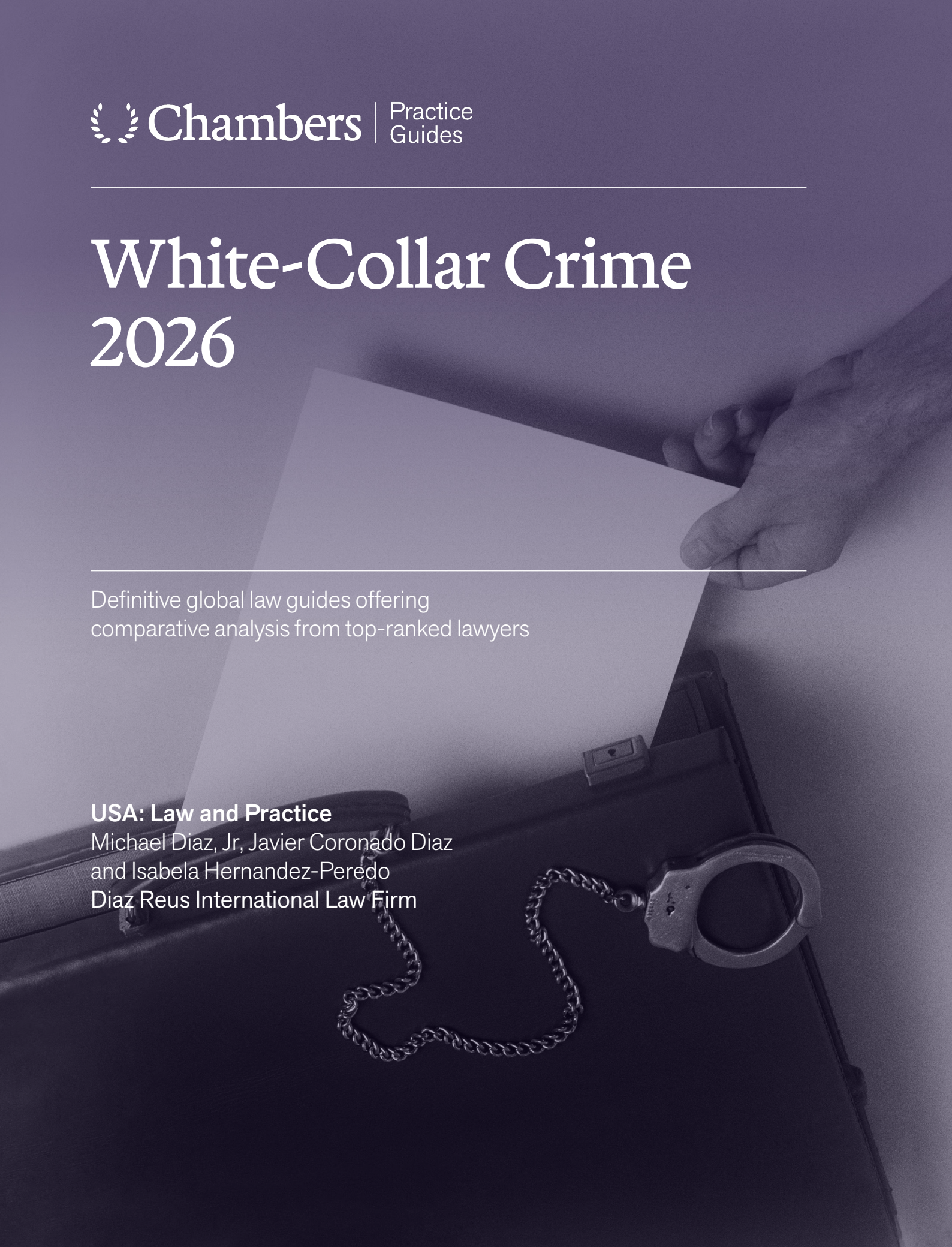
Chambers | Practice Guides

White-Collar Crime 2026

Definitive global law guides offering comparative analysis from top-ranked lawyers



USA: Law and Practice

Michael Diaz, Jr, Javier Coronado Diaz and Isabela Hernandez-Peredo
Diaz Reus International Law Firm

USA



Law and Practice

Contributed by:
Michael Diaz, Jr, Javier Coronado Diaz and Isabela Hernandez-Peredo
Diaz Reus International Law Firm

Contents

1. Criminal Law P.4
1.1 Criminal Offences p.4
1.2 Burden of Proof p.4
1.3 Statute of Limitations p.4
1.4 Extraterritorial Reach and Cross-Border Co-Operation p.5
1.5 Corporate and Personal Liability p.5
1.6 Sentencing and Penalties p.5
1.7 Damages and Compensation p.6

2. Enforcement P.6
2.1 White-Collar Enforcement Authorities p.6
2.2 Initiating an Investigation p.7
2.3 Powers of Investigation p.7
2.4 Use of Technology in Investigations p.7
2.5 Internal Investigations p.8
2.6 Prosecution p.8
2.7 Deferred Prosecution p.9

3. White-Collar Offences P.9
3.1 Criminal Company Law and Corporate Fraud p.9
3.2 Bribery, Influence Peddling and Related Offences p.9
3.3 Anti-Bribery Regulation p.10
3.4 Insider Dealing, Market Abuse and Criminal Banking Law p.10
3.5 Tax Fraud p.11
3.6 Financial Record-Keeping p.11
3.7 Cartels and Criminal Competition Law p.12
3.8 Consumer Criminal Law p.12
3.9 Cybercrimes, Computer Fraud and Protection of Company Secrets p.13
3.10 Financial/Trade/Customs Sanctions p.13
3.11 Concealment p.14
3.12 Aiding and Abetting p.14
3.13 Money Laundering p.14
3.14 ESG-Related Offences p.15
3.15 Artificial Intelligence and Automation Misuse p.15
3.16 Crypto-Assets and Digital Currency Crimes p.15

4. Pleas and Defences P.16
4.1 White-Collar Defences p.16
4.2 De Minimis p.16
4.3 Plea Agreements, Co-Operation, Self-Disclosure and Leniency p.17
4.4 Whistle-Blower Protection p.17
4.5 Cross-Border Defence Strategies p.17

5. Key Trends and Future Outlook P.18
5.1 The Year Ahead p.18

Diaz Reus International Law Firm operates on five continents, across 40 offices in key business centres, offering a global practice centred around national and international trade, finance, parallel proceedings and business transactions. The firm, its founders, and key partners are world-renowned board-certified experts in International Law and International Litigation & Arbitration. Diaz Reus International is a recognised for its work in sensitive criminal matters involving government and foreign corruption investigations, including money laundering, OFAC & trade sanctions, Foreign Sovereign Immunity (FSIA) disputes, and global asset recovery matters, and has been ranked by Chambers in Corporate Crime & Investigations.

