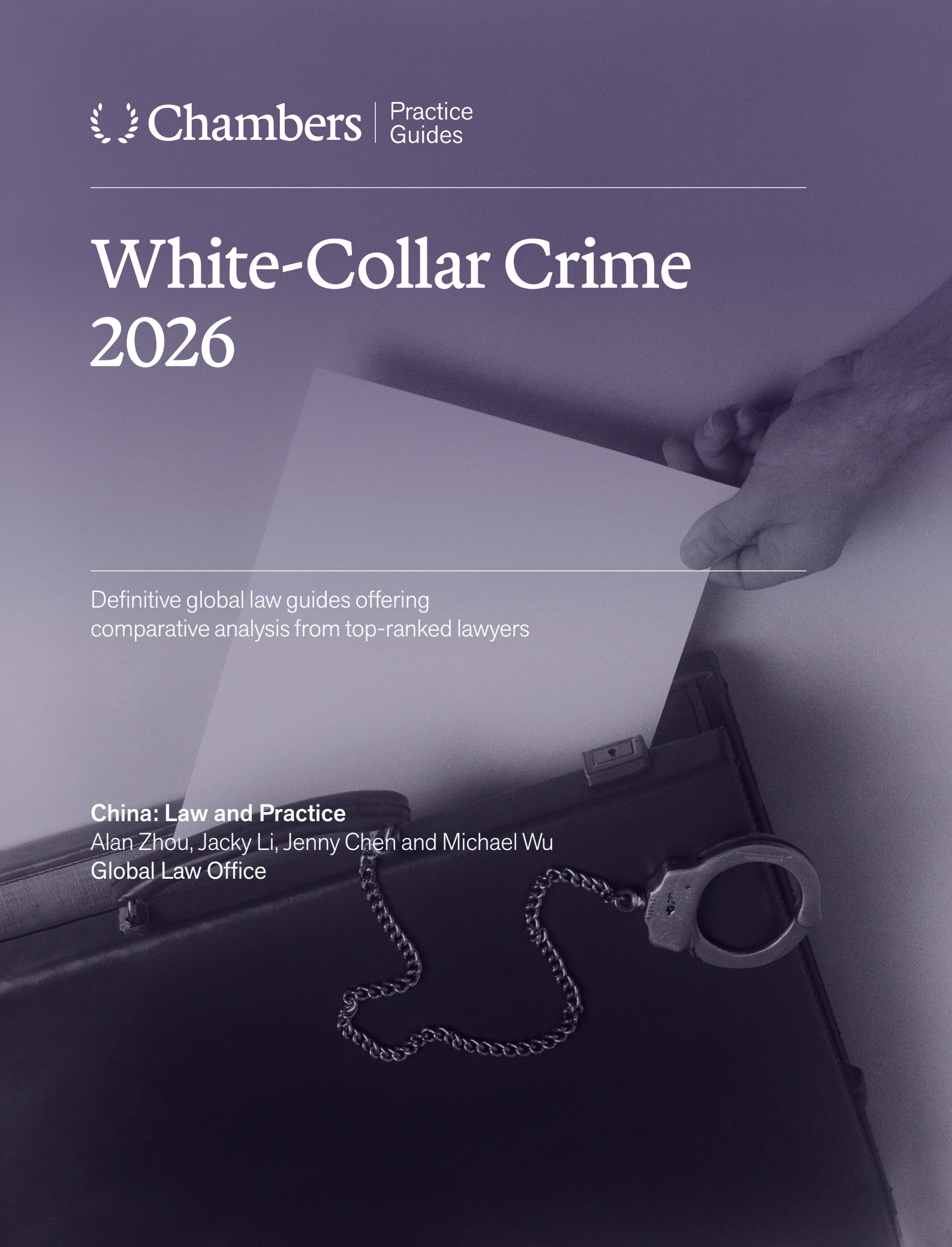
Chambers | Practice Guides

White-Collar Crime 2026

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



China: Law and Practice

Alan Zhou, Jacky Li, Jenny Chen and Michael Wu
Global Law Office

CHINA

Law and Practice

Contributed by:
Alan Zhou, Jacky Li, Jenny Chen and Michael Wu
Global Law Office

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.5
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.6
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.8
2.4 Use of Technology in Investigations p.8
2.5 Internal Investigations p.8
2.6 Prosecution p.9
2.7 Deferred Prosecution p.9

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

4. Pleas and Defences P.15
4.1 White-Collar Defences p.15
4.2 De Minimis p.15
4.3 Plea Agreements, Co-Operation, Self-Disclosure and Leniency p.15
4.4 Whistle-Blower Protection p.16
4.5 Cross-Border Defence Strategies p.16

5. Key Trends and Future Outlook P.16
5.1 The Year Ahead p.16

Global Law Office dates back to the establishment of the Legal Consultant Office of China Council for the Promotion of International Trade (CCPIT) in 1979, when it became the first Chinese law firm approved by the PRC government, and has retained the privilege of clients' trust in various areas over four decades. The firm has offices in Shanghai, Beijing, Shenzhen and Chengdu, with 160 partners and over 600 lawyers across China. The firm is experienced in meeting all public and private enterprises' regulatory compliance needs, including risk assessment, compliance policy, reporting, training and investigation. The firm has resolved dozens of government investigation cases relating to anti-corruption, antitrust, promotion and advertising, insider trading, and food and drug safety, as well as cross-border investigations in multiple jurisdictions.

Authors



Alan Zhou is head of the compliance practice of Global Law Office. Based in Shanghai, his practice focuses on general corporate, transactions, compliance and risk control. An expert on legal issues surrounding compliance and M&A in China, Mr Zhou has extensive experience in resolving complex and challenging issues, and in advising on creative and strategic solutions. He has a particularly strong background in the life sciences and healthcare industries. As a participant or as an external counsel, Mr Zhou has been engaged by local authorities and industrial associations for advice on legislation and industrial standards related to online hospitals, digital marketing, medical insurance reform, medical representative management and other compliance matters.



