Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

White-Collar Crime 2023

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

USA: Law & Practice

Brian Benczkowski, John Lausch, Kim Nemirow and Sunil Shenoi
Kirkland & Ellis

USA

Law and Practice

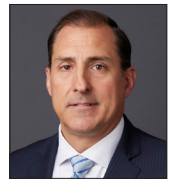
Contributed by:
Brian Benczkowski, John Lausch, Kim Nemirow and Sunil Shenoi
Kirkland & Ellis

Contents

Kirkland & Ellis has one of the largest government, regulatory and internal investigations (GR&II) groups in the world, with more than 200 attorneys who work on white-collar criminal defence and securities enforcement matters, including more than 50 who served as DOJ officials, and at the SEC, the FTC, the UK's Serious Fraud Office and other global government agencies. Kirkland's GR&II group is best known for representing Fortune 500 companies and their officers and directors in their most sensitive matters, which are typically resolved confidentially, but have also included some of the largest public representations in history. Recently, the group has led some of the most high-profile white-collar matters, including representing Celsius Network in the resolution of parallel government investigations; Nikola Motors in response to a damaging report issued by the activist hedge fund Hindenburg Research; and J.P. Morgan Chase in relation to allegations of market manipulation and "spoofing".

Authors

Brian Benczkowski is a partner in Kirkland & Ellis's government, regulatory and internal investigations group. He has significant government enforcement and investigations experience from multiple government leadership positions, including having served as Assistant Attorney General for the DOJ's Criminal Division, where he oversaw many of the most wide-ranging complex criminal cases and implemented policy changes related to how the DOJ prosecutes corporations. At Kirkland, Brian represents corporations in government enforcement matters before state and federal entities. He also conducts internal investigations on behalf of clients, represents companies and individuals in congressional investigations and prepares clients for testimony at committee hearings.



John Lausch is a partner in Kirkland & Ellis's government, regulatory and internal investigations group. He is the former United States Attorney for the Northern District of Illinois, where he led the office to numerous successful and significant prosecutions in public corruption, national security and financial fraud, among others. John also served on the U.S. Attorney General's Advisory Committee, which advised the Attorney General on policy, management and operational issues impacting the DOJ nationwide. At Kirkland, John represents clients before governmental entities and leads confidential internal investigations, including in connection with allegations of FCPA violations, healthcare fraud and environmental crimes.

Kim Nemirow is a partner in Kirkland & Ellis's government, regulatory and internal investigations group. She advises multinational organisations and individuals in a wide variety of DOJ and SEC investigations, internal investigations and compliance matters. She has led countless investigations for private equity, pharmaceutical, technology and other clients into potential violations of the FCPA, securities laws and various healthcare fraud statutes. A frequent author and speaker, Kim is regularly called upon to advise clients on highly sensitive matters, including those involving workplace misconduct and compliance. She also teaches a class at the University of Chicago Law School, titled "Enforcement Risks in Cross-Border Transactions".

Sunil Shenoi is a partner in Kirkland & Ellis's government, regulatory and internal investigations group. He represents multinational organisations and individuals in a wide variety of DOJ and SEC investigations, including numerous investigations for private equity, medical device, retail and other clients involving the FCPA, financial statement and disclosure issues, insider trading and other securities enforcement issues. Sunil also advises clients on data security and data privacy matters, with a focus on responding to data breaches, defending against data breach litigation and advising clients on compliance with laws and providing regulatory guidance relating to these issues.

Kirkland & Ellis

300 N LaSalle
Chicago
IL 60654
USA

Tel: +1 312 862 2000
Web: www.kirkland.com

KIRKLAND & ELLIS

1. Legal Framework

1.1 Classification of Criminal Offences

In the United States, both federal law and state law define and prohibit crimes. US law classifies crimes as felonies or misdemeanours. A third category of offences punishable only by fine, civil penalty or forfeiture, rather than imprisonment, includes petty crimes – sometimes referred to as violations, infractions, petty offences or petty misdemeanours. Felonies and misdemeanours are sometimes subdivided based on the seriousness and severity of the offence (a Class A offence, a Class B offence, etc) (18 USC § 3559).

Felonies are the most serious offences. Both property crimes (including white-collar crimes) and crimes against persons can be felonies. Any crime punishable by more than one year in prison is classified as a felony, but not all felonies result in imprisonment. Punishments for felonies can range from fines or limited time in prison to life without parole or death. Punishments for misdemeanours, which are punishable by one year or less in prison or jail, could entail a fine, restitution, house arrest, probation or community service.

To prove a criminal offence, prosecutors must generally establish proof beyond a reasonable doubt of an act or omission (actus reus) and a culpable state of mind (mens rea). The mental state required for conviction varies by crime. For example, prosecutors may need to prove that a defendant acted purposely, knowingly, recklessly or negligently, depending on the offence charged. Some categories of crimes are strict liability offences requiring no mens rea showing, including some regulatory offences.

Attempts to commit crimes can also carry criminal liability. Typically, a prosecutor must prove that the accused intended to commit the crime and knowingly took a substantial step, beyond mere preparation, in furtherance of the attempt.

1.2 Statute of Limitations

A statute of limitations sets the maximum amount of time that a prosecutor in criminal cases, or a plaintiff in civil cases, has to bring charges or initiate legal proceedings. Most offences are subject to such a statute. The general federal statute of limitations is five years (18 USC § 3282). However, certain securities and tax crimes, and major frauds against the US, have up to six- or seven-year limitation periods (18 USC § 1031; 26 USC § 6531). Other serious crimes or conspiracies involving fraud or embezzlement affecting banks and other financial institutions have ten-year periods (18 USC § 3293(2)). Several serious crimes have no limitation periods, such as capital murder and certain acts of terrorism (18 USC §§ 3281 and 3286).

Statute of limitation periods normally begin to run when the crime is “complete”, which occurs when the last element of the crime is satisfied. For “continuing crimes” that do not occur at a discrete time, such as conspiracy, the limitation period may not begin to run until the last affirmative act is committed in furtherance of the scheme.

Limitation periods may also be paused or tolled. In fact, regulators often request that potential subjects or targets of investigations enter into an agreement (known as a tolling agreement) to toll the limitation period for a specific period of time.

1.3 Extraterritorial Reach

A number of US criminal statutes apply extraterritorially. As such, federal courts and some agencies may punish defendants for criminal acts that occur outside of US territory. Extrater-

ritorial reach is permitted when a federal statute expressly states that it applies to conduct outside the US. One such statute is the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), which allows the Securities and Exchange Commission (SEC) to enforce anti-fraud provisions of the federal securities laws where conduct occurring outside the US has a "foreseeable substantial effect" within the US (15 USC § 78aa(b)(2)).