Authors



Michael Diaz, Jr is the global managing partner at Diaz Reus. Board certified in international litigation and arbitration and a certified anti-money laundering specialist, he has extensive experience handling federal criminal investigations, visa recovery efforts, FCPA, FARA and OFAC violations, and SDN and blocked-persons classifications cases. He regularly counsels on preventative arbitration and litigation strategies, international trade and exports control including sanctions, and conducts parallel investigations in complex, high-stakes regulatory, investigative and compliance matters that involve alleged white-collar and corruption crimes. Michael's sophisticated asset-tracing techniques have resulted in hundreds of millions of dollars in recoveries for US government agencies, foreign governments and their entities, financial institutions, and individual fraud victims.



Javier Coronado Diaz is a partner at Diaz Reus, and is licensed to practice in Florida, New York, Colombia and before various US federal courts and Government agencies, with certifications in anti-money laundering and global economic sanctions. He represents individuals and corporations in international investigations and litigation, asset recovery, and cases involving white-collar crimes, domestic and foreign corruption, anti-money laundering laws, sanctions, and financial fraud, including investigations and enforcement actions by the DOJ, the OFAC, and the DHS. He also advises clients in business transactions, corporate governance, and entity formation, particularly in securing the client's compliance with international, US and Colombian legal standards, regulations, and best practices.



Isabela Hernandez-Peredo is an associate attorney and is licensed to practice law in New York and Mexico, bringing her legal experience to Diaz Reus' extensive Latin America practice. She regularly represents individuals and corporations in complex cross-border matters, including international litigation, asset recovery, economic sanctions, OFAC compliance, and the design and implementation of corporate compliance programmes. Previously, Isabela practised at one of Mexico's most prestigious law firms, where she advised on strategy development for defending and resolving complex commercial disputes across key economic industries, including infrastructure, finance, energy, environmental, and antitrust. She represented clients in both administrative and judicial proceedings before Mexican courts and regulatory authorities.

Diaz Reus International Law Firm

100 SE 2nd Street
Suite 3400
Miami FL33131
USA

Tel: +1 305 375 9220
Email: mdiaz@diazreus.com
Web: diazreus.com

1. Criminal Law

1.1 Criminal Offences

In the United States, criminal offences are established under both federal and state law and are generally classified as felonies, misdemeanours or petty offences.

Felonies are the most serious category and may include both offences against persons and property-related crimes, including certain white-collar offences. They are generally punishable by more than one year of imprisonment, although penalties may also include fines and other sanctions. Misdemeanours are less serious offences and are generally punishable by no more than one year of imprisonment, together with possible fines, restitution, probation, home confinement or community service.

Depending on the offence, the applicable mens rea may include purpose, knowledge, recklessness or negligence. Certain strict-liability offences, including some regulatory offences, do not require proof of a culpable mental state.

Liability may also attach where the intended offence is not completed. An attempt generally requires proof that the defendant intended to commit the underlying crime and took a substantial step toward its commission that went beyond mere preparation.

1.2 Burden of Proof

In criminal cases, the government bears the burden of proof. The prosecution has to prove beyond a reasonable doubt: (i) a prohibited act or omission; (ii) and the required mental state. The defendant is presumed innocent unless and until that burden is satisfied.

In civil and administrative matters, the plaintiff asserting the claim generally must prove it, most commonly under a preponderance-of-the-evidence standard, although some proceedings apply substantial-evidence standard. A defendant who relies on an affirmative defence typically bears the burden of establishing that defence, usually by a preponderance of the evidence or, in some circumstances, by clear and convincing evidence.

1.3 Statute of Limitations

For most federal criminal offences, the applicable statute of limitations is five years from the date the offence is completed, unless a statute provides a different period. Certain offences are subject to longer periods; for example, specified financial institution offences, including bank fraud and certain mail and wire fraud offences affecting a financial institution, are subject to a ten-year limitation period.

The limitations period generally begins when all elements of the offence have occurred. However, continuing offences are treated differently. In those cases, the period does not begin until the continuing conduct ends. For example, conspiracy is treated as continuing offence; where an overt act is required, the limitations period generally runs from the last overt act in furtherance of the conspiracy.

1.4 Extraterritorial Reach and Cross-Border Co-Operation

US criminal law does not generally have extraterritorial application; it ordinarily applies only to conduct within US territory. However, certain federal statutes expressly or by interpretation reach conduct outside the US, particularly in areas such as 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 specially designated global terrorists (SDGTs). Since then, the State Department has designated about 20 cartels and other 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 US.

Cross-border criminal investigations are supported by an extensive framework of mutual legal assistance treaties (MLATs). Each MLAT defines the participating states' obligations, the available forms of assistance, and the requirements for making a request. However, some countries may not have MLATs with the US, or may interpret the treaties narrowly, limiting the scope of cooperation.

The US also has extradition and tax treaties, which may contain mutual legal assistance provisions. In addition, 18 USC Section 3512 authorises US federal courts to issue orders to execute qualifying requests from foreign authorities, including orders compelling testimony or document production and authorising searches and seizures. However, practical difficulties may arise where foreign law restricts production of documents sought by US authorities.

1.5 Corporate and Personal Liability

A corporation may be criminally liable under applicable federal or state statutes. At the federal level, corporate criminal liability is also governed by the common-law doctrine of respondeat superior. Under that doctrine, a corporation may be liable for the acts of its directors, officers, employees or other agents where the conduct was within the scope of the agent's duties and was intended, at least in part, to benefit the corporation.

Corporations and the individuals responsible for misconduct may both face prosecution. The Department of Justice (DOJ) exercises prosecutorial discretion when determining whether to charge a corporation. Its Principles of Federal Prosecution of Business Organizations identify factors including the nature and seriousness of the offence, pervasiveness of wrongdoing, prior misconduct, voluntary disclosure and co-operation, the adequacy and effectiveness of the compliance programme, remedial measures, collateral consequences, available civil or regulatory remedies, prosecution of responsible individuals and the interests of victims. However, managers and directors are not criminally liable merely because the corporation itself is liable. Their personal liability ordinarily depends on their own conduct and whether the government can establish the elements of the relevant offence.

Additionally, a parent company may be held liable for a subsidiary's misconduct in limited circumstances. Liability may arise where the parent directly participated in, directed, or otherwise exercised sufficient involvement in the wrongful conduct. A parent may also be liable under traditional agency principles where the subsidiary acted as its agent. In assessing agency, the key consideration is control, including the parent's knowledge of and direction over the subsidiary's activities generally and, more importantly, with respect to the specific transaction or misconduct at issue.