Jacky Li is a partner at Global Law Office. He is an attorney-at-law in the PRC and California, a US ACFE-certified fraud examiner and a contributing expert for the UK's The Law Reviews. He focuses primarily on regulatory compliance, corporate and government investigations, dispute resolution and litigation, healthcare and life sciences. Mr Li is an expert member of the National Corporation Compliance Committee of CCPIT, the Compliance Management Committee of CPIA and the Shanghai Elite Legal Professional Experts Pool. He also serves as the deputy chief of the Corporate Compliance Committee of the Shanghai Bar Association.



Jenny Chen is a partner at Global Law Office, based in Shanghai, who focuses mainly on compliance, government investigations, internal investigations and data security. She is well versed in conducting investigations into anti-corruption, the FCPA, data falsification, financial fraud, occupational embezzlement, self-dealing and trade secrets, from Chinese and relevant foreign law perspectives. Ms Chen has extensive experience in cybersecurity and data compliance, assisting numerous large enterprises in identifying and responding to potential cybersecurity risks and incidents, and establishing data compliance management systems and structures. She has handled multiple large-scale projects in e-discovery, cross-border data protection and security, providing comprehensive compliance solutions to clients.



Michael Wu is a senior associate at Global Law Office. His practice focuses on general corporate, compliance and risk control, with professional knowledge and practical experience in medical services, drugs, medical devices, and health management. Mr Wu has participated in internal compliance investigations and provided legal advice on the administration of advertisements, and on unfair competition and anti-bribery matters. He has served multinational corporations in general corporate affairs and in the establishment of compliance systems in areas such as clinical trials, procurement and supplier management, distribution, pharmacovigilance, licensing, and foreign investment.

Global Law Office

35th and 36th Floors, One ICC
Shanghai ICC 999
Middle Huai Hai Road
Xuhui District
Shanghai 200031
PRC

Tel: +86 21 2310 8211
Fax: +86 21 2310 8299
Email: alanzhou@glo.com.cn
Web: www.glo.com

1. Criminal Law

1.1 Criminal Offences

Criminal offences are defined in the Criminal Law of the People's Republic of China ("the Criminal Law") and are generally categorised by the nature of the protected legal interest, including crimes related to bribery and corruption, fraud, money laundering, tax evasion, market manipulation and trade secrets.

An offence is constituted where the statutory elements are met, typically involving:

- a protected legal interest;
- objective conduct causing harm;
- the subject (a natural person or legal entity); and
- subjective fault (intent or negligence).

Most white-collar offences require intent, while negligence is punishable only where expressly provided by law. Motive, while often irrelevant for the constitution of a crime, is a critical factor in sentencing. In addition, according to Article 23 of the Criminal Law, a person may be held liable for an attempted offence if the crime was not completed due to external factors. Penalties for an attempted offence are typically lighter than for a completed crime.

1.2 Burden of Proof

Under the Criminal Procedure Law and relevant Supreme Court judicial interpretations, the burden of proof for the guilt of the defendant in a public prosecution case rests with the public prosecutors, while in a private prosecution case it lies with the individual or entity that commenced the private prosecution. Such cases are limited to those that are to be handled only upon complaint (such as insult, defamation and embezzlement cases), minor cases supported by the victim's evidence (such as manufacturing or selling counterfeit goods and intellectual property infringement cases) and cases where the Public Security Bureau (PSB) or Procuratorate has declined to pursue criminal liability despite evidence showing criminal infringement of the victim's personal or property rights.

For special crimes, the burden of proof is shifted, and the defendant needs to provide evidence for certain constituent elements. For example, in a crime involving an unidentified source of a huge amount of property, the defendant needs to prove the legal source of the property. For the crime of illegally holding state top-secret and confidential documents, materials and articles, the defendant needs to prove the source and purpose of the relevant documents and articles. In addition, the defendant has the right to raise any affirmative defences and shall bear the burden of proof in this respect. This includes circumstances that may exempt or mitigate criminal liability, such as justifiable defence, emergency avoidance, exceeding the limitations period and being incapable of criminal responsibility.

Pursuant to the Criminal Procedure Law, the standard of proof is confirmative and adequate evidence, which means:

- the facts of the conviction and sentence are proved by evidence;

- the evidence on which the case is based has been verified by legal procedures; and
- the facts found have been proved beyond reasonable doubt.

1.3 Statute of Limitations

Under the Criminal Law, limitation periods are determined by the maximum statutory penalty applicable to the offence and shall be calculated from the date when the crime is completed. The limitation periods are tiered, with the maximum period being 20 years, applicable to crimes for which the maximum legally prescribed punishment is life imprisonment or the death penalty. For offences with lower statutory penalties, shorter periods apply. For instance, for the crime of offering bribery to state functionaries, the period is further divided into three limitation periods (three years, ten years and 20 years) corresponding to the applicable sentencing range.

Expiry of the limitation period does not necessarily preclude prosecution. For instance, for a crime for which the maximum statutory punishment is life imprisonment or the death penalty, even if 20 years have elapsed, the criminal suspect may still be prosecuted upon the approval of the Supreme People's Procuratorate. In addition, where a criminal suspect commits another crime before the original limitation period expires, the limitation period for the earlier crime shall also be recalculated from the date of the subsequent crime. Furthermore, under circumstances where a criminal suspect evades investigation after a case has been formally filed by relevant judicial authorities or where a victim brings a complaint against a criminal suspect, the limitation period shall not apply.

1.4 Extraterritorial Reach and Cross-Border Co-Operation

The Criminal Law mainly adopts the principle of territorial jurisdiction over criminal offences, supplemented by extraterritorial jurisdiction in circumstances where the perpetrator is a Chinese citizen or where a foreign national commits a crime against China or a Chinese citizen.