A presumption exists against extraterritorial application of US law, so the statute must clearly apply to any extraterritorial conduct charged. Nevertheless, criminal conduct that involves only minor contact with US territory, such as processing financial payments through the US banking system or the use of US wires, may be sufficient to invoke territorial jurisdiction. This can be the case even where most of the conduct was extraterritorial.

In certain limited circumstances, courts have construed US statutes broadly to allow prosecutors to bring cases against defendants who commit offences abroad, particularly through the Foreign Corrupt Practices Act (FCPA) (15 USC §§ 78dd-1 et seq). Other federal criminal statutes with potential extraterritorial application include:

- money laundering (18 USC § 1956);
- wire fraud (18 USC § 1343);
- conspiracy (18 USC § 371);
- false statements (18 USC § 1001); and
- the Racketeer Influenced and Corrupt Organizations Act (RICO) (18 USC § 1961 et seq).

1.4 Corporate Liability and Personal Liability

Criminal liability can apply to individuals or legal entities, which are treated as "legal persons" under the law. Individuals and entities may be liable for the same offence, but a separate case must be made against each individual and against each entity. Individual directors and officers are not liable for offences committed by their entities. In some circumstances, directors and officers of an entity may be liable for misconduct of the entity's agents if they failed to exercise their authority to prevent the misconduct.

Under the doctrine of respondeat superior, an entity is liable for the acts of its directors, officers, employees and agents that are both committed within the scope of their employment and at least partially motivated by an intent to benefit the entity. Entities are responsible for the actions of their employees that meet these conditions even if the actions violated the entity's express policies or instructions. Knowledge of individual directors, officers, employees or agents can be imputed collectively to the entity as a whole under the collective knowledge doctrine. A parent entity is generally not liable for the acts of its subsidiary but can be if the parent exercises sufficient control over that subsidiary. Liability flows from a subsidiary to the parent if the parent treats the subsidiary as an extension of itself, rather than a separate entity, such that the subsidiary is an agent or alter ego of the parent.

In the context of mergers, the surviving entity is responsible for the predecessors' liabilities under the doctrine of successor liability. In cases of acquisition, however, a successor entity does not always assume the liabilities of the acquired entity. Courts consider several factors in determining whether a successor entity can be held responsible for the acquired entity's liabilities. Those factors include, but are not limited to:

- whether there was an assumption of liabilities;

- whether the transfer was legitimate or a legal fiction;
- whether the buyer is a mere continuation of the seller; and
- whether the buyer continues essentially the same work as the seller.

Department of Justice (DOJ) policy generally favours prosecuting individuals as well as legal entities in cases of corporate wrongdoing. The government prosecutes entities to address crimes typically exclusive to entities, such as environmental crime, and to encourage a culture of legal compliance. Based on the fact that knowledge of many directors, officers and employees can be imputed to the entity, it is often easier to prove a culpable mental state for an entity than for an individual. DOJ prosecutors weigh various factors when deciding whether to criminally prosecute entities (see **2.6 Prosecution**).

1.5 Damages and Compensation

The Crime Victims' Rights Act provides that victims of federal crimes have the "right to full and timely restitution as provided in law" (18 USC § 3771(a)(6)). The Mandatory Victims Restitution Act (MVRA) requires a sentencing judge to award full restitution to victims of crimes against property, such as wire fraud, mail fraud and many financial crimes (18 USC § 3663A). The MVRA applies if the individual or entity suffering the loss is a "victim" that is "directly and proximately harmed as a result" of the crime.

Some statutes explicitly provide for damages for victims. For example, RICO provides that any person injured may sue in federal district court to recover treble damages, as well as reasonable attorneys' fees (18 USC § 1964).

1.6 Recent Case Law and Latest Developments

In 2022, the DOJ's Fraud Section achieved seven corporate resolutions, which generated USD2.1 billion in monetary recovery. Five corporate resolutions were handled by the FCPA Unit, and two were handled by the Market Integrity and Major Frauds Unit.

In FY2022, the SEC filed 760 enforcement actions, obtaining judgments and orders amounting to nearly USD2.2 billion in disgorgement, and over USD4.2 billion in penalties, the latter of which was the highest on record. Although whistle-blower awards decreased from USD564 million in FY2021 to USD229 million in FY2022, the FY2022 awards remained the second highest total in SEC history. The SEC's Whistleblower Program also received more than 12,300 whistle-blower tips in FY2022, a record number.

In March 2022, the US Attorney General, the Deputy US Attorney General and the Assistant Attorney General clarified key areas of focus for the DOJ in white-collar enforcement, specifically announcing four significant policy changes.

- A budget increase of more than USD350 million was proposed, to hire additional federal prosecutors and law enforcement agents to beef up white-collar crime enforcement.
- Focus was heightened on prosecutions of individuals who commit crime in the corporate context, including through "force multipliers" such as data analytics and collaborative partnerships with both domestic and international enforcement agencies. The Assistant Attorney General also added that companies should consider replacing leadership in certain circumstances, even if there is no evidence that an executive or director personally

committed a crime: namely, when leadership creates a corporate culture in which wrongdoing is enabled or goes undetected.
- Emphasis on a victim-centric approach to white-collar crime enforcement was renewed, including expectations that corporate defendants will address "victim issues" in Filip Factors presentations (see **2.6 Prosecution**) in which companies state the case against prosecution.
- A Director of COVID-19 Fraud Enforcement was appointed to continue the DOJ's efforts to combat fraud perpetrated in the context of the COVID-19 pandemic. In August 2023, the DOJ announced that its most recent efforts in this arena had resulted in 718 enforcement actions relating to COVID-19 fraud, involving more than USD830 million. This brought the total seizure amount to USD1.4 billion and the total number of charged defendants to more than 3,000. The Deputy Attorney General also announced the creation of two strike forces at the US Attorney's Offices for the Districts of Colorado and New Jersey to supplement the three existing strike forces launched in September 2022 in California, Florida and Maryland.

Furthermore, in January 2023, the Assistant Attorney General announced the first significant changes to the DOJ Criminal Division's Corporate Enforcement Policy since 2017. The changes are designed to further incentivise companies to self-report potential wrongdoing by allowing prosecutors to offer declinations even in the face of aggravating circumstances. For companies in this situation to qualify for a declination, they must be able to show that they:

- made a self-disclosure immediately upon discovery of the alleged misconduct;
- had an effective compliance programme and set of internal accounting controls in place; and
- provided extraordinary co-operation and implemented extraordinary remediation.