Furthermore, in mergers and acquisitions, the successor company generally assumes the predecessor's existing liabilities, including civil and criminal liabilities. This principle prevents companies from avoiding liability through corporate reorganisations and can extend to FCPA violations. At the same time, the DOJ and SEC recognise the benefits of M&A transactions, particularly where the acquiring company has a robust compliance programme and promptly implements it at the acquired entity.

1.6 Sentencing and Penalties

Federal criminal sentences are determined by the court with reference to the US Sentencing Guidelines. Although the Guidelines are advisory rather than mandatory, federal judges must consider them in deter-

mining an appropriate sentence and generally explain any material departure from the applicable Guidelines range. The framework considers matters including the defendant's culpability and the harm resulting from the offence. Corporate and individual defendants may face a variety of consequences. Companies may be subject to criminal fines, restitution, forfeiture and disgorgement, while individuals may also face imprisonment. Corporate convictions can lead to collateral consequences including suspension or debarment from federal contracting, cross-debarment by multilateral development banks, loss of export privileges and, in appropriate cases, court-supervised probation or compliance monitoring. Corporate compliance and remediation are also relevant. US enforcement authorities assess the effectiveness of a company's compliance programme both at the time of the misconduct and when making charging or resolution decisions. Relevant considerations include management commitment, risk assessment, internal controls, testing and auditing, employee training and continuous improvement.

Non-Prosecution Agreements (NPAs) and Deferred Prosecution Agreements (DPAs) are commonly used in the US to resolve corporate investigations without proceeding to a full prosecution. In exchange, companies typically agree to measures such as paying penalties or disgorgement, cooperating with the government, admitting relevant facts, waiving limitation periods and undertaking remediation, sometimes including a compliance monitor.

Under an NPA, the government agrees not to bring charges so long as the company complies with the agreement. Under a DPA, charges are filed but prosecution is deferred; if the company satisfies the agreement, the government seeks dismissal. These mechanisms offer greater efficiency and flexibility than litigation, although they are sometimes criticised as being too lenient.

1.7 Damages and Compensation

Victims of white-collar offences may seek compensation through criminal restitution and through separate civil proceedings. At the federal level, the Mandatory Victims Restitution Act (MVRA) requires restitution for certain offences, including property offences committed by fraud or deceit, where an identifiable victim has suffered direct and proximate harm. Restitution may include the return of property or payment for the value of property lost, as well as certain other losses and expenses attributable to the offence. The Crime Victims' Rights Act also recognises a victim's right to full and timely restitution as provided by law.

Restitution is generally determined by the federal district court as part of sentencing in the underlying criminal case. Depending on the offence, restitution may be mandatory under 18 USC Section 3663A or discretionary under 18 USC Section 3663. Restitution is intended to compensate victims for losses caused by the offence and is distinct from fines, forfeiture and other penalties imposed on the defendant.

Victims may also pursue civil remedies where the underlying conduct gives rise to a private cause of action, such as claims involving fraud, securities violations, breach of fiduciary duty or other applicable federal or state causes of action. Such proceedings may be brought independently of the criminal prosecution, subject to the jurisdictional requirements of the relevant federal or state court.

Class actions are available in appropriate civil cases arising from white-collar misconduct.

2. Enforcement

2.1 White-Collar Enforcement Authorities

At the federal level, the DOJ, acting through the US Attorneys' Offices and specialised components of the DOJ, is the principal authority responsible for prosecuting white-collar crime. Investigations are frequently conducted with other federal law-enforcement agencies whose jurisdiction depends on the nature of the alleged misconduct. These include the Federal Bureau of Investigation (FBI), Internal Revenue Service Criminal Investigation, Homeland Security Investigations and the US Secret Service.

Civil and administrative enforcement may proceed alongside criminal investigations. The Securities and Exchange Commission (SEC) investigates and brings civil enforcement actions involving federal securities

laws; the Commodity Futures Trading Commission (CFTC) regulates derivatives markets; the Federal Trade Commission (FTC) addresses consumer protection and competition matters; and the Financial Crimes Enforcement Network (FinCEN), the Office of Foreign Assets Control (OFAC), federal banking regulators and other agencies exercise specialised regulatory and enforcement powers. Jurisdiction therefore often overlaps, and parallel criminal, civil and administrative proceedings arising from the same conduct are common.

The US does not generally rely on separate criminal courts devoted exclusively to white-collar offences. Such cases are ordinarily heard in the federal district courts, although investigative and prosecutorial agencies maintain specialised units and personnel with expertise in areas such as fraud, corruption, money laundering, sanctions and financial crime.

Enforcement priorities can shift significantly with changes in public policy and presidential administrations. The current DOJ approach places particular emphasis on matters involving public trust and financial integrity, healthcare, tax and revenue offences, global trade and commerce, and corporate misconduct. The DOJ has also indicated that matters involving substantial victim losses, senior-level culpability, obstruction, cartels, terrorist organisations, drug-related money laundering and sanctions evasion will receive heightened attention. Recent policy changes also reflect a greater national-security focus in white-collar enforcement, particularly where financial crime intersects with sanctions, transnational criminal organisations and terrorist financing. This illustrates the extent to which enforcement priorities may be influenced by broader governmental and foreign-policy objectives.

2.2 Initiating an Investigation

White-collar investigations in the US may be initiated when a government agency receives credible information suggesting a violation of federal or state law. Such information may come from victims, witnesses, whistle-blowers or informants, regulatory filings or reports, requests from foreign authorities or members of Congress, or publicly available information. The applicable threshold and procedures depend on the agency involved and the nature of the suspected misconduct. In practice, agencies have broad discretion to open investigations based on credible allegations or other information indicating potential wrongdoing, subject to their statutory authority and internal enforcement policies.

2.3 Powers of Investigation

US investigative authorities have broad powers to obtain information and evidence in white-collar investigations. Subpoenas are commonly used to require companies and third parties to produce documents and other materials, including records within their possession, custody or control. A recipient may challenge a subpoena through a motion to quash or modify, including on grounds such as lack of jurisdiction, privilege, confidentiality or undue burden.

Authorities may also execute search warrants against corporate premises. To obtain a warrant, the government must establish probable cause to believe that a crime has been committed and that evidence will be found at the location identified in the warrant. A valid warrant permits investigators to enter the premises and seize evidence within its scope; evidence obtained through an unlawful search may be subject to exclusion.

Individuals may also be compelled to provide testimony or documents through a grand jury subpoena. The Fifth Amendment protects individuals from being compelled to provide self-incriminating testimony, although the privilege does not apply to corporations in the same manner. State authorities have comparable mechanisms for compelling testimony and document production. Federal authorities also use asset seizure and forfeiture tools in investigations involving digital assets and cryptocurrency.

Additionally, 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.

2.4 Use of Technology in Investigations

US enforcement authorities increasingly use AI, data analytics and other advanced digital tools in white-

collar investigations. In fact, a 13 August 2026 DOJ memorandum setting out the National Fraud Enforcement Division's enforcement explains that the DOJ is building the most sophisticated, innovative and data-driven white-collar law enforcement component in the word, positioned to fight fraud at every level.