Article 10 of the Criminal Law stipulates the principle of Passive Recognition of Foreign Criminal Judgments, stating that any Chinese citizen who commits a crime outside the territory of China may still be investigated for his or her criminal liabilities under Chinese laws, even if he or she has already been tried in a foreign country. However, if he or she has already received criminal punishment in the foreign country, he or she may be exempted from punishment or given a mitigated punishment.

Article 8 further specifies the principle of protective jurisdiction, under which the Criminal Law applies to foreign nationals committing crimes abroad against China or Chinese citizens, provided that the offence carries a minimum statutory penalty of not less than three years' imprisonment and is also punishable under the law of the place where it was committed.

Notably, in August 2026, China released the Draft Law on Anti-Cross-Border Corruption, which aims to establish a dedicated statutory framework for this purpose, including specific mechanisms for cross-border investigations, mutual legal assistance, fugitive recovery and asset recovery, etc.

China actively engages in international and regional criminal justice co-operation, including through international conventions such as the United Nations Convention against Corruption, and participates in international task forces such as INTERPOL, making use of tools such as Red Notices in pursuing fugitives involved in transnational crimes including corruption, cybercrime and other white-collar and economic offences. Moreover, the enactment of the International Criminal Justice Assistance Law and its implementation rules have further enhanced the fundamental framework of international co-operation in criminal justice. As of August 2026, China has entered extradition treaties and mutual legal assistance treaties on criminal matters with 57 countries.

1.5 Corporate and Personal Liability

Bribery and other white-collar offences committed by an employee of a company could be deemed as either an individual crime or a unit crime, depending on various factors such as:

- whether the conduct was decided or organised by the company;

- whether illicit benefits were obtained by the company; and
- whether the offence was committed in the name of the company.

If the charge is raised against the individual employee, the company would not bear legal liabilities.

However, if the charge is against the company as a unit crime, the so-called "dual punishment system" would apply: the entity is subject to a criminal fine, and the main persons responsible (including the person in charge of the company and other persons directly liable) may also be subject to criminal detention or imprisonment.

In the context of a merger or division, if an entity assumes the rights and obligations of the predecessor entity, the criminal liability of the predecessor entity and the relevant responsible persons shall still be pursued. The predecessor entity shall still be listed as the defendant, and the legal representative or the person chiefly in charge of the new entity that assumes the rights and obligations of the predecessor entity shall be the litigation representative. The successor entity shall bear the criminal liability of the predecessor entity in accordance with the property it inherited.

The Criminal Law does not yet have a standalone "failure to prevent" offence like the UK Bribery Act. However, enforcement trends show that the establishment of a robust and effective compliance programme is increasingly pivotal in assessing whether the offence can be attributed to the company as a unit crime, as it may, on a case-by-case basis, negate or weaken the inference that the conduct reflected the corporate intent.

1.6 Sentencing and Penalties

The Criminal Law clarifies the sentencing ranges for each crime, and relevant judicial interpretations will further specify the criminal threshold in each sentencing range.

The sentence shall be determined by the court based on certain factors, including the facts, nature and circumstances of the crime, and the extent of the harm done to society. In addition, the court shall abide by the principles of legality and suiting the punishment to the crime during the sentencing process. The principle of legality refers to the fact that no-one may be convicted or punished for an act that is not defined as a crime in the specific provisions of the Criminal Law. The principle of suiting the punishment to the crime refers to the concept that the punishment shall be adaptable to the nature and the circumstances of the crime.

Although China does not formally recognise deferred prosecution agreements or non-prosecution agreements, leniency mechanisms exist, including plea leniency mechanism under which criminal suspects and defendants who voluntarily and truthfully admit guilt and accept punishment (plea agreement) may receive significant reductions in their sentence. With respect to other key factors that may be relevant to mitigation, corporate remediation efforts such as repaying taxes returning illicit gains, and implementing a monitored compliance system have also become grounds for leniency in practice.

1.7 Damages and Compensation

Under the Criminal Procedure Law, if the victim suffers material damage due to the defendant's criminal conduct, he or she has the right to bring an incidental civil action during criminal proceedings. If the victim dies or is incapacitated, the victim's legal representative or close relatives have the right to bring an incidental civil action. In addition, if the loss is suffered by the state property or collective property, the Procuratorates may bring an incidental civil action when filing a public prosecution.

Collective redress mechanisms remain limited in China. Class actions are generally not available in criminal cases. A limited form of class action is recognised only in the context of securities-related civil litigation, since the amendment of the Securities Law in 2019, and is confined to claims arising from securities fraud, such as insider trading and market abuse.

2. Enforcement

2.1 White-Collar Enforcement Authorities

White-collar offences not involving public officials shall be investigated and handled by the PSB and transferred to the People's Procuratorate (the "Procuratorate") for

prosecution. White-collar offences involving public officials are investigated by the Supervisory Commission and prosecuted by the Procuratorate. During the review and prosecution stage and thereafter, the Procuratorate may, on its own authority, conduct supplementary investigations when time is critical, or when the investigative authority's efforts have proven ineffective or present a conflict of interest. The suspects are finally found guilty by the court. The authorities responsible for the enforcement of criminal judgments in white-collar offences include the courts, prisons, community correction institutions and the PSB.

Regarding civil enforcement, victims who have sustained material losses resulting from white-collar offences may initiate incidental civil actions during the course of criminal proceedings. In terms of administrative enforcement, although the PSB is categorised as an administrative authority within the Chinese judicial system, it is empowered to investigate white-collar-related crimes. Although other administrative authorities cannot conduct criminal investigations, the evidence obtained during administrative law enforcement can be used in criminal proceedings, and they are obliged to co-operate with the PSB or other investigating authorities in the criminal investigation and provide technical support or advisory assistance.