In addition, the changes increased the permissible reduction from the sentencing guidelines for instances in which these conditions have been met but a criminal resolution is still pursued, and also dictated that a corporate guilty plea will generally not be required in such situations.

Two months later, in March 2023, the Assistant Attorney General announced changes to the DOJ Criminal Division's Evaluation of Corporate Compliance Programs that take into account corporate compliance policies and procedures regarding the use of so-called ephemeral messaging applications, or applications that delete communications after they are sent. The Assistant Attorney General also announced the creation of the Pilot Program Regarding Compensation Incentives and Clawbacks, which will require every defendant entering into a corporate resolution with the Criminal Division to adhere to certain criteria when issuing bonuses, such as a prohibition on bonuses for non-compliant employees.

In addition, the SEC signalled its intent to pursue the enforcement of new rules governing the conduct of investment advisers and investment companies. In the investment adviser space, the SEC enacted a new Marketing Rule that prohibits advertisements that include a material misstatement of fact. With respect to investment companies, the Commission enacted:

- a new Derivatives Rule that requires funds engaging in derivatives transactions to main-

tain a compliance programme to manage corresponding risks; and
- a Fair Valuation Rule that mandates that funds' securities and asset valuations must be made in good faith to approximate their fair market value.

In August 2023, the SEC also amended the Investment Advisers Act of 1940 to impose new requirements on private fund advisers, including quarterly reporting and auditing responsibilities and certain restrictions relating to fees imposed on investors. Beyond the enforcement of these new rules, the SEC is likely to continue to focus on previous areas of interest, such as environmental, social and governance issues and practices related to crypto-assets.

Lastly, the SEC also announced new rules in July 2023 that require public companies to disclose any material cybersecurity events in their Form 8-K. To supplement this new rule, newly registered public companies must also disclose any internal processes relating to cybersecurity compliance.

2. Enforcement

2.1 Enforcement Authorities

Both federal and state governments can investigate, prosecute and enforce laws related to white-collar offences.

Federal white-collar offences are investigated by a variety of governmental agencies. Civil investigations and enforcement actions may be initiated by, among others, civil attorneys at the DOJ, the SEC, the Commodity Futures Trading Commission, the Federal Reserve Bank, the Federal Trade Commission (FTC), the Office of Foreign Assets Control (OFAC), the Environmental Protection Agency and the Internal Revenue Service (IRS). All federal criminal offences are investigated and prosecuted through the DOJ, often in partnership with other agencies. Both civil and criminal federal cases are heard by federal courts. Some administrative actions are litigated within the agencies themselves, with the possibility of appeal to the federal courts.

States have a parallel set of criminal and civil laws, and their own courts to hear cases. State prosecutors' offices (often called state's attorneys or district attorneys) bring cases based on criminal offences within their jurisdiction. State investigation and enforcement regimes for civil offences vary by state, but most have a series of state investigative agencies and a state Attorney General, who acts as chief legal officer for the state.

Self-regulatory organisations (such as the Financial Industry Regulatory Authority, the Options Clearing Corporation and the New York Stock Exchange) also enforce industry rules and professional regulations.

2.2 Initiating an Investigation

Investigations may be initiated by agencies or prosecutors whenever they have reason to believe that an offence has been committed within their jurisdiction. Regulatory agencies each possess their own set of standards for initiating investigations, which are based on their authorising statutes and their respective enforcement manuals. Investigations vary in formality. For example, the SEC's Division of Enforcement, which investigates and prosecutes wrongdoing under the federal securities laws, may investigate through a relatively informal process, known as a "matter under inquiry", or a formal investigative order. The less formal "matter under inquiry" investigation often arises from an entity's self-

reporting of possible misconduct or in response to media publicity of possible misconduct, and it may lead to a formal investigation.

Civil investigations begin when a regulatory agency, such as the SEC, begins exploring a civil claim against a defendant. Criminal investigations are initiated by agencies working in partnership with the DOJ, often through the local United States Attorney's Office. Potential targets of investigations can be identified by a whistleblower who voluntarily shares knowledge or suspicion of wrongdoing or illegal activity with the government.

In federal cases with possible civil and criminal claims, the DOJ encourages co-ordination of investigations with civil regulatory agencies – known as parallel proceedings – to facilitate information-sharing between civil and criminal investigators, where permitted.

2.3 Powers of Investigation

In both civil and criminal investigations, the government can conduct voluntary interviews, make informal requests for documents or information and issue subpoenas to both investigation targets and third parties for the production of evidence. Although it is possible to seek to quash a subpoena in court as being overly broad, companies and individuals often negotiate with the government to narrow the subpoena's scope and the type of documentation sought. In federal civil cases, one form of information-gathering is a civil investigative demand requiring the production of specified documents or information.

In criminal investigations, the government may use a grand jury to issue subpoenas that compel the production of documents or testimony. The government may also obtain search warrants, which can be used to search particular places such as offices or databases, and to seize documents. To obtain a search warrant, investigators must make a showing to an authorising judge of probable cause that the stated offence has been committed and that evidence of said offence is located in a certain place.

During a voluntary interview with the government, the interviewee has no obligation to answer questions. The government can compel people to submit to questioning in limited circumstances. A person responding to a grand jury subpoena for testimony must appear but may consult with their attorney outside the presence of the grand jury before answering questions. A person may always refuse to answer a question if an answer would tend to incriminate that person but may not refuse to answer questions that would tend only to incriminate an entity or another person.

2.4 Internal Investigations

While not always required, internal investigations allow entities to identify and remediate problems, and to self-report to the government. Internal investigations are also used to demonstrate a commitment to compliance and reform that can justify leniency from the government. The existence and adequacy of internal investigations is one factor considered by the federal government when deciding whether to charge entities. For this reason and others, including the applicability of attorney-client privilege in the US, careful attention needs to be paid to the structuring and execution of internal investigations.

Officers and directors of an entity must often promptly investigate possible wrongdoing to fulfil their legal and fiduciary obligations. For example, statutes such as the Sarbanes-Oxley Act (Sarbanes-Oxley) require entities to establish procedures for employees to report possi-

ble wrongdoing to company leaders. Reports of possible violations by employee "whistle-blowers" should trigger an investigative response. Failing to investigate reports of possible misconduct can subject both the leadership of an entity and the entity itself to liability.