There is no specific federal statute governing the use of AI or advance analytics specifically in the white-collar investigations. However, on 3 December 2024, the DOJ responded to Executive Order 14110*Safe*, *Secure*, *and Trustworthy Development and Use of Artificial Intelligence* (EO 14110) in a report 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.

Additionally, the DOJ's September 2024 Evaluation of Corporate Compliance Programs instructs prosecutors to consider how a company identifies and manages risks arising from AI and other new technologies, including whether such risks are integrated into enterprise risk management, which governance structures apply, whether controls exist to ensure the technology's trustworthiness and reliability, how deliberate or reckless misuse is prevented, and how accountability is monitored and enforced.

2.5 Internal Investigations

Internal investigations are not generally mandatory under US law simply because potential misconduct has been identified. However, the DOJ and other federal agencies encourage them as they help to identify potential misconduct and relevant information, to remedy wrongdoing and, where appropriate, to facilitate voluntarily disclosure of misconduct to the government. For example, Under the DOJ's Department-wide Corporate Enforcement and Voluntary Self-Disclosure Policy issued on 10 March 2026, companies that voluntarily self-disclose, fully cooperate with a government investigation and remediate on an appropriate and timely basis can, absent certain aggravating circumstances, avoid prosecution by the DOJ.

While no federal statute regulates companies' internal investigations, relevant guidance includes the DOJ's Principles of Federal Prosecution of Business Organizations, its Evaluation of Corporate Compliance Programs and its Corporate Enforcement and Voluntary Self-Disclosure Policy.

The US has no comprehensive federal data protection law. Internal investigations may therefore be subject to sector-specific federal laws, such as HIPAA and the Gramm-Leach-Bliley Act, state privacy laws, and applicable document-preservation requirements. DOJ guidance also recommends that companies maintain access to and preserve relevant business communications, including those made through personal devices and third-party applications. There is likewise no general federal employment law governing employee rights in internal investigations. However, employees who report suspected misconduct or participate in protected activity may benefit from whistle-blower and anti-retaliation protections under statutes including the Sarbanes-Oxley Act and the Dodd-Frank Act.

Companies are not generally required to disclose the findings of an internal investigation to enforcement authorities. However, voluntary disclosure may provide significant cooperation benefits. Companies seeking cooperation credit are generally expected to disclose relevant non-privileged information.

2.6 Prosecution

White-collar prosecutions may arise from investigations initiated after a government agency receives credible information suggesting a violation of federal or state law. Such information may come from victims, witnesses, informants, suspicious activity reports, foreign governments, members of Congress or publicly available sources. At the federal level, the DOJ, including the US Attorneys' Offices, is the principal authority responsible for prosecuting federal criminal offences, often working with investigative agencies such as the FBI, IRS Criminal Investigation, Homeland Security Investigations and other specialised regulators or enforcement bodies.

Federal prosecutors have substantial discretion in deciding whether to charge a company or an individual. In the corporate context, the DOJ's Principles of

Federal Prosecution of Business Organizations identifies factors prosecutors should consider, including the nature and seriousness of the offence, the pervasiveness of wrongdoing, the company's history of misconduct, voluntary disclosure and cooperation, the effectiveness of its compliance programme, remedial action, collateral consequences, the adequacy of alternative remedies, the prosecution of responsible individuals and the interests of victims.

The DOJ's corporate enforcement policies further influence that discretion. For example, voluntary self-disclosure, full cooperation and timely remediation may materially affect whether the DOJ prosecutes a company and the form of any resolution. Individual charging decisions are likewise discretionary and depend on the available evidence, the applicable offence and general federal prosecutorial principles.

2.7 Deferred Prosecution

A criminal investigation may be resolved through NPAs or DPAs. Under both mechanisms, 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).

3. White-Collar Offences

3.1 Criminal Company Law and Corporate Fraud

Beyond the offences addressed in **3. White-Collar Offences**, corporate and individual defendants may also face liability under the Racketeer Influenced and Corrupt Organizations Act (RICO). RICO applies where a person participates in the conduct of an enterprise through a pattern of qualifying racketeering activity, which may consist of predicate offences such as fraud, bribery or money laundering.

RICO may give rise to both criminal and civil liability. Criminal violations may result in imprisonment of up to 20 years, fines and forfeiture of property connected to the racketeering activity. Civil RICO claims may permit recovery of treble damages and attorneys' fees.

3.2 Bribery, Influence Peddling and Related Offences

Federal law prohibits several forms of bribery and influence peddling involving domestic and foreign public officials. There is no general federal commercial bribery statute applicable to all private-sector conduct, although private bribery may give rise to liability under specific federal statutes, the Travel Act and state law.

- Bribery of federal public officials: Under 18 USC Section 201 (b), it is an offence to corruptly give, offer or promise anything of value to a federal public official, directly or indirectly, with intent to influence an official act, induce fraud against the US or induce the official to violate an official duty. It likewise applies to a federal public official who corruptly demands, seeks, receives, accepts or agrees to accept anything of value in return for such action.
- Bribery involving federally funded programmes – 18 USC Section 666: This provision prohibits corrupt payments to, or demands or acceptance of payments by, agents of certain organisations and state, local or tribal governments that receive federal programme benefits, where the relevant transaction meets the statutory monetary thresholds.
- Bribery of foreign public officials – FCPA: The anti-bribery provisions of the FCPA prohibit covered persons and entities from corruptly offering, pay-

ing, promising or authorising anything of value to a foreign official, foreign political party or candidate for specified improper purposes in order to obtain or retain business or direct business to another person.
- Receipt or demand of foreign bribes – Foreign Extortion Prevention Act (FEPA), 18 USC Section 1352: FEPA addresses the demand side of foreign bribery by making it an offence for certain foreign officials to corruptly demand, seek, receive, accept or agree to receive anything of value in return for exercising official authority, violating an official duty, conferring an improper advantage or using influence over a foreign government in connection with obtaining or retaining business.
- Private-sector bribery: There is no generally applicable federal offence covering all commercial bribery between private parties. However, such conduct may give rise to federal liability where another jurisdictional basis exists, including under the Travel Act where interstate or foreign commerce is used to facilitate bribery prohibited by applicable state law. Federal law also contains sector-specific provisions, such as 18 USC Section 215, which addresses corrupt payments involving officers, directors, employees, agents or attorneys of financial institutions.

3.3 Anti-Bribery Regulation

The US does not impose a general federal obligation on companies to prevent bribery or influence peddling, nor is there a generally applicable offence based solely on a company's failure to maintain an anti-bribery compliance programme.