The PSB has established specialised police units for certain white-collar offences. For instance, the economic investigation departments of the PSB are primarily responsible for crimes such as bribery, money laundering and tax evasion, while the PSB's food, drug and environmental investigation detachments mainly handle intellectual property crimes, environmental crimes, food and drug crimes, etc. Specialised courts or tribunals have also been established to adjudicate certain white-collar offences, including maritime courts, environmental and resources tribunals, and intellectual property tribunals.

Public policy may influence law enforcement. For instance, anti-corruption has consistently been a core area of enforcement, particularly in industries involving public interests and people's livelihoods. Taking the pharmaceutical industry as an example, China has issued notices in recent years requiring the rectification of unethical practices in the industry and launched initiatives such as investigating both bribe-takers and bribe-givers simultaneously. These measures have driven enforcement authorities including Supervisory Commissions, administrations for market regulation, healthcare security administrations and the PSB to continuously strengthen anti-corruption enforcement efforts over the past few years. Official enforcement statistics reflect this ongoing trend of strict enforcement: in the first half of 2026, the Supervisory Commissions placed 19,000 individuals under investigation for bribe-giving and transferred 1,938 individuals to Procuratorate authorities, while the Procuratorates prosecuted 1,410 individuals for bribery offences.

2.2 Initiating an Investigation

The initiation of white-collar investigation involves case acceptance, investigation and verification, case filing and review, etc. The sources of cases may include criminal reporting, accusation and surrender, case transfer from administrative authorities, and criminal clues found by the PSB, the Procuratorate and the Supervisory Commission.

Taking the PSB as an example, the relevant provisions for investigation initiation include the Provisions on the Procedures for Handling Criminal Cases by the PSB and the Provisions on the Division of Criminal Cases under the Jurisdiction of the Ministry of Public Security. According to the relevant regulations, written records shall be made for cases involving reporting, accusation and voluntary surrender, and audio and video recordings can be made when necessary. Cases transferred by other administrative authorities shall be examined within three days. If the facts or clues of the case are found to be unclear, further investigation and verification could be conducted with the approval of the person in charge. If, after examination, it is considered that there are criminal facts that need to be investigated with regard to criminal responsibility, the case shall be filed with the approval of the person in charge of the PSB. If the case is beyond the PSB's jurisdiction, it shall be transferred to the relevant authorities.

Other authorities have similar provisions, including the Rules of Criminal Procedure of the Procuratorate, the Supervision Law, the Implementing Regulations of the Supervision Law, the Rules for the Supervision and Discipline Enforcement of the Discipline Inspec-

tion Organs of the Communist Party of China and the Regulations on Case Inspection of the Discipline Inspection Organs of the Communist Party of China.

2.3 Powers of Investigation

For criminal investigations of white-collar offences, the PSB, the Procuratorate (supplementary investigation) and the Supervisory Commission are empowered to:

- interrogate the criminal suspect;
- interview the witnesses;
- inspect or examine the sites, objects and persons relevant to a crime (including dawn raids);
- search the criminal suspect and his or her belongings and residence, and anyone who might be hiding a criminal or criminal evidence, as well as other relevant places;
- seal up or seize property and documents;
- access or freeze a criminal suspect's deposits, remittance, bonds, stocks, shares, funds or other property; and
- implement technical investigation measures.

Before filing a case, the PSB may, when necessary, investigate and verify the criminal clues and obtain evidence, but may not seal up or detain the investigated object. The Supervisory Commission may adopt a similar preliminary verification method.

After filing a case, the PSB, the Procuratorate (supplementary investigation) and the Supervisory Commission may request relevant entities to submit any relevant documents. Entities have the obligation to hand over material evidence, documentary evidence, audio-visual material, etc, to the extent that such evidence is relevant to proving that the suspect is guilty or innocent. In addition, with the approval of the person in charge of the PSB and other persons in charge, they can search the sites of relevant entities and take the initiative to obtain relevant documents. A search warrant is required for a search, except in case of emergency during arrest or detention.

The Criminal Procedure Law and Supervision Law distinguish two procedures: interrogation of suspects and interview with witnesses. Therefore, an employee, officer or director of a company under investigation, or a third party, remains under an obligation to submit to questioning based on their involvement in the alleged crime.

Pursuant to the relevant provisions of the Criminal Procedure Law, the PSB, the Procuratorate (supplementary investigation) and the Supervisory Commission possess the authority to seal or seize digital assets discovered during investigation that are capable of proving the guilt or innocence of a criminal suspect. Furthermore, based on the exigencies of the case, these authorities may trace and freeze the digital assets of the criminal suspect, a process with which relevant entities and individuals are legally obligated to co-operate.

2.4 Use of Technology in Investigations

In investigations of white-collar offences, the enforcement authorities have widely adopted AI and advanced digital tools (eg, predictive analytics, big data review, blockchain analysis). Although no specific laws or guidelines governing such use have been promulgated to date, relevant provisions are set forth in the Criminal Procedure Law, the Data Security Law, the Personal Information Protection Law, the Provisions on Several Issues Concerning the Collection, Extraction, Review, and Judgment of Electronic Data in Handling Criminal Cases, the Rules on Electronic Data Evidence Collection by PSB in Handling Criminal Cases, etc.

It should be noted that any materials obtained through AI-enhanced investigations must conform to the statutory types of evidence in criminal proceedings, possess legality, authenticity and relevance, and be capable of proving the facts of the case before they can be accepted by enforcement authorities.

2.5 Internal Investigations

In general, conducting internal investigations is not a statutory obligation in China, unless prescribed in the applicable industry-specific legislation (mostly in response to safety incidents). In addition, Chinese authorities (often industry supervision authorities) may initiate enforcement actions and require companies to conduct self-inspections and report non-compliant activities.

In practice, internal investigations are incorporated into the internal control mechanism by companies for

compliance purposes. The cause of the actions varies by company but white-collar crime and fraud (eg, commercial bribery, bid-rigging and embezzlement) are among the focuses for the majority of companies in China.