2.5 Mutual Legal Assistance Treaties and Cross-Border Co-operation

DOJ co-ordination with foreign counterparts has increased in recent years, particularly with respect to enforcement of the FCPA. The US has Mutual Legal Assistance Treaties with many countries, allowing prosecutors and regulators to share information and investigative work across borders. The US also has extradition agreements with a number of countries, but the terms of each agreement vary. For example, the US and the European Union allow extradition for all crimes that are punishable in both jurisdictions.

2.6 Prosecution

Prosecutors have broad discretion in choosing whom to prosecute and which charges to bring. That said, both the DOJ and the SEC provide their attorneys with guidance to govern the decision-making process when bringing cases. Prosecutors are also bound by general ethics rules as well as additional requirements to support charges with probable cause and refrain from abusing their discretion.

When deciding whether to criminally prosecute entities, DOJ prosecutors weigh various culpability factors, pursuant to the DOJ guidance entitled the "Principles of Federal Prosecution of Business Organizations", also known as the "Filip Factors" (named for then-Deputy Attorney General Mark Filip), including:

- the nature and seriousness of the offence;
- the pervasiveness of wrongdoing;
- the corporation's history of similar misconduct;
- any co-operation from the corporation;
- the adequacy of the corporation's compliance regime;
- whether the corporation voluntarily and quickly disclosed problems to authorities;
- the corporation's remedial actions;
- collateral consequences of prosecution for employees, stakeholders or the public;
- the adequacy of the prosecution of individuals;
- the interests of any victims; and
- the adequacy of alternate remedies and whether the corporation obstructed the investigation.

Similarly, the SEC issued its Seaboard Report in 2001, which outlined elements of corporate conduct that can play a significant role in whether the Commission pursues an enforcement action. As per the so-called Seaboard Factors, charges against a corporate defendant may be reduced when the company can demonstrate:

- co-operation;
- remediation;
- self-policing; and/or
- self-reporting.

Prosecutors may charge by indictment, information or complaint. Criminal indictments must be approved by a grand jury – which nearly always approve prosecutors' requests. Criminal complaints must set forth adequate probable cause for a charge and be signed by a judge. Complaints provide authority for an arrest but must be followed by an information or indictment within a set period. For felony violations, a defendant has a waivable right under the Constitution to indictment by a grand jury, which, if

waived, can result in the filing of an information detailing the charge.

2.7 Deferred Prosecution

Deferred prosecution agreements (DPAs) and non-prosecution agreements (NPAs) are mechanisms by which a company or individual can avoid prosecution in exchange for a commitment to abide by the terms of an arrangement for a period of time. If the signatory successfully complies with the terms of the agreement, the government will either:

- not file charges (NPAs); or
- move to dismiss the charges, without the signatory being subject to trial (DPAs).

Consequences for breaching these arrangements can be severe. The government may extend the company's obligations under the agreement, or otherwise it may terminate the agreement and prosecute the company.

Recently, DPAs have been the mechanism most used by the DOJ in corporate criminal cases; NPAs are less common. Negotiation for DPAs and NPAs takes place between the prosecution and the defendant.

For federal criminal cases, the DOJ provides guidance on when DPAs and NPAs may be used. For example, prosecutors traditionally offer DPAs or NPAs where "the collateral consequences of a corporate conviction for innocent third parties would be significant". However, individual prosecutors and their supervisors have great latitude to pursue DPAs and NPAs, and to craft the terms of the agreements.

DOJ guidance provides that conditions contained within the agreements should be "designed, among other things, to promote compliance with applicable law and to prevent recidivism". Such conditions may include an acknowledgment of wrongdoing or admitting relevant facts, co-operation in ongoing investigations (including of culpable individuals), the establishment of a corporate monitor to supervise a defendant's compliance, ongoing reporting obligations, fines, and penalties or business reforms.

DPAs and NPAs typically grant prosecutors significant oversight of and leverage over entities, and entities can employ internal or third-party investigators to collect compliance information and report to the government.

Courts must approve DPAs but tend to have very limited involvement. Courts are not involved in approving NPAs.

2.8 Plea Agreements

Plea agreements allow defendants, both individual and corporate, to acknowledge wrongdoing voluntarily in exchange for lesser penalties or convictions on potentially reduced charges. Plea agreements also offer entities and individuals predictability in outcomes and penalties that trials do not. Defendants may plead guilty to one type of charge in exchange for the dismissal of other types of charges or of other counts of the same charge. Defendants may also plead guilty without receiving reduced charges in exchange for a recommendation from prosecutors for a reduced sentence. Sentencing recommendations from prosecutors are not binding on courts, however, and all sentences are determined by a judge. For these and other reasons, plea agreements (as opposed to trials) are commonly used to resolve criminal cases in the US.

At the federal level, plea agreement procedures are governed by Rule 11 of the Federal Rules of Criminal Procedure. Defendants must admit

to sufficient facts to prove each element of the crime to which they are pleading, as well as the crime itself.

Plea agreement policy varies among prosecutors' offices, although all federal prosecutors are guided by ethical and policy guidance promulgated by the DOJ. In addition, federal and state prosecutors follow common charging and plea practices established for their various offices, which tend to be recorded in confidential internal guidance.

3. White-Collar Offences

3.1 Criminal Company Law and Corporate Fraud

In addition to the crimes described throughout **3. White-Collar Offences**, RICO criminalises conduct that is part of a "pattern of racketeering activity" to carry out the goals of an enterprise. "Racketeering activity" includes fraud and the obstruction of law enforcement. Officers and employees can be liable under RICO.

RICO cases may be brought civilly or criminally. Individuals face imprisonment of up to 20 years, a USD250,000 fine and forfeiture of any property derived from the unlawful activity. Defendants may also face treble damages and be liable for reasonable attorney fees in civil cases.

3.2 Bribery, Influence Peddling and Related Offences

Both federal and state law prohibit domestic bribery, but state laws vary by jurisdiction. The general federal bribery statute punishes giving or receiving anything of value to or from a public official to influence official acts (18 USC § 201(b)). Prosecutors must prove that the defendant gave, offered or promised something of value to someone who was a public official and that the defendant had corrupt intent to influence an official act. The key to a successful prosecution is showing a quid pro quo – that the thing of value was given in exchange for the official act. Direct evidence of a quid pro quo is not required. Courts construe "public official" and "thing of value" broadly.

A similar law prohibits the bribery of many state and local officials. Specifically, federal law prohibits bribing agents of an organisation, state or local government or agency with anything of value worth at least USD5,000 when the subject organisation receives at least USD10,000 in federal programme funds annually (18 USC § 666). No federal funds need to be implicated in the bribery for conviction. The statute provides a safe harbour for bona fide salary, wages, fees or other compensation from the usual course of business (18 USC § 666(c)).