Federal law does not prescribe a single mandatory anti-bribery compliance programme applicable to all companies; however, the DOJ strongly encourages companies to maintain effective, risk-based compliance programmes.

There is likewise no general federal obligation requiring companies or individuals to report all suspected bribery to law-enforcement authorities. Voluntary self-disclosure is nevertheless strongly encouraged, and can result in substantial benefits under DOJ corporate enforcement policies. Reporting obligations may also arise in particular regulated industries, pursuant to securities or other regulatory requirements, contractual obligations, or the terms of an existing government resolution. Failure merely to report suspected bribery does not ordinarily constitute a separate federal offence.

3.4 Insider Dealing, Market Abuse and Criminal Banking Law

The principal federal offences relating to insider dealing, market abuse and criminal banking law include the following.

- Insider trading – Section 10 (b) of the Securities Exchange Act and Rule 10b-5: Liability generally arises where a person trades securities while aware of material non-public information, in breach of a fiduciary duty or other duty of trust or confidence. Liability may also extend to persons who improperly disclose such information. Wilful violations may result in imprisonment for up to 20 years and fines of up to USD5 million for individuals or USD25 million for entities (15 USC Section 78ff), in addition to civil penalties and disgorgement.
- Securities and commodities fraud – 18 USC Section 1348: This provision applies where a person knowingly executes, or attempts to execute, a scheme to defraud in connection with certain securities or commodities, or to obtain money or property through false or fraudulent pretences in connection with their purchase or sale. Violations are punishable by a fine and imprisonment for up to 25 years.
- Market manipulation – Sections 9 (a) and 10 (b) of the Securities Exchange Act: These provisions prohibit manipulative trading practices intended to create a false or misleading appearance of market activity or artificially affect security prices, including wash trades, matched orders and other deceptive schemes. Wilful violations may result in imprisonment for up to 20 years and fines of up to USD5 million for individuals or USD25 million for entities, as well as civil remedies.
- Bank fraud – 18 USC Section 1344: A person commits bank fraud by knowingly executing, or attempting to execute, a scheme to defraud a financial institution or obtain property under its custody or control by false or fraudulent pretences.

Violations are punishable by a fine of up to USD1 million, imprisonment for up to 30 years, or both.
- Unlicensed money transmission – 18 USC Section 1960: It is an offence knowingly to operate or control a money-transmitting business that lacks a required state licence, fails to satisfy applicable federal registration requirements, or transmits funds known to derive from or promote unlawful activity. Violations are punishable by a fine, imprisonment for up to five years, or both.
- Unauthorised deposit-taking – 12 USC Section 378: Federal law restricts persons and entities from engaging in the business of receiving deposits unless appropriately authorised or regulated. Wilful violations may result in a fine of up to USD5,000, imprisonment for up to five years, or both.

Additional federal and state laws may apply depending on the type of financial activity and the conduct involved.

3.5 Tax Fraud

The principal federal tax offences include the following.

- Tax evasion: Under 26 USC Section 7201, the government must prove a tax deficiency, wilfulness and an affirmative act intended to evade or defeat tax. Penalties include a fine of up to USD100,000 for individuals or USD500,000 for corporations, imprisonment for up to five years, or both.
- False tax returns or statements: Under 26 USC Section 7206 (1), it is an offence wilfully to make and sign, under penalties of perjury, a return or other tax document that the person does not believe to be true and correct as to a material matter. Penalties include imprisonment for up to three years and fines of up to USD100,000 for individuals or USD500,000 for corporations.
- Aiding or assisting false tax filings: Under 26 USC Section 7206 (2), it is an offence wilfully to aid, assist in, procure, counsel or advise the preparation or presentation of a return or other tax document that is fraudulent or false as to a material matter. The same maximum penalties under Section 7206 apply.
- Wilful failure to file, provide information or pay tax: Under 26 USC Section 7203, liability arises where a person who is legally required to file a return, maintain records, provide information or pay tax wilfully fails to do so. The offence is generally punishable by up to one year's imprisonment and a fine.
- Failure to collect or pay over tax: Under 26 USC Section 7202, a person required to collect, account for and pay over tax who wilfully fails to do so may be imprisoned for up to five years and fined.

There is no general federal offence based solely on a company's failure to prevent another person from committing tax evasion. Liability instead arises where the company or individual participates in, aids or assists the offence, or breaches a specific tax obligation.

Federal law also imposes various tax and financial reporting requirements, including tax-return and information-reporting obligations, foreign-account and foreign-asset reporting, and reporting of certain cash transactions. Failure to comply may result in civil penalties and, where the violation is wilful, criminal liability.

3.6 Financial Record-Keeping

Federal law imposes a number of financial record-keeping obligations, particularly on public companies and other issuers of securities. The most relevant requirements arise under the FCPA and federal obstruction statutes.

- FCPA books-and-records and internal-controls requirements: The FCPA requires issuers to keep books, records and accounts that, in reasonable detail, accurately and fairly reflect their transactions and dispositions of assets. It also requires issuers to maintain a system of internal accounting controls designed to provide reasonable assurances that transactions are properly authorised and recorded and that assets are appropriately accounted for (15 USC Sections 78m(b)(2)(A)-(B)). These requirements apply independently of the FCPA's anti-bribery provisions, meaning that a books-and-records or internal-controls violation may exist even where no bribery is established. Criminal liability may arise where a person knowingly circumvents or fails to implement internal accounting controls, or knowingly falsifies the issuer's books, records or accounts. Wilful viola-

tions may result in imprisonment for up to 20 years and fines of up to USD5 million for individuals or USD25 million for entities.
- Destruction or falsification of records: Under 18 USC Section 1519, a person may be liable for knowingly altering, destroying, concealing or falsifying records, or making false entries, with intent to impede or influence a federal investigation, bankruptcy proceeding or other matter within federal jurisdiction. Violations are punishable by a fine, imprisonment for up to 20 years, or both.
- Destruction of corporate audit records: Under 18 USC Section 1520, accountants auditing issuers are required to retain specified audit and review records. A knowing and wilful violation of the applicable record-retention requirements is punishable by a fine, imprisonment for up to ten years, or both.

Failure to maintain accurate books and records or adequate internal controls may also result in civil or administrative enforcement by the SEC even where the requirements for criminal liability are not satisfied.

3.7 Cartels and Criminal Competition Law

In recent years, the US has significantly expanded the criminal and sanctions framework applicable to international drug cartels and other transnational criminal organisations.

In January 2025, President Trump issued Executive Order 14157 authorising the designation of certain international cartels and other organisations as Foreign Terrorist Organizations (FTOs) and Specially Designated Global Terrorists (SDGTs). Since then, the State Department has designated numerous cartels and other transnational criminal organisations as FTOs, bringing dealings with those organisations within the scope of federal terrorism and sanctions laws.