Commonly, internal investigations are undertaken by in-house counsels in the company or external local counsels, depending on the nature and severity of the issues under investigation. The methodology and process for these internal investigations usually includes document review, financial review and interviews with employees and other personnel. The key issues during internal investigations include:

- identifying the legal issue;
- designing and implementing the analysis process based on the findings; and
- determining the solutions.

Notably, due process and evidence preservation are often overlooked by companies, as it is very likely that the facts and evidence gathered under internal investigation may end up in labour arbitration tribunals or court for litigation purposes – or be submitted to the Chinese authorities. Therefore, how to preserve the integrity of the internal investigation and ensure the admissibility of the evidence should be carefully evaluated during the preparation and implementation of the internal investigation.

In internal company investigations, the Cybersecurity Law, the Civil Code and the Personal Information Protection Law regulate the collection, processing or transfer of personal information. The Labour Law and the Labour Contract Law require that internal investigation procedures comply with company rules and regulations and protect employees' legitimate rights and interests. If an employment contract is terminated based on investigation findings, the procedure must be lawful, and the facts must be clear.

Companies are not obligated to share all findings of internal investigations with enforcement authorities, but they have the duty to report or inform enforcement authorities upon discovering criminal facts or criminal suspects. Such duty is merely declaratory, and simply not reporting does not give rise to any punishment as long as the company does not actively conceal or harbour the offenders, which would be separately prosecuted under the Criminal Law.

In China, there is a general duty of confidentiality stipulated in the Law on Lawyers, which is imposed on lawyers to keep confidential any state or trade secrets obtained in the course of practising law, although there is no equivalent regime of legal privilege that prevents confidential communications between a client and their lawyer being disclosed to third parties. The Criminal Procedure Law further provides the defence attorney with the right to refuse to disclose the relevant information of the client in criminal investigations and proceedings; however, this is subject to a few exceptions where national security, public security or an individual's personal security are endangered.

2.6 Prosecution

Under the Criminal Procedure Law, prosecutions need to be examined and decided by the Procuratorate. When examining cases, the Procuratorate should interrogate the suspect and hear the opinions of the defence lawyers. The Procuratorate may request that the investigation authorities supplement the evidence and investigation. If the Procuratorate considers that the facts are adequate, the evidence is reliable and sufficient, and the criminal liabilities should be pursued, it shall initiate a public prosecution by filing an indictment with the competent people's court.

2.7 Deferred Prosecution

China does not have the Deferred Prosecution Agreement (DPA) system known in common law jurisdictions. Under the Criminal Procedure Law, for white-collar crime, there are four main types of non-prosecution that resolve a criminal investigation without a trial, as set forth below. The fundamental difference between these statutory non-prosecution provisions and a DPA regime is that the former are legal determinations made by the procuratorate based on the facts and the law (eg, no crime, minor circumstances, insufficient evidence, or special approval), and a DPA is a negotiated agreement between the prosecutor and the defendant, conditioned on compliance with certain obligations over a probationary period. The four types of non-prosecution include:

- statutory non-prosecution – where a criminal suspect has committed no criminal act, or where there are circumstances prescribed by law (circumstances so minor as not to be deemed a crime, expiration of the statute of limitations for prosecution, etc), the Procuratorate shall render a decision of non-prosecution;
- discretionary non-prosecution – where the circumstances of a crime are minor and, in accordance with the provisions of the Criminal Law, it is unnecessary to impose a criminal penalty, or the penalty may be exempted, the Procuratorate may render a decision of non-prosecution;
- non-prosecution due to insufficient evidence – with respect to cases subjected to supplementary investigation twice, where the Procuratorate still considers the evidence insufficient, and the conditions for prosecution are not met, it shall render a decision of non-prosecution; and
- approved non-prosecution – where a criminal suspect voluntarily and truthfully confesses to the facts of the suspected crime and has rendered major meritorious service, or the case involves major national interests, the Procuratorate may, upon approval by the Supreme People's Procuratorate, render a decision of non-prosecution.

3. White-Collar Offences

3.1 Criminal Company Law and Corporate Fraud

The offences related to criminal company law are primarily stipulated in Section 3, Chapter III of the Criminal Law, titled "Crimes of Obstructing the Administration of Companies and Enterprises", encompassing 16 offences. Among these, ten offences may be committed by units, including the crimes of:

- falsely reporting registered capital;
- making false capital contributions or surreptitiously withdrawing contributed capital;
- fraudulent issuance of securities;
- illegal disclosure or non-disclosure of important information;
- obstructing liquidation;
- concealing or intentionally destroying accounting vouchers, accounting books or financial accounting reports;
- false bankruptcy;
- bribing non-state functionaries;
- bribing foreign public officials or officials of international public organisations; and
- harming the interests of a listed company through breach of trust.

The offences in this section are predominantly intentional crimes, while the "crime of being defrauded due to serious irresponsibility in signing or performing a contract" and the "crime of dereliction of duty by personnel of state-owned companies, enterprises, or public institutions" are classified as crimes of negligence.

The penalties for offences in this section include life imprisonment, fixed-term imprisonment, criminal detention and fines.

Corporate fraud offences primarily include the crimes of contract fraud and fundraising fraud:

- if a person/company, with the purpose of illegal possession, defrauds the other party of property during the conclusion or performance of a contract, and the amount is relatively large, the crime of contract fraud is constituted; and
- if a person/company, with the purpose of illegal possession, uses fraudulent methods to illegally raise funds, and the amount is relatively large, the crime of fundraising fraud is constituted.

The penalties for both offences include fixed-term imprisonment, criminal detention, fines and, in serious cases, life imprisonment and confiscation of property.

3.2 Bribery, Influence Peddling and Related Offences

China criminalises a comprehensive range of bribery and influence-peddling offences. There are a total of 11 crimes relating to bribery, which generally forbid the act of offering a bribe to any state functionary or non-state functionary, and the receiving of that bribe by any state functionary or non-state functionary.