The FCPA criminalises bribery of foreign officials. A prosecutor must prove that the defendant made a payment, offer or promise to pay anything of value:

- to a foreign government official or someone who would pass the payment, offer or promise to the official;
- with corrupt intent;
- for the purpose of influencing the official's acts or decisions, or inducing the official to influence other official acts or securing an improper advantage; and
- to acquire or retain business, or to direct it to someone.

The FCPA applies to individuals and entities with formal ties to the US, including but not limited to:

- US citizens and residents;

- "issuers" that have a registered class of securities or are required to file periodic or other reports with the SEC;
- entities organised under federal or state law within the US; and
- entities whose principal place of business is in the US.

The FCPA also applies to anyone who takes actions in furtherance of an FCPA violation while within the US.

There is no de minimis defence to an FCPA violation, and a bribe need not actually be paid. The mere offer of payment incurs liability. There is a limited safe harbour for "facilitation" payments that merely encourage a government official to perform a routine governmental action, such as processing visas or scheduling inspections.

The SEC investigates and brings civil enforcement actions under the FCPA. The SEC can seek civil monetary penalties from entities of up to USD500,000 and from individuals of up to USD100,000 per violation based on the gross amount of monetary gain to the defendant as a result of the violation.

The DOJ can bring criminal and civil prosecutions under the FCPA. In criminal prosecutions, individuals face imprisonment of up to five years, fines up to USD250,000 per violation, or both. Individuals' fines may not be paid by the culpable entity. Entities can face criminal fines of up to USD2 million per violation. As with other federal criminal offences (including many set forth throughout **3. White-Collar Offences**), the alternative fines provision specifies that an individual or entity can alternatively be criminally fined up to twice the gross monetary gain or loss resulting from the violation if that figure is greater than the otherwise applicable fine amount (18 USC § 3571(d)). In civil prosecutions, individuals and entities can be fined up to USD10,000 in an action brought by the DOJ. Importantly, an entity may be required to disgorge ill-gotten gains (ie, net profits obtained as a result of the bribery scheme), which could total billions of dollars.

A "wilful" FCPA violation in a criminal case carries a fine of up to USD25 million for entities or USD5 million for individuals. Individuals face imprisonment of up to 20 years. Violations must be knowing in order to incur criminal liability. FCPA violations may also trigger exclusion from federal programmes or suspension or debarment within the securities industry.

Bribery of foreign non-governmental officials is also prohibited under the Travel Act (18 USC § 1952), which criminalises interstate travel or foreign commerce or using interstate facilities, such as the mail, in furtherance of an unlawful activity.

3.3 Anti-bribery Regulation

The FCPA contains provisions that require entities to keep accurate records and to create internal accounting controls to reasonably verify financial statements. Sarbanes-Oxley requires officers to certify the integrity of company financial statements and to assess internal controls. These provisions are discussed in **3.6 Financial Record-Keeping**.

As described in **3.2 Bribery, Influence Peddling and Related Offences**, the SEC typically investigates and brings civil enforcement actions under the FCPA, and the DOJ brings criminal prosecutions.

3.4 Insider Dealing, Market Abuse and Criminal Banking Law

Federal law prohibits corporate insiders from using material and non-public information

(MNPI) to their advantage or passing that information to outsiders, known as "tipping". Both the giver and the receiver of the information are liable. Federal law also prohibits corporate outsiders from misappropriating and trading based on MNPI in breach of a duty of confidence or trust. Liability of a corporate outsider is premised upon whether the source or "tipper" disclosed the information with an expectation of confidentiality – ie, with the expectation that such information would not be shared with other parties.

The SEC holds authority under Section 10(b) of the Securities Exchange Act and Rule 10b-5 to bring a civil action for insider trading for injunctive relief and disgorgement of profits. In addition, the Insider Trading Sanctions Act and Insider Trading and Securities Fraud Enforcement Act allow the SEC to seek civil penalties of up to three times the profits gained or losses avoided from insider trading (15 USC § 78u et seq).

Private persons who traded at the same time and in the same securities as defendants can also bring an insider trading case under Section 20A of the Securities Exchange Act.

Under Section 32(a) of the Securities Exchange Act, individual insider trading defendants face criminal fines of up to USD5 million and 20 years of imprisonment. Entities that are liable as controlling persons for their employees face fines of up to USD25 million. Insider trading defendants can also be charged with wire fraud (18 USC § 1343), which is punishable by up to 20 years in prison.

3.5 Tax Fraud

Under the Internal Revenue Code, multiple criminal statutes concern omission, evasion and false statements regarding the filing and paying of taxes (IRC §§ 7201-7216). Criminal enforcement of the tax code is accomplished through the IRS's Criminal Investigation division and the DOJ's Tax Division. IRS civil actions can proceed at the same time as a criminal investigation.

Tax Evasion

The elements of tax evasion under 26 USC § 7201 are wilfulness, the existence of a tax deficiency and an affirmative act constituting an evasion or attempted evasion of the tax. The government bears the burden of proving all elements of tax evasion beyond a reasonable doubt. Filing a false return or failing to file a return can constitute evasion if the acts were wilful and resulted in tax evasion. Making a false statement to an IRS agent or concealing assets can also be charged as tax evasion. Participating in the filing of a bankruptcy petition containing false statements of indebtedness, and thereby intentionally stalling tax collection, can also be punished as attempted tax evasion. Conviction results in a fine of up to USD100,000 (USD500,000 in the case of a corporation) or imprisonment of not more than five years, or both, together with the costs of prosecution.

Assistance With False Returns

A person is guilty of a felony under IRC § 7206(1) if they wilfully make and subscribe to a tax return, verified by a written declaration that is made under penalties of perjury, that they do not believe to be true and correct as to every material matter. Those convicted are subject to fines of not more than USD100,000 (USD500,000 in the case of a corporation) or imprisonment of not more than three years, or both, together with the costs of prosecution (26 USC § 7206).

Concealment of Assets

A person is guilty of concealing assets under IRC § 7206(2) if the defendant wilfully aided, assist-

ed, procured, counselled, advised or caused the preparation and presentation of a return that was fraudulent or false as to a material matter. To convict, the government must prove the defendant acted with specific intent to defraud the government in the enforcement of its tax laws. Those convicted are subject to fines of not more than USD100,000 (USD500,000 in the case of a corporation) or imprisonment of not more than three years, or both, together with the costs of prosecution (26 USC § 7206).

3.6 Financial Record-Keeping

The FCPA

As noted in **3.2 Bribery, Influence Peddling and Related Offences** and **3.3 Anti-bribery Regulation**, the FCPA requires "issuers" that have a registered class of securities or that are required to file periodic or other reports with the SEC to keep accurate records and create internal accounting controls to reasonably verify financial statements.

