIDER TAKING?

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 conduct an internal investigation, it should ensure that the process complies with the requirements established in ***Upjohn v United States*** to preserve the protections of the attorney–client privilege and the work-product doctrine. Pursuant to ***Upjohn***, a lawyer must disclose their role as corporate counsel to witnesses, particularly if the interests of the witness may diverge from those of the company or if there is any misunderstanding about whom the lawyer represents. 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.

36 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. It should then 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 any privileged information and submit all collected non-privileged information to the requesting authorities in compliance with the subpoena's requirements.

37 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 SEC'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 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.

38 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, it 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

39 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 35). 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.

40 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.

41 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 their 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.

42 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.

43 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 DOJ'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 SEC, have followed suit. Nevertheless, to receive cooperation credit, government agencies require companies to disclose all facts relevant to the misconduct being investigated. In practice, federal agencies may treat a company's willingness to waive privileges as indicative of its willingness to cooperate with the investigation.

44 DOES THE CONCEPT OF LIMITED WAIVER OF PRIVILEGE EXIST 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 in which 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.

45 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 in which 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.

46 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.

47 CAN PRIVILEGE BE CLAIMED OVER COMMUNICATIONS WITH THIRD PARTIES?

Yes, especially if the third parties could benefit from or facilitate attorney–client communications. Courts vary on whether communications made in the presence of the lawyer's employees or staff are 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

48 DOES YOUR COUNTRY PERMIT THE INTERVIEWING OF WITNESSES AS PART OF AN INTERNAL INVESTIGATION?

Yes.

49 CAN A COMPANY CLAIM THE ATTORNEY–CLIENT PRIVILEGE OVER INTERNAL WITNESS INTERVIEWS OR ATTORNEY REPORTS?

Yes, if the lawyers conducting a witness interview of an employee provide an ***Upjohn*** warning (see question 35).

50 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's 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 them.

To protect the company's privilege, the company and its counsel should take steps to maintain the confidentiality of interviews and ensure 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 them that the interview is confidential and whether or not the company intends to disclose its contents to a third party.

51 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 them evidence. To reduce the risk of inadvertent waiver of a privilege, evidence provided to witnesses should be limited to materials that they have 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 they 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 they may request this.

REPORTING TO THE AUTHORITIES

52 ARE THERE CIRCUMSTANCES UNDER WHICH REPORTING MISCONDUCT TO LAW ENFORCEMENT AUTHORITIES IS MANDATORY IN YOUR COUNTRY?

US law does not generally require disclosure 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, which requires disclosure of all information with a material financial impact on a public company in periodic financial reports;
- the BSA, 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 10 March 2026, the DOJ released its first-ever department-wide Corporate Enforcement Policy for criminal matters, which supersedes the Enforcement Policy for Business Organizations and promotes uniformity, predictability and fairness in how

the DOJ pursues white-collar cases to protect US citizens. For companies that voluntarily self-disclose, in the absence of certain limited aggravating circumstances, the DOJ will decline to prosecute them. Incentivising corporate self-disclosure – while still permitting prosecutions in appropriate circumstances – allows the DOJ to quickly pursue culpable individuals, secure justice for victims and deter white-collar crime, all while not unduly burdening US businesses.

53 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. 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.

54 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

55 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 any 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.

56 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.

57 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. Therefore, communication providers cannot comply with production orders from other countries if those orders seek 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.

58 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.

59 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 an MLAT framework 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 of 2009, 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.

60 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 of 1974, 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. Upon discovery of disclosure, 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.

61 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, a company in this situation should first identify whether 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 it. 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.

62 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. Therefore, communication providers cannot comply with production orders from other countries if those orders seek 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.