With respect to influence-peddling crimes, conviction needs to take various factors into account, such as whether the person conducting the influence peddling is a state or non-state functionary or any person who has a close relationship with a state functionary, as well as the specific manifestations of the influence on decision-making.

For example, any close relative of a state functionary, or any other person closely related to a state functionary, who secures illegitimate benefits for an entrusting person through the state functionary's performance of his or her duties – or through another state functionary's performance of his or her duties – by taking advantage of the state functionary's functions, powers or position, and who extorts from or accepts the entrusting person's money or property, shall be convicted of the crime of accepting bribes via influence. Anyone who, for the purpose of securing illegitimate benefits, offers bribes to any of the close relatives of the state functionary or other persons closely related to that state functionary, or to any state functionaries who have been removed from their positions, their close relatives or other persons closely related to them, shall be convicted of the crime of offering bribes to persons with influence.

Bribery of foreign public officials is also criminalised under the Criminal Law. Anyone giving any property to a state functionary of a foreign country or an official of an international public organisation for any improper commercial benefit will be convicted of the crime of bribery of foreign public officials and international public organisation officials.

Both individuals and entities may be held criminally liable under these bribery offences. Penalties for such offences include criminal detention, fixed-term imprisonment and fines.

3.3 Anti-Bribery Regulation

The Criminal Law does not impose a standalone statutory obligation equivalent to a "failure to prevent bribery" offence, nor does it mandate the adoption of a compliance programme as an independent legal requirement. While failure to implement a compliance programme is not itself a criminal offence, enforcement practice increasingly treats the existence and effectiveness of internal controls and compliance systems as relevant factors in charging decisions, case characterisation and sentencing.

According to the Criminal Procedure Law, any entity or individual that discovers the facts of a crime or a criminal suspect shall have a duty and right to report the case or provide information to a public security organ, the People's Procuratorate or a people's court. Said report is described as a duty in the Criminal Procedure Law, but no legal liabilities or any other penalties are explicitly stipulated.

3.4 Insider Dealing, Market Abuse and Criminal Banking Law

Insider trading, stipulated under the Criminal Law, refers to the conduct of buying or selling securities or engaging in futures trading related to insider information, or leaking such information or expressing or implying that others could engage in trading activities, resulting in serious circumstances.

The Criminal Law prohibits the act of manipulating securities and futures markets, including by hoarding spots, influencing the market quotations of specific futures and conducting related futures transactions. Offences related to insider dealing and market abuse require intent and can be committed by either individuals or entities. Penalties for such offences include criminal detention, fixed-term imprisonment and fines.

In the banking sector, the main criminal offences include illegally taking deposits from the public, defrauding loans, accepting bills or financial bills, forging or altering financial bills, and forging or altering negotiable securities of the state (or stocks or corporate bonds). These offences also require intent and can be committed by either individuals or entities. Penalties for such offences similarly include criminal detention, fixed-term imprisonment, life imprisonment, confiscation of property and fines.

3.5 Tax Fraud

Common tax crimes include tax evasion, resisting tax and evading recovery of outstanding taxes. All such crimes require intent and can be committed by either individuals or entities. Penalties for such offences

include criminal detention, fixed-term imprisonment, life imprisonment, confiscation of property and fines.

The Criminal Law does not criminalise the failure to prevent tax evasion as a standalone offence. Taxpayers are bound by an extensive set of statutory obligations in respect of tax filing, declaration and record-keeping; non-compliance with these obligations will generally attract administrative penalties, and where the circumstances are serious, such non-compliance will escalate to criminal liability.

3.6 Financial Record-Keeping

Criminal offences in relation to financial record-keeping mainly include:

- concealing or destroying accounting documents;
- fabricating financial records; and
- concealing or fabricating key information in financial disclosures.

Constituent elements typically require intent and serious consequences, such as investor harm or obstruction of supervision.

Such crimes can be committed by either individuals or entities. Penalties include criminal detention, fixed-term imprisonment and fines.

3.7 Cartels and Criminal Competition Law

Cartels are regulated by the Anti-Monopoly Law, which are administrative violations. Crimes related to unfair competition primarily include:

- counterfeiting registered trade marks;
- offering bribes;
- infringing upon trade secrets;
- false advertising; and
- colluding in bidding.

Such crimes all require intent and can be committed by either individuals or entities. Penalties for such crimes include criminal detention, fixed-term imprisonment, life imprisonment, confiscation of property and fines.

3.8 Consumer Criminal Law

General consumer protection violations are regulated by the Law on the Protection of Consumer Rights and Interests and the Product Quality Law, which are generally administrative violations.

Crimes related to consumer protection primarily include:

- producing or selling fake or substandard products;
- producing or selling toxic or harmful food;
- producing or selling counterfeit or inferior drugs; and
- false advertising.

Such crimes generally require intent and often necessitate meeting specific thresholds regarding the involved amount or other serious circumstances. They can be committed by either individuals or entities. Penalties for such crimes include criminal detention, fixed-term imprisonment, life imprisonment, the death penalty (specifically for crimes involving toxic/harmful food or fake drugs), confiscation of property and fines.

3.9 Cybercrimes, Computer Fraud and Protection of Company Secrets

Cybercrimes and crimes related to company fraud and breach of company secrets primarily include:

- sabotaging computer information systems;
- refusal to fulfil the obligation of safety administration in respect of information networks;
- illegal use of information networks;
- assistance in cyber-criminal activities;
- infringing citizens' personal information; and
- infringing trade secrets.

Such crimes generally require intent and often necessitate meeting specific thresholds regarding the involved amount or other serious circumstances. All the aforementioned crimes can be committed by either individuals or entities. Penalties generally include criminal detention, fixed-term imprisonment and fines.