Of particular relevance, 18 USC Sections 2339A and 2339B criminalise certain forms of "material support or resources" connected with terrorism. Section 2339B makes it unlawful knowingly to provide material support or resources to an organisation designated as an FTO, or to attempt or conspire to do so. "Material support or resources" is broadly defined and includes, among other things, currency or monetary instruments, financial services, lodging, training, expert advice or assistance, communications equipment, facilities, weapons, transportation and other tangible or intangible property or services.

Accordingly, companies may face criminal exposure where, through their employees or agents, they knowingly provide prohibited funds, goods, services or other assistance to a designated cartel. The statute may also apply extraterritorially in specified circumstances, creating potential exposure for both US and non-US persons and entities whose dealings with designated cartels have a sufficient jurisdictional nexus to the US.

A violation of Section 2339B may result in substantial criminal penalties. In addition, where the designated cartel is also an SDGT, OFAC sanctions generally require the blocking of its property and interests in property within US jurisdiction and prohibit US persons from engaging in transactions or dealings with it unless authorised by OFAC. Violations of applicable sanctions may give rise to civil or criminal penalties.

3.8 Consumer Criminal Law

Consumer protection in the US is enforced through a combination of federal criminal, civil and administrative laws. The FTC is the principal federal consumer-protection agency and may bring enforcement actions against unfair or deceptive acts or practices, including false advertising, deceptive marketing, fraud and other conduct that causes or is likely to cause consumer harm.

Other federal agencies also enforce consumer-protection laws within their respective areas of authority. The Consumer Financial Protection Bureau (CFPB) enforces federal consumer-financial laws, including prohibitions on unfair, deceptive or abusive acts or practices by financial institutions and other covered persons. The US Food and Drug Administration (FDA) enforces laws concerning, among other things, adulterated or misbranded food, drugs, medical devices and other regulated products. The DOJ prosecutes serious consumer-related misconduct, including schemes involving mail or wire fraud, deceptive telemarketing, healthcare fraud and violations of certain food, drug and product-safety laws.

Criminal liability generally requires the government to establish the elements of the underlying statute, including any required intent or knowledge. For example, mail and wire fraud require a scheme to defraud and use of the mails or interstate or foreign wire communications in furtherance of that scheme, and are generally punishable by imprisonment for up to 20 years and a fine. Other consumer-protection violations may result in civil penalties, injunctions, restitution, forfeiture or, where the applicable statute provides for criminal liability, fines and imprisonment.

State attorneys general and other state authorities may also bring actions under state consumer-protection and unfair-or-deceptive-practices laws.

3.9 Cybercrimes, Computer Fraud and Protection of Company Secrets

Federal cybercrime and computer-fraud offences are principally governed by the Computer Fraud and Abuse Act (CFAA), while theft of company secrets is addressed by the Economic Espionage Act (EEA).

Under the CFAA (18 USC Section 1030), prohibited conduct includes intentionally accessing a protected computer without or beyond authorisation to obtain information, accessing a protected computer with intent to defraud and obtain something of value, causing unauthorised damage, and trafficking in passwords or similar access information. Penalties generally include fines and imprisonment of up to one to ten years for a first offence, with higher penalties for aggravated or repeat violations.

18 USC Section 1029 separately covers knowingly and fraudulently producing, using, possessing or trafficking in counterfeit or unauthorised access devices, including account numbers or payment credentials. First-offence penalties may include imprisonment for up to ten or 15 years, depending on the conduct.

Under 18 USC Section 1832, a person may be liable for knowingly stealing, obtaining, copying, transmitting, receiving or possessing a trade secret without authorisation, with intent to benefit someone other than the owner and knowing or intending that the owner will be injured. Individuals face up to ten years' imprisonment, while organisations may be fined the greater of USD5 million or three times the value of the trade secret.

Where the conduct is intended to benefit a foreign government, instrumentality or agent, 18 USC Section 1831 provides enhanced penalties of up to 15 years' imprisonment and a USD5 million fine for individuals, and the greater of USD10 million or three times the value of the trade secret for organisations.

Attempts and conspiracies may also be punishable, together with forfeiture and civil remedies.

3.10 Financial/Trade/Customs Sanctions

Through the Office of Foreign Assets Control (OFAC), within the US Department of the Treasury. OFAC administers sanctions against foreign countries, regions, entities and individuals in furtherance of US foreign-policy and national-security objectives.

OFAC sanctions generally require US persons to block assets or restrict financial or commercial dealings with sanctioned persons or jurisdictions. Some programmes are comprehensive and prohibit all transactions with a targeted country, while others restrict only specified persons, sectors or activities. Transactions that would otherwise be prohibited may be authorised through general or specific licences.

US law imposes both civil and criminal penalties for violations, attempted violations, conspiracies and causing another person to violate OFAC sanctions. Civil liability may arise without proof of knowledge, while criminal liability generally requires a wilful violation. Foreign persons may also face liability where they conspire to violate or cause a violation of US sanctions, and certain programmes permit secondary sanctions, including designation on the SDN List.

OFAC generally looks to the economic substance of a transaction, including whether blocked persons are acting through agents or intermediaries while retaining a direct or indirect interest in the relevant assets or transactions.

Export-control violations are principally governed by the EAR and the Export Control Reform Act. Wilful violations may result in fines of up to USD1 million per

violation and imprisonment for up to 20 years, while civil or administrative sanctions may include monetary penalties, licence revocation and denial of export privileges. US-origin items generally remain subject to the EAR wherever located, and certain foreign-produced items may also be covered. For defence articles and services, the Arms Export Control Act and ITAR impose separate licensing requirements, with wilful violations carrying fines of up to USD1 million per violation and imprisonment for up to 20 years.

Finally, customs violations may give rise to criminal and civil liability. Under 18 USC Section 545, knowingly importing goods contrary to law, smuggling merchandise or using fraudulent customs documentation may result in imprisonment for up to 20 years and a fine. Under 19 USC Section 1592, materially false statements or omissions in customs entries may result in civil penalties.

3.11 Concealment

Concealment is typically prosecuted through obstruction and false-statement statutes.

Under 18 USC Section 1503, a person may be liable for corruptly influencing, obstructing or impeding the due administration of justice in a federal judicial proceeding. Violations generally carry imprisonment for up to ten years.

Under 18 USC Section 1505, it is an offence to obstruct or impede proceedings before federal agencies or Congress, including by concealing, destroying or falsifying material relevant to an investigation. Violations are generally punishable by imprisonment for up to five years.

18 USC Section 1001 prohibits knowingly and wilfully concealing or covering up a material fact by trick, scheme or device in a matter within federal jurisdiction. Where liability is based on nondisclosure, the government generally must also establish a duty to disclose. Violations are generally punishable by imprisonment for up to five years.