63 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 of 1966. 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

64 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 for misconduct, including criminal fines, disgorgement, restitution and forfeiture. Individuals

may also face imprisonment, depending on the nature of the offence. Civil liability may also arise in addition to governmental fines and criminal sanctions. A corporation convicted of criminal misconduct may be subject to substantial fines, required to forfeit the proceeds of its crimes, disgorge any profits obtained and face significant collateral consequences. These may include suspension or debarment from federal government contracting, cross-debarment by multilateral development banks, and suspension or revocation of export privileges. In certain cases, federal courts may appoint a monitor to oversee the corporation's operations during a term of probation or prohibit the company from operating in the United States for a defined period.

65 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.

66 WHAT DO THE AUTHORITIES IN YOUR COUNTRY CONSIDER 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 decisions. These Guidelines aim to ensure consistency by considering both the subjective guilt of the defendant and 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 October 2025 report by Good Jobs First, penalties for corporate misconduct in the United States have been rapidly increasing, highlighting a cumulative total of more than US$1 trillion in penalties across 700,000 corporate misconduct cases.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

67 ARE NON-PROSECUTION AGREEMENTS OR DEFERRED PROSECUTION AGREEMENTS AVAILABLE IN YOUR JURISDICTION FOR CORPORATIONS?

Formal and informal NPAs and 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.

68 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.

69 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.

70 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 SEC and the DOJ,

many other government agencies have adopted the use of compliance monitors, including the FTC, the Environmental Protection Agency and the Food and Drug Administration.

71 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, although they may gain access to some materials indirectly by using subpoenas against the defendant company, reviewing the public docket of the criminal case or filing a freedom of information request with the government.

PUBLICITY AND REPUTATIONAL ISSUES

72 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.

73 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 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.

74 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

75 IS DISCLOSURE TO THE MARKET MANDATORY IN CIRCUMSTANCES WHERE A SETTLEMENT HAS BEEN AGREED BUT NOT YET MADE PUBLIC?

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

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE

76 DOES YOUR COUNTRY REGULATE OR PROSECUTE ENVIRONMENTAL, SOCIAL AND GOVERNANCE MATTERS?

Yes. The United States regulates environmental, social and governance (ESG) matters through federal securities laws, industry-specific laws and state-level initiatives, and prosecutes ESG-related conduct when it rises to the level of a criminal offence. Criminal prosecution most often occurs under federal environmental laws such as the Clean Air Act of 1970, the Clean Water Act of 1972 and the Resource Conservation and Recovery Act of 1976, where knowing violations can result in felony charges. The DOJ's Environment and Natural Resources Division has recently brought cases involving illegal pollution, hazardous waste violations and falsification of compliance records, with state prosecutors pursuing similar actions under their own environmental laws. ESG-related enforcement is more frequently civil rather than criminal, particularly under disclosure and antifraud provisions.

In 2024, the SEC adopted a climate disclosure rule requiring public companies to report greenhouse gas emissions and climate risks. However, the rule was put on hold the following month due to ongoing litigation. In 2025, the SEC announced that it would no longer defend the rule in court, effectively rendering it inactive while legal proceedings continue, and in 2026, the SEC proposed formally rescinding the rule.

77 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, AND WHAT HAS BEEN THE RESPONSE TO ANY RECENT REGULATORY OR LEGISLATIVE CHANGE?

Significant new federal ESG regulations appear unlikely in the short term, following the SEC's decision not to defend its climate disclosure rule in court in 2025. The SEC has since proposed rescinding the rule. This has left the federal rule inactive while litigation continues, leading to more reliance on state-led initiatives. Notably, California's climate disclosure laws under Senate Bills 253 and 261 are moving through rulemaking, with phased compliance with Senate Bill 253 beginning in 2026. Other states are evaluating similar measures, particularly on greenhouse gas emissions and climate-risk reporting.

However, federal authorities are expected to continue enforcing existing anti-fraud and disclosure provisions, while prosecutors focus their efforts on environmental crimes and regulators pursue civil cases for alleged greenwashing or misstatements. Further, the resolution of court challenges to stock exchange diversity disclosure rules and climate-related mandates will likely influence the direction and timing of any future federal ESG initiatives.