Under the FCPA's books and records provision, issuers must "make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer" (15 USC § 78m(b)(2)(A)). "Reasonable detail" means "such level of detail and degree of assurance as would satisfy prudent officials in the conduct of their own affairs" (15 USC § 78m(b)(7)).

Under the FCPA's internal controls provision, issuers must devise and maintain a system of internal accounting controls that provide reasonable assurances that transactions are authorised by management and recorded as necessary to permit the preparation of financial statements in conformity with generally accepted accounting principles (15 USC § 78m(b)(2)(B)(i)-(ii)). Issuers are also required to maintain accountability for assets, including restricting access to assets unless authorised by management (15 USC § 78m(b)(2)(B)(iii)). Finally, issuers must have adequate internal controls to make sure recorded assets are compared with the existing assets at reasonable intervals and that appropriate action is taken with respect to any differences (15 USC § 78m(b)(2)(B)(iv)).

An issuer must act knowingly to violate the statute. The FCPA imposes criminal liability only when the party knowingly circumvents or knowingly fails to implement a system of internal accounting controls, or knowingly falsifies books or records (15 USC § 78m(b)(5)).

The SEC has two additional rules to aid in the enforcement of the FCPA's record-keeping provisions:

- no person shall directly or indirectly falsify any book, record or account; and
- officers and directors of issuers are prohibited from making material misrepresentations or omissions in the preparation of reports (17 CFR § 240.13b2-1; 17 CFR § 240.13b2-2).

Individuals who wilfully violate the FCPA face a maximum fine of USD5 million or imprisonment of not more than 20 years, or both; entities that wilfully violate the FCPA face fines up to USD25 million (15 USC § 78ff(a)).

Securities Fraud

Under Sarbanes-Oxley, it is a felony to knowingly execute, or attempt to execute, a scheme or artifice to defraud any person in connection with any security of an issuer that has a registered class of securities or is required to file periodic or other reports with the SEC. The penalty for violations of the law can include a fine or

imprisonment of not more than 25 years, or both (18 USC § 1348).

Sarbanes-Oxley also requires financial statements to be filed periodically with the SEC, and that the submissions are accompanied by written certifications from the company's CEO and CFO (18 USC § 1350). The penalties under this provision for CEOs and chief financial officers (CFOs) who certify statements knowing that the periodic report violates the requirements are fines of up to USD1 million and imprisonment for ten years. If the conduct is found to be wilful, the maximum fine increases to USD5 million and the prison term increases to up to 20 years (18 USC § 1350).

Sarbanes-Oxley also contains an executive clawback provision requiring CEOs and CFOs of issuers that are "required to prepare an accounting restatement due to the material noncompliance of the issuer" with "any financial reporting requirement" under the federal securities laws, "as a result of misconduct", to forfeit for a 12-month period their bonus, certain other compensation and profits from the sale of company stock (15 USC § 7243(a)).

Other Financial Fraud

A variety of financial or accounting frauds may be prosecuted federally as instances of mail, wire or bank fraud. The mail fraud statute prohibits using the mail to execute a scheme intended to defraud others (18 USC § 1341). Similarly, the wire fraud statute prohibits making an interstate telephone call or electronic communication, including a transfer of funds, in furtherance of a scheme to defraud (18 USC § 1343). The bank fraud statute criminalises executing a scheme to defraud a financial institution insured by the Federal Deposit Insurance Corporation or to obtain any assets under the control of such an institution (18 USC § 1344). Mail, wire or bank fraud violators must knowingly devise a scheme to defraud others through materially false or fraudulent pretences, representations or promises, and must act with the intent to defraud.

Individuals who violate the mail or wire fraud statutes face up to 20 years' imprisonment and a USD250,000 fine, and entities face up to a USD500,000 fine, for each charged mailing or wire. Mail, wire and bank fraud violators face 30 years' imprisonment and a USD1 million fine if the fraud affected a financial institution.

3.7 Cartels and Criminal Competition Law

The Antitrust Division of the DOJ enforces federal criminal competition laws and is taking an increasingly aggressive stance. Fines for antitrust violations continue to grow.

The Sherman Act

The Sherman Antitrust Act (Sherman Act) is a federal statute that outlaws contracts, conspiracies or combinations of business interests in restraint of foreign or interstate trade (15 USC § 1). Federal courts evaluate most antitrust claims under a so-called "rule of reason", which requires proof that a defendant with market power unreasonably engaged in anti-competitive conduct. Examples of practices that might be evaluated for reasonableness include:

- sharing competitive information;
- tying arrangements (where the availability of one item is conditioned upon agreement to purchase another item); or
- exclusive dealing arrangements (where a buyer or seller agrees to sell to, or purchase from, only one particular buyer or seller).

In contrast, "per se" violations of the Sherman Act involve a class of anti-competitive arrangements that are considered illegal on their face (such as an agreement among competitors to fix prices, divide markets or rig bids).

The Sherman Act also prohibits the monopolising of trade or commerce among states or with other countries (15 USC § 2). The elements of such a violation are possession of or attempt to possess monopoly power in the relevant market and wilfully acquiring or maintaining that power, as opposed to growth resulting from a superior product, business strategy or historic accident.

The Sherman Act imposes criminal penalties of up to USD100 million for corporations or USD1 million for individuals, or imprisonment of up to ten years, or both. The DOJ, state Attorneys General and private parties can also bring civil actions and win damages of three times the injuries sustained.

The Clayton Act

The Clayton Act prohibits a seller from discriminating in price between purchasers of goods of similar quality when doing so may result in substantial competitive injury, and from making promotional payments or services available only to some customers (15 USC § 13a). Violators face fines of USD5,000 and imprisonment of a year.

Section 7 of the Clayton Act prohibits any merger or acquisition that will result in substantially less competition or a monopoly within a relevant market (15 USC § 18). The DOJ and FTC are both authorised to enforce Section 7, and private parties may also seek injunctive relief against a transaction that would result in a Section 7 violation (15 USC § 26).

The Clayton Act is enforceable by both the DOJ, which enforces it through civil actions in federal courts, and the FTC, which primarily enforces it through administrative proceedings before the agency itself (15 USC §§ 21, 25 and 53(b)). The FTC can also seek injunctive relief in federal court.

3.8 Consumer Criminal Law

The FTC's Bureau of Consumer Protection regulates business practices including advertising and financial practices, data security, hi-tech fraud and telemarketing. The FTC investigates and brings civil actions against violators and also co-ordinates with the DOJ and state prosecutors to bring criminal suits.