In addition, 18 USC Section 1512 (c) prohibits corruptly altering, destroying or concealing records or other objects with intent to impair their use in an official proceeding. Violations may result in imprisonment for up to 20 years.

3.12 Aiding and Abetting

Federal and state laws may impose liability on persons who conspire with, aid or otherwise assist others in committing corporate offences.

Under 18 USC Section 371, conspiracy generally requires an agreement between two or more persons to commit a federal offence or defraud the US, knowing and intentional participation in the agreement, and an overt act by at least one conspirator in furtherance of it. The underlying offence need not be completed. A violation is punishable by a fine and imprisonment for up to five years, subject to the maximum penalty for the underlying offence where the object of the conspiracy is a misdemeanour.

Under 18 USC Section 2, a person who aids, abets, counsels, commands, induces or procures the commission of a federal offence may be held liable as a principal. Liability generally requires commission of the underlying offence, intentional assistance or facilitation, and the requisite intent. A person who wilfully causes another to commit an act constituting a federal offence may also be liable as a principal.

Aiding and abetting does not carry a separate penalty; the defendant is subject to the same penalties as the principal offender.

3.13 Money Laundering

The principal federal money-laundering offences are set out in 18 USC Sections 1956 and 1957.

Under Section 1956, liability generally requires that a person know the property represents proceeds of unlawful activity and conduct or attempt a financial transaction involving those proceeds with a prohibited purpose, such as promoting unlawful activity, concealing the nature or source of the proceeds, or avoiding transaction-reporting requirements. Violations are punishable by imprisonment for up to 20 years and a fine of up to USD500,000 or twice the value involved, whichever is greater.

Under Section 1957, it is an offence knowingly to engage in a monetary transaction exceeding USD10,000 involving criminally derived property from specified unlawful activity. Violations are punishable by imprisonment for up to ten years and a fine. Predicate offences are broadly defined and include, among others, fraud, bribery, drug trafficking, terrorism, racketeering, human trafficking, and certain smuggling and export-control offences.

Separately, the Bank Secrecy Act (BSA) requires covered financial institutions to maintain risk-based AML programmes and comply with record-keeping and reporting requirements, including suspicious activity reports (SARs).

FinCEN administers and enforces the BSA, together with federal banking and other functional regulators, while the DOJ prosecutes criminal money-laundering and wilful BSA violations. Failure to maintain an adequate AML programme or comply with reporting obligations may result in civil or administrative penalties. Wilful BSA violations may also result in criminal fines of up to USD250,000 and imprisonment for up to five years, increasing to USD500,000 and up to ten years in aggravated cases.

3.14 ESG-Related Offences

ESG-related misconduct may be pursued under a range of existing federal and state laws rather than through a single ESG-specific regime. The DOJ, SEC, CFTC and state authorities have addressed conduct involving, among other things, forced-labour imports under the UFLPA, misleading ESG or environmental disclosures, carbon-market manipulation, investment and consumer fraud, false claims and anti-competitive practices.

3.15 Artificial Intelligence and Automation Misuse

The US does not currently have a general federal criminal offence specifically addressing misuse of AI or automated decision-making. Existing fraud, securities and market-manipulation laws instead apply where AI or automated systems are used to engage in unlawful conduct.

For example, materially false or misleading statements regarding AI may result in liability under federal fraud or securities laws. The SEC has pursued "AI washing" cases involving misleading representations about the use of AI, with potential sanctions including civil penalties, disgorgement and injunctions, as well as criminal fines and imprisonment where the requirements of an applicable criminal offence are met.

Algorithmic trading is likewise subject to existing market-manipulation rules, including prohibitions on spoofing and other deceptive trading practices.

The DOJ also considers AI-related risk management when assessing corporate compliance programmes, including whether companies have appropriate controls, human oversight and measures to identify and mitigate deliberate or reckless misuse of AI.

3.16 Crypto-Assets and Digital Currency Crimes

The DOJ generally addresses misconduct involving crypto-assets under existing federal laws, including wire fraud, money laundering, sanctions violations and unlicensed money transmission. Its April 2025 memorandum *Ending Regulation by Prosecution* stated that enforcement should focus on intentional criminal conduct rather than using criminal cases to impose regulatory requirements absent wilful misconduct.

Classification remains relevant to enforcement. Depending on the asset and transaction, securities, commodities, tax or money-transmission rules may apply. In April 2026, the Treasury proposed regulations to implement the GENIUS Act's AML and sanctions-compliance requirements for payment stablecoin issuers.

Crypto exchanges and other service providers may also be subject to FinCEN registration, AML, record-keeping and suspicious-activity-reporting requirements, as well as state licensing laws. Knowingly operating an unlicensed money-transmitting business may result in fines and imprisonment for up to five years under 18 USC Section 1960.

4. Pleas and Defences

4.1 White-Collar Defences

There is no single set of defences applicable to all federal white-collar offences. The defences available depend on the elements of the particular charge and the facts of the case. However, common arguments and defences include:

- Failure to prove the required mental state – many white-collar offences require proof of intent, knowledge or wilfulness. A defendant may argue that the conduct was undertaken in good faith or without the state of mind required by the relevant statute.
- Failure to establish other elements of the offence – defendants may challenge whether the government has proved each statutory element beyond a reasonable doubt, including, where applicable, materiality, falsity, a scheme to defraud or other offence-specific requirements.
- Jurisdictional or extraterritorial limitations – a defendant may argue that the relevant conduct falls outside the territorial or jurisdictional reach of the statute.
- Authorised or lawful conduct – depending on the applicable statutory or regulatory framework, a defendant may contend that the conduct was licensed, authorised or otherwise permitted.
- Statute-specific exceptions or affirmative defences – certain federal statutes expressly provide particular defences. For example, the FCPA permits a defendant to establish that a payment, gift, offer or promise was lawful under the written laws and regulations of the foreign official's country (15 USC Section 78dd-1 (c)(1)).
- Generally applicable criminal-law defences – depending on the circumstances, defences such as duress or entrapment may be available.
- Constitutional or procedural challenges – defendants may seek to exclude evidence obtained in violation of constitutional protections or otherwise challenge unlawful investigative conduct.
- Statute of limitations – a defendant may argue that the prosecution was commenced outside the applicable limitations period.

An effective compliance programme does not generally constitute a substantive defence to federal criminal liability. A corporation may therefore be held criminally liable for misconduct by its employees or agents even where the conduct violated internal policies or compliance procedures. Nevertheless, the existence and effectiveness of a compliance programme can materially affect the government's exercise of prosecutorial discretion, the form and terms of a corporate resolution, and the penalties imposed. The US Sentencing Guidelines also provide potential sentencing credit to organisations that maintained an effective compliance and ethics programme, subject to specified conditions.