3.10 Financial/Trade/Customs Sanctions

Crimes related to financial sanctions primarily encompass violations of foreign exchange administration and cross-border capital flows. Key categories include the

crime of money laundering and the crime of illegal business operations (frequently invoked for unauthorised financial activities such as underground banking or illegal trading of foreign exchange).

Crimes related to trade and customs sanctions primarily relate to smuggling, including smuggling prohibited goods (eg, weapons, nuclear materials), restricted items (eg, waste, dual-use items) or ordinary goods involving tax evasion.

China's criminal sanctions enforcement is strictly national-level and governed by domestic laws, and China does not enforce unilateral extraterritorial sanctions of other countries. All the aforementioned crimes generally require intent and often necessitate meeting specific thresholds regarding the involved amount or other serious circumstances. Such crimes can be committed by either individuals or entities. Penalties generally include criminal detention, fixed-term imprisonment, life imprisonment, confiscation of property and fines.

3.11 Concealment

Crimes related to concealment primarily relate to concealing or disguising crime-related income and the yields therefrom. These crimes require intent and can be committed by either individuals or entities. The predicate offences can be any upstream criminal activities, serving as a general provision. However, under the principle that a special provision prevails over a general provision, if an upstream crime falls within the seven designated categories (see **3.13 Money Laundering**) regulated by the crime of money laundering, that specific offence applies preferentially.

Liability generally extends to third parties who assist the principal offender. A person who commits the predicate offence is typically not liable for concealment (as the act of concealment is absorbed into the predicate offence), unless the act constitutes the specific crime of money laundering. Penalties for concealment include criminal detention, fixed-term imprisonment and fines.

3.12 Aiding and Abetting

A person who conspires with or assists another to commit a corporate offence with joint intent will be held liable.

The principal offender shall be punished for all crimes in which he or she participated, or which he or she organised or directed. An accessory shall be given a lighter or mitigated punishment, or be exempted from punishment. A coerced accomplice shall be given a mitigated punishment or be exempted from punishment. An abettor shall be punished according to his/her role in joint crime.

3.13 Money Laundering

The crime of money laundering is stipulated under the Criminal Law. Upstream crimes of money laundering include drug crimes, crimes of mafia-type organisations, crimes of terrorism, smuggling crimes, corruption and bribery crimes, crimes against the order of financial management and financial fraud crimes. The crime of money laundering requires the perpetrator to have the purpose of concealing or disguising the source and nature of the proceeds of the crime, and the proceeds it generates. This crime can be committed by individuals or entities.

Regarding prevention, primarily regulated by the Anti-Money Laundering Law, financial institutions and specific non-financial institutions (eg, real estate developers/agencies, accounting/law firms managing client assets and dealers in precious metals) bear statutory obligations to prevent money laundering. Failure to fulfil these obligations is primarily an administrative violation enforced by the People's Bank of China, subject to fines, disqualification of executives and potential licence revocation. However, if the failure involves knowingly facilitating criminal funds, it may trigger criminal liability.

3.14 ESG-Related Offences

The Criminal Law recognises criminal offences tied to ESG misconduct.

Environmental offences are primarily stipulated in Section 6, Chapter VI of the Criminal Law, titled "Crimes of Damaging Environmental and Resources Protection", which encompasses a total of 16 offences. All these

offences are applicable to both individuals and units. The penalties for offences in this section include fixed-term imprisonment, criminal detention, public surveillance, fines and confiscation of property.

Crimes under the social dimension primarily include the following.

- Offences involving failure to respect workers' rights, including the crime of forced labour, the crime of refusing to pay labour remuneration and the crime of employing child labour for hazardous work. All three offences are intentional crimes and apply to both individuals and units.
- Offences related to failure to fulfil occupational safety obligations include the crime of causing a major labour safety accident and the crime of causing a major liability accident. Both are negligence-based offences. The former applies to both individuals and units, while the latter applies only to individuals.
- Offences involving disregard for the legitimate rights and interests of consumers (see **3.8 Consumer Criminal Law**).

Offences in the area of governance are primarily crimes related to corporate governance (see **3.1 Criminal Company Law and Corporate Fraud**), crimes in the field of anti-bribery (see **3.2 Bribery, Influence Peddling and Related Offences** and **3.3 Anti-Bribery Regulation**) and crimes in the tax domain (see **3.5 Tax Fraud**). Additionally, the crimes of embezzlement in office and misappropriation of funds are intentional offences applicable to individuals. The penalties for such offences include fixed-term imprisonment, criminal detention and fines.

Companies are expected to monitor supply chains for compliance. Administrative regulations in areas such as environmental protection, labour, anti-unfair competition and taxation, as well as relevant administrative regulatory authorities, have imposed corresponding requirements. Failure of a company to meet the compliance requirements in its supply chains may give rise to criminal liability. For example, if a company's production facilities or production conditions fail to meet national compliance requirements, thereby resulting in a major casualty accident or having other serious consequences, this will constitute the crime of major labour safety accidents.

3.15 Artificial Intelligence and Automation Misuse

Under the Criminal Law and relevant judicial precedents, common offences related to the misuse of AI, algorithmic trading or automated decision-making include, but are not limited to, the following.

- The crime of manipulating securities or futures markets: Engaging in market manipulation behaviours – such as high-frequency trading without a genuine intention to trade, spoofing or making false declarations – through the utilisation of AI or algorithms may constitute this crime. This offence is an intentional crime applicable to both individuals and units. The penalties include criminal detention, fixed-term imprisonment and fines.
- The crime of fundraising fraud: Using AI to generate false information, financial statements or forged transaction records, or employing algorithms to construct fraudulent trading systems and data to induce victims to invest, may constitute this crime. This offence is an intentional crime applicable to both individuals and units. The penalties include fixed-term imprisonment, life imprisonment, fines and confiscation of property.
- The crime of illegal business operations: Operating financial intermediary services without approval by utilising AI, algorithmic trading or automated decision-making may constitute this crime. This offence is an intentional crime applicable to both individuals and units. The penalties include criminal detention, fixed-term imprisonment, fines and confiscation of property.
- The crime of aiding information network criminal activities: Knowingly providing AI technical support, algorithmic tools or automated decision-making systems to assist others in committing crimes via information networks may constitute this crime. This offence is an intentional crime applicable to both individuals and units. The penalties include criminal detention, fixed-term imprisonment and fines.