The Consumer Financial Protection Bureau, the US Food and Drug Administration and the DOJ also enforce various consumer protection laws, including:

- the Consumer Financial Protection Act;
- the Fair Debt Collection Practices Act;
- the Fair Credit Reporting Act;
- the Truth in Lending Act;
- the Gramm-Leach-Bliley Act; and
- the Food, Drug and Cosmetic Act.

State Attorneys General prosecute consumer fraud violations under a variety of state laws. Many states have adopted the Uniform Deceptive Trade Practices Act, which prohibits fraudulent business practices and misleading advertising.

3.9 Cybercrimes, Computer Fraud and Protection of Company Secrets

The Computer Fraud and Abuse Act prohibits intentionally obtaining access to computers "without authorisation" or by "exceeding authorised access" with the intent to defraud, cause

damage or extort (18 USC § 1030). Sanctions include up to ten years' imprisonment and a USD250,000 fine.

The Stored Communications Act prohibits intentionally accessing email or voicemail without authorisation or in a way that exceeded authorised access (18 USC § 2701). Sanctions include up to five years' imprisonment and a USD250,000 fine, or ten years for subsequent offences.

Wire fraud prohibits schemes to defraud that use wire, radio or television communication (18 USC § 1343). Prosecutors may charge other computer fraud violations (which have similar elements) as wire fraud due to the wire fraud statute's higher penalties, including fines up to USD1 million and imprisonment for up to 30 years if the fraud affects a financial institution.

The Wiretap Act prohibits intentionally intercepting or endeavouring to intercept communications without consent from the speaker (18 USC § 2511). Violators face a USD250,000 fine and up to five years' imprisonment.

The Theft of Trade Secrets statute prohibits the theft of trade secrets and the knowing possession or use of stolen trade secrets (18 USC § 1832). Violators are subject to fines of up to USD5 million or three times the value of the stolen trade secret. Related criminal laws prohibit economic espionage (18 USC § 1831) and the wilful infringement of copyright for the purpose of commercial advantage or private financial gain (17 USC § 506(a); 18 USC § 2319).

3.10 Financial/Trade/Customs Sanctions

OFAC enforces economic and trade sanctions against countries, entities and individuals who engage in certain prohibited transactions. Prohibited transactions are designated based on US foreign policy or national security interests. For example, OFAC sanctions the transfer of assets to, or trade with, certain countries, and maintains a list of "blocked" persons with whom US entities or individuals cannot conduct any business. OFAC can take administrative actions such as licence denial, imposing a civil monetary penalty for violations and referring violations for possible criminal prosecution.

Smuggling and other importation violations are crimes under 18 USC §§ 541, 542, 544 and 545. Smuggling is knowingly and clandestinely bringing goods into the US with the intent to defraud the government by failing to properly declare the goods. Prosecutors must prove intent for a smuggling conviction. The punishment for smuggling is a fine of up to USD250,000 and imprisonment of up to 20 years. In addition, the defendant forfeits the merchandise smuggled, or its value.

3.11 Concealment

Defendants can incur liability for both concealment and an underlying offence. State and federal laws criminalise efforts to conceal wrongdoing improperly, which are generally referred to as obstruction of justice.

The provision in 18 USC § 1503 punishes corrupt attempts to obstruct the "due administration of justice" in connection with a pending judicial proceeding. Violators face up to ten years' imprisonment and a USD250,000 fine.

Similarly, 18 USC § 1505 punishes attempts to impede the "due and proper administration of the law" in any proceeding before a US agency, department or committee, including Congress. Violators face up to five years' imprison-

ment, or eight years' in terrorism cases, and a USD250,000 fine.

Even when the offences are not charged separately, prosecutors and regulators consider efforts to conceal wrongdoing to be aggravating factors in charging and sentencing.

Federal law prohibits making false statements to the government, including by misleading misrepresentations (18 USC § 1001). The government must prove that the defendant made a statement or representation that was:

- false;
- made knowingly and wilfully;
- material; and
- made within the federal government's jurisdiction.

Courts may fine guilty parties USD250,000 and imprison them for up to five years, or up to eight years in terrorism cases.

When a person or entity has a duty to disclose facts, such as to maintain accuracy on a government form, a failure to disclose such facts can be a basis for liability.

3.12 Aiding and Abetting

Both state and federal courts recognise liability for aiding and abetting, although state laws may vary from federal law. A director, officer or employee of a corporation can incur liability for aiding and abetting the commission of a corporate crime. Under federal law, anyone who "aids, abets, counsels, commands, induces or procures" the commission of an offence is punishable in the same manner and to the same extent as the principal actor (18 USC § 2(a)).

Certain actors may also be liable for "causing" another to violate a federal statute. For example, any person or entity who causes another to violate the federal securities laws may also be liable. For such "causing" liability to attach, the SEC must prove three elements:

- a primary violation;
- an act or omission by the respondent that was a cause of the violation; and
- the respondent knew, or should have known, that its conduct would contribute to the violation.

3.13 Money Laundering

The Money Laundering Control Act (18 USC §§ 1956 and 1957) criminalises money laundering. Prosecutors must show that a defendant knowingly transported or transmitted funds between states or between the US and another country, knowing the funds were the proceeds of unlawful activity and knowing the movement was designed to conceal the nature, location or source of the proceeds of the unlawful activity.

The penalty is up to 20 years in prison, a fine of up to USD500,000 or twice the value of the property involved, and the mandatory forfeiture of property involved in the offence or traceable to the offence, or of substitute assets (18 USC § 982(a)(1) & (b)(2)).

Under 18 USC § 1957, liability extends to persons who knowingly engage in monetary transactions that meet three criteria:

- involving property derived from certain criminal activities;
- knowing the property is derived from criminal activities; and
- when the property has a value greater than USD10,000.

Violators face up to ten years' imprisonment and a fine of not more than twice the amount of the criminally derived property involved in the transaction.

In addition, financial institutions have obligations under the Bank Secrecy Act and related regulations to help detect and report suspicious activity. Specifically, financial institutions must file a currency transaction report for transactions involving more than USD10,000. Courts may punish individuals for structuring transactions to evade the USD10,000 reporting requirement.

Financial institutions must also establish effective programmes to combat money laundering. The Department of the Treasury uses enforcement actions to ensure compliance with the Bank Secrecy Act. The criminal penalty for a wilful violation of the Bank Secrecy Act is a fine of up to USD250,000 and imprisonment for up to five years. A higher penalty may apply if the violation occurs with another crime or as part of a pattern of illegal activity.