4.2 De Minimis

There is no general de minimis exception applicable to federal white-collar offences in the US, nor are particular industries or sectors generally exempt from federal criminal laws. Liability instead depends on whether the elements of the particular statutory offence are satisfied.

Certain federal offences contain specific monetary thresholds, exclusions or other limitations that operate as part of the statutory definition of the offence. For example, 18 USC Section 1957 applies to certain monetary transactions involving criminally derived property valued at more than USD10,000, while federal programme bribery under 18 USC Section 666 generally requires the relevant transaction to involve USD5,000 or more and the organisation or government entity concerned to receive more than USD10,000 annually in federal programme benefits. Other statutes may contain specific exclusions, exceptions or affirmative defences. For example, the FCPA's anti-bribery provisions contain a narrow exception for certain facilitating or expediting payments for routine governmental action, as well as affirmative defences relating to payments lawful under written foreign law and reasonable bona fide business expenditures.

Although particular industries may be subject to specialised regulatory regimes, there is no general industry or sector exemption from federal white-collar criminal liability.

4.3 Plea Agreements, Co-Operation, Self-Disclosure and Leniency

Federal prosecutors and defendants may negotiate plea agreements under Rule 11 of the Federal Rules of Criminal Procedure. A defendant may plead guilty or nolo contendere to a charged, lesser or related offence in exchange for the government agreeing not to bring, or to dismiss, other charges; recommending or agreeing not to oppose a particular sentence or sentencing range; or agreeing that a particular sentence or sentencing range is appropriate.

A defendant's acceptance of responsibility can also reduce the applicable sentencing range. Under the US Sentencing Guidelines, a defendant who clearly demonstrates acceptance of responsibility generally receives a two-level reduction in the offence level, with a possible additional one-level reduction where the applicable requirements are met. Co-operation with investigators or prosecutors may result in additional leniency. Where a defendant provides substantial assistance in the investigation or prosecution of another person, the government may move for a sentence below the applicable Guidelines range and, in appropriate circumstances, below a statutory mandatory minimum.

Self-disclosure is particularly significant for corporate defendants. Under the DOJ's Department-wide Corporate Enforcement and Voluntary Self-Disclosure Policy, issued in March 2026, the DOJ will generally decline to prosecute a company that voluntarily self-discloses misconduct, fully co-operates with the government's investigation and remediates the misconduct on an appropriate and timely basis, provided that no specified aggravating circumstances are present.

Individuals may also obtain significant benefits from voluntary disclosure. Under the Criminal Division's Pilot programme on Voluntary Self-Disclosures for Individuals, qualifying individuals involved in certain corporate criminal conduct may receive a non-prosecution agreement where, among other requirements, they voluntarily and truthfully disclose original information, fully co-operate and provide substantial assistance, and forfeit illicit gains and compensate victims. Other forms of leniency available in appropriate cases include non-prosecution agreements, deferred prosecution agreements and grants of immunity.

4.4 Whistle-Blower Protection

The US has several federal programmes that protect whistle-blowers from retaliation and offer financial incentives for reporting misconduct. For example, the DOJ Criminal Division's Corporate Whistleblower Awards Pilot Program may provide awards to individuals who submit original, truthful information concerning specified criminal misconduct that results in forfeitures exceeding USD1 million in net proceeds.

The SEC, CFTC, OSHA and FinCEN also operate whistle-blower programmes designed to encourage reporting of misconduct within their respective jurisdictions. In addition, the proposed AI whistle-blower Protection Act seeks to protect individuals involved in developing or deploying AI from restrictive severance and non-disclosure agreements that could discourage reports to federal authorities, although the legislation has not yet been enacted. Separately, on 1 April 2026, FinCEN issued a proposed rule for a whistle-blower programme covering AML, sanctions and other violations. Under the proposal, eligible whistle-blowers could receive between 10% and 30% of collected monetary sanctions, with a presumption in favour of the maximum 30% award where that amount would not exceed USD15 million in the aggregate.

Companies are encouraged to implement internal reporting and anti-retaliation mechanisms as part of their compliance programmes, including confidential reporting channels, escalation procedures and policies prohibiting retaliation.

4.5 Cross-Border Defence Strategies

White-collar investigations involving multiple jurisdictions can significantly affect defence strategy because the same conduct may expose a company or individual to parallel investigations, different substantive laws and inconsistent procedural or disclosure obligations.

There is no general rule preventing multiple sovereigns from investigating or prosecuting the same conduct. Under the US separate-sovereigns doctrine, a resolution in another country does not necessarily bar a US prosecution arising from the same core facts.

However, the DOJ has adopted an "anti-piling on" policy encouraging coordination with US and foreign authorities to avoid unnecessary duplicative corporate penalties. That policy was reaffirmed in June 2025, with the caveat that coordination should not reduce or eliminate compensation to victims.

Co-ordinated or "global" settlements are common in complex multinational matters, particularly in areas such as foreign bribery and antitrust. In such cases, defence strategy often involves seeking consistency among settlement terms, financial penalties, compliance obligations and monitorship requirements across jurisdictions.

Cross-border co-operation is not unlimited. Mutual legal assistance treaties are an important mechanism for evidence gathering and information sharing, but their availability and scope vary by country, and some jurisdictions may interpret them narrowly or may be less willing or able to cooperate because of political, legal or resource constraints. Differences in substantive law may also complicate the defence; conduct that is lawful or exempt in one jurisdiction may be prohibited in another.

5. Key Trends and Future Outlook

5.1 The Year Ahead

The DOJ is expected to roll out its Department-wide Corporate Enforcement and Voluntary Self-Disclosure Policy, issued in March 2026. Under the policy, companies that promptly self-report misconduct, fully cooperate with the government and undertake appropriate remediation may benefit from a presumption in favour of declination, absent specified aggravating circumstances. The policy is therefore likely to encourage companies to investigate potential wrongdoing quickly and assess voluntary disclosure at an earlier stage.

FinCEN and the federal banking regulators have also proposed a revised AML/CFT framework centred on effective, risk-based compliance. If adopted, the framework would require financial institutions to place greater emphasis on documented risk assessments, FinCEN's national priorities, governance, testing and oversight. FinCEN has also proposed rules governing AML whistle-blower incentives and additional AML, customer identification, suspicious activity reporting and sanctions obligations for payment stablecoin issuers.

Further regulatory attention to the use of artificial intelligence is also expected. The FTC is considering guidance addressing potentially misleading claims regarding the accuracy and objectivity of AI systems, which could increase scrutiny of representations concerning AI capabilities, training data, testing, safeguards and human oversight.

At the same time, updated model-risk guidance and interagency statements promote responsible use of AI, machine learning and advanced analytics in AML compliance. As a result, technology governance, data quality and validation are likely to become increasingly important in corporate compliance and investigations.

Chambers | Practice Guides

Chambers Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Luke.Wilson@Chambers.com