3.16 Crypto-Assets and Digital Currency Crimes

In Chinese judicial practice, crypto-assets, blockchain-based assets and digital currencies are primarily associated with offences such as the illegal absorption of public deposits, fundraising fraud, illegal business operations, money laundering, concealing or disguising the proceeds of crime and criminal gains, aiding information network criminal activities, and organising or leading pyramid selling schemes. These offences are all classified as intentional crimes and are applicable to both individuals and units.

China has implemented a comprehensive ban on business activities related to crypto-assets, classifying them as illegal financial activities. Consequently, crypto-asset service providers are strictly prohibited within China. Any individual or organisation providing or participating in crypto-asset services may be suspected of involvement in the aforementioned crimes, including the crime of illegal business operations.

However, the non-commercial possession of virtual currencies by individuals is not explicitly prohibited. In judicial practice, crypto-assets are recognised as possessing property under the Criminal Law and may serve as the objects of property crimes (such as theft and fraud). Accordingly, the theft or fraudulent acquisition of crypto-assets constitutes a criminal offence, for which the enforcement authorities may pursue criminal liability.

4. Pleas and Defences

4.1 White-Collar Defences

Common defences primarily focus on challenging the constituent elements of the crime, specifically mens rea and actus reus. Defence counsel often asserts a lack of illegal possession or criminal intent, arguing that the conduct in question constitutes a legitimate commercial irregularity rather than a criminal act. For corporate defendants, a critical defence involves distinguishing individual misconduct from unit crimes, arguing that the act was a personal violation against company rules rather than an entity's decision. Procedural defences are also critical. For example, counsel may file motions for the exclusion of illegal evidence if confessions or evidence were obtained through procedural violations. Specific statutory defences exist for certain offences. For instance, in bribery cases, providing property under extortion without obtaining any undue advantage does not constitute a crime.

The existence of compliance programmes is not a statutory defence for criminal liability. However, enforcement trends show that establishing an effective compliance programme may be a factor in determining the charging decisions, case characterisation and sentencing.

4.2 De Minimis

The Criminal Law sets forth the thresholds for prosecuting white-collar crimes. For example, the general threshold amount for offering bribes to a state functionary and to a non-state functionary is CNY30,000 (approximately USD4,250). Under certain circumstances, the threshold may be lowered to CNY10,000 (approximately USD1,420), such as where bribes are offered to three or more state functionaries, or where bribes are offered to state functionaries responsible for the supervision of food, drugs, workplace safety or environmental protection for conducting illegal activities. A judicial interpretation effective from 1 May 2026 further aligns the conviction and sentencing standards for bribery involving non-state functionaries, occupational embezzlement and misappropriation of funds with those for the corresponding public-sector offences.

Conduct falling below these thresholds is generally treated as an administrative violation subject to administrative penalties rather than criminal prosecution. For state functionaries or Party members, such conduct also triggers strict internal disciplinary actions that can end careers even without criminal charges. No sectors or industries are exempt from these laws.

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

In accordance with the Criminal Procedure Law, China implements the leniency for admission of guilt and acceptance of punishment system, allowing defendants to receive lenient treatment by accepting sentencing recommendations. The Criminal Law defines voluntary surrender and truthful confession as statu-

tory mitigating circumstances. Meritorious service, such as exposing others' crimes, is also a statutory ground for lenient punishment, which can lead to sentence reduction or even exemption from punishment in major cases. Moreover, specific leniency provisions exist for certain white-collar offences. For instance, Article 164 of the Criminal Law provides that any briber who confesses voluntarily prior to prosecution may receive a mitigated punishment or be exempted from punishment. However, these measures are discretionary. Courts may refuse mitigation if the crime involves particularly egregious circumstances, even if the defendant has confessed.

4.4 Whistle-Blower Protection

For the protection of whistle-blowers, specific rules have been formulated to provide a comprehensive mechanism at both substantial and procedural levels, such as the Rules of the Supreme People's Procuratorate on Protecting Citizens' Tip-Off Rights. Retaliation against whistle-blowers is entirely prohibited by law, and administrative penalties, criminal detention or imprisonment can be imposed.

Regarding incentives, regulations such as the Provisions on Rewards for Whistleblowers for Securities and Futures Violations offer significant material rewards for substantiated reports. At the corporate level, companies typically implement third-party anonymous hotlines and anti-retaliation policies; nevertheless, official anonymous reporting channels provided by regulators offer a more independent supervision path protected by strict laws.

4.5 Cross-Border Defence Strategies

When white-collar investigations span multiple jurisdictions, defence strategies must transcend a single-jurisdiction focus and adopt a globally co-ordinated approach. For multinational enterprises, three core considerations are particularly critical to this end.

- First, upon the commencement of a governmental investigation in any jurisdiction, the defence team must immediately assess whether the underlying conduct gives rise to parallel criminal liability or regulatory exposure in other jurisdictions.
- Second, multinational enterprises must identify and address potential conflicts of law and legal restrictions governing cross-border investigatory conduct. For instance, the International Criminal Judicial Assistance Law restricts foreign parties from conducting criminal procedural activities in China, and Chinese parties from providing evidence or related assistance to foreign parties, without the consent of the competent Chinese authorities.
- Third, multinational enterprises must comply with applicable restrictions on cross-border data transfer and the protection of sensitive information, as mandated by the Cyber Security Law, Data Security Law and Personal Information Protection Law, as well as relevant legislation governing state secret protection. Accordingly, minimising cross