4. Defences/Exceptions

4.1 Defences

Common defences to white-collar crimes include the following.

- Evidentiary gaps – the prosecutor has not met its burden to prove each element of the offence beyond a reasonable doubt.
- Lack of intent/acts in good faith – for charges requiring a showing of specific intent or a guilty mind, acts made in good faith or without such intent may provide a defence. Similarly, where knowledge is an element of an offence, demonstrating absence of the relevant knowledge may operate as a defence.
- Lack of jurisdiction/extraterritoriality – the prosecutor does not have the required legal authority or has not established the required nexus to exercise its jurisdiction.
- Coercion and entrapment – a defendant was forced or coerced to perform an illegal act by others. In the same vein, the government may have entrapped the defendant by creating a set of circumstances in which an otherwise law-abiding person would be induced to commit a crime.
- Statute-specific defences – some statutes provide for specific affirmative defences. The FCPA, for example, allows defendants to show that a payment or promise was lawful under the local law where it was made (15 USC § 78dd-1(c)(1)). Similarly, under the FCPA's accounting provisions, adequate internal controls will safeguard an entity (15 USC § 78m(b)(2)).
- Conduct was authorised – an entity may argue that it was authorised or licensed to conduct certain activity, or that its activity was not prohibited.

An effective compliance programme is not a defence to criminal charges, but agencies view an effective compliance programme as a mitigating factor weighing against prosecution or enforcement actions.

4.2 Exceptions

No industry or sector is exempt from compliance with white-collar crime-related laws. Exceptions to white-collar offences exist under statute-specific provisions. For example, the FCPA contains an exception for so-called "grease payments" used to expedite or secure the performance of routine governmental actions (15 USC § 78dd-1(b)). However, courts and regulators construe the exception narrowly, and payments typically involve small amounts. No de minimis excep-

tions exist under the FCPA or other white-collar fraud statutes.

4.3 Co-operation, Self-Disclosure and Leniency

Voluntary self-disclosure and meaningful co-operation with investigators are considered mitigating factors by agencies and prosecutors. Other common leniency measures include remediation efforts, the mitigation of possible harm, restitution and reform (including changes in internal policies). The payment of restitution in advance of enforcement action also demonstrates a corporation's acceptance of responsibility.

Examples of proactive steps that legal counsel can take to receive co-operation credit include:

- flagging key documents and making witnesses available on an expedited basis;
- offering translations of documents where necessary;
- providing informed factual explanations outside of mere advocacy; and
- helping clients who may have violated the law to admit that violation and work in good faith to remedy it.

4.4 Whistle-Blower Protection

Whistle-blowers have express protection against retaliation by employers under several statutes relevant to white-collar offences, including the False Claims Act (FCA) (31 USC § 3730(h)), Sarbanes-Oxley and the Dodd-Frank Act (15 USC § 78u-6).

Under the FCA, an employer may not take an adverse employment action against an employee for providing a tip to a regulator nor for assisting in a regulatory investigation. Under Sarbanes-Oxley, whistle-blowers may even pursue reinstatement, back pay and other compensation from the Department of Labor.

The identity of a whistle-blower is also protected by statute. For example, under the Dodd-Frank Act, the SEC may not disclose information that could reasonably be expected to reveal the identity of a whistle-blower, except in limited circumstances.

Large financial incentives exist for whistle-blowers to report white-collar offences. Whistle-blowers who voluntarily provide the SEC with original, timely and credible information that leads to a successful enforcement action in which the monetary sanctions exceed USD1 million may be eligible for an award of 10% to 30% of the money collected. The FCA provides for awards between 15% and 30% of the proceeds of the action or settlement of the claim.

Typically, whistle-blowers are protected by companies through specific whistle-blower policies or company ethics codes that provide permutations of the following.

- The entity will protect individuals who make good-faith reports of possible violations, even where these reports are mistaken. The entity will protect good-faith reporters from retaliation, harassment or other adverse employment consequences.
- A whistle-blower may report potential misconduct on a confidential or anonymous basis via email or a hotline.
- Companies may give whistle-blowers access to confidential advice from an independent body.
- An employee who retaliates against a possible whistle-blower may be subject to disciplinary action, including termination of employment. Employees who believe they have been

subject to retaliation or reprisal are encouraged to report retaliation.

Companies should never prohibit or discourage an employee from sharing information with the SEC, and should not impose overly broad confidentiality obligations that could reasonably be interpreted to prevent employees from sharing information with the SEC. The federal securities laws prohibit any person from "imped(ing) an individual from communicating directly with the (SEC) about a possible securities law violation" (17 CFR § 240.21F–17(a)). The SEC has taken an expansive view of that rule and brought enforcement actions against companies based upon only the inclusion of certain provisions in confidentiality or other agreements, even in matters in which the company did not affirmatively seek to enforce those provisions.

5. Burden of Proof and Assessment of Penalties

5.1 Burden of Proof

The government has the burden of proof for criminal offences and must prove each element of a crime beyond a reasonable doubt. There is a presumption of innocence in all criminal cases.

In civil cases and administrative proceedings, plaintiffs have the burden of proof and must generally show the validity of their claims by a preponderance of the evidence, meaning that a fact is more likely than not. In some administrative proceedings, plaintiffs must establish substantial evidence of their claims.

Defendants have the burden of proving any affirmative defences, usually by clear and convincing evidence or preponderance of the evidence.

5.2 Assessment of Penalties

For both individual and institutional defendants in federal criminal courts, the guidelines of the United States Sentencing Commission provide a uniform framework for recommending sentences and fines. Each offence has a pre-determined level. Judges weigh aggravating and mitigating factors, including an individual defendant's criminal history, to calculate a recommended sentencing range or fine. The guidelines set forth the rules for punishing entities. Restitution for identifiable victims is mandatory.

The guidelines shape federal judges' sentencing decisions but are not binding, and judges may vary from the guidelines range. In particular, judges are directed under 18 USC § 3553 to consider the following for each individual defendant:

- the nature and circumstances of the offence, and the history and characteristics of the defendant;
- the need to reflect the seriousness of the offence, promote respect for the law and provide just punishment;
- the need to afford adequate deterrence to criminal conduct;
- the need to protect the public from further crimes;
- the need to provide the defendant with necessary training or treatment;
- the need to avoid unwarranted disparities among defendants with similar conduct; and
- the need to provide restitution to victims.

For institutional defendants, the guidelines set forth culpability factors that determine appropriate multipliers applied to a base fine for determining an applicable fine range.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global 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 Katie.Burrington@chambers.com