78 HAS THERE BEEN AN INCREASE IN RELATED LITIGATION, INVESTIGATIONS OR ENFORCEMENT ACTIVITY IN RECENT YEARS IN YOUR COUNTRY?

Yes. ESG-related litigation, investigations and enforcement activity have increased in the United States, although the current environment reflects both heightened scrutiny of ESG initiatives and a growing "anti-ESG" backlash. Recent SEC policy shifts – such as withdrawing its defence of the 2024 climate disclosure rule, narrowing shareholder proposal eligibility under Rule 14a-8 (requiring certain proposals in a company's proxy statements) and limiting when investors may rely on Schedule 13G (a simplified ownership report for passive investors) if engaging on ESG topics – signal a less permissive stance towards ESG engagement. Similarly, the DOJ's 12 May 2025 memorandum reprioritised certain white-collar enforcement to cover corporate sanctions and immigration and procurement fraud, potentially increasing ESG-linked governance exposure.

Additionally, state attorneys have intensified inquiries and initiated novel antitrust suits, including a pending case in the Eastern District of Texas that alleges coordinated efforts by major asset managers to reduce coal output. Courts have issued mixed rulings in ESG-related cases:

- in ***Craig v Target Corp***, a securities suit concerning diversity, equity and inclusion disclosures survived dismissal;
- in ***Spence v American Airlines***, the court found a breach of the duty of loyalty under the Employee Retirement Income Security Act of 1974 (ERISA) arising from ESG investing; and
- in ***Utah v Micone***, the court upheld the Department of Labor's ESG-related ERISA rule.

The Delaware Court of Chancery continues to debate whether directors' oversight duties extend beyond legal compliance to business risks, including ESG.

ANTICIPATED DEVELOPMENTS

79 DO YOU EXPECT TO SEE ANY KEY REGULATORY OR LEGISLATIVE CHANGES EMERGE IN THE NEXT YEAR OR SO DESIGNED TO ADDRESS CORPORATE MISCONDUCT OR THAT MAY BE RELEVANT TO THE INVESTIGATION OF ALLEGED CORPORATE MISCONDUCT?

Yes.

The DOJ is expected to implement its new department-wide Corporate Enforcement and Voluntary Self-Disclosure Policy, issued in March 2026. The policy offers a presumption of declination to companies that voluntarily disclose misconduct, fully cooperate and appropriately remediate, subject to limited aggravating circumstances. This is likely to place greater pressure on companies to investigate potential misconduct promptly and make early disclosure decisions.

In parallel, FinCEN and the federal banking agencies have proposed a new AML/countering the financing of terrorism framework focused on effective, risk-based compliance. If finalised, financial institutions would be expected to base their programmes on documented risk assessments, FinCEN's national priorities, and stronger governance, testing and oversight. FinCEN has also proposed rules for the AML whistleblower programme, which could increase internal reporting and government investigations, and new AML, customer-identification, suspicious-activity-reporting and sanctions requirements for payment stablecoin issuers.

Additional guidance and enforcement concerning corporate use of AI is also likely. The FTC is considering a policy statement addressing potentially deceptive representations about the

accuracy and objectivity of AI systems. Companies may therefore face greater scrutiny of claims concerning AI capabilities, training data, testing, accuracy, safeguards and human oversight.

Finally, updated model-risk guidance and interagency statements encourage responsible use of AI, machine learning and advanced analytics in AML compliance. These developments are likely to make technology governance, data quality and validation increasingly important in investigations of alleged corporate misconduct.

ACKNOWLEDGEMENTS

The authors would like to thank Keven Lacayo and Veronica Mayoral, law clerks at Diaz Reus International Law Firm.

Michael Diaz Jr mdiaz@diazreus.com
Javier D Coronado Diaz jcoronado@diazreus.com
Isabela Hernández-Peredo ihernandezperedo@diazreus.com

100 S.E. 2nd Street, Suite #3400, Miami, FL 33131, USA

Tel: +1 305 375 9220

https://diazreus.com/

Read more from this firm on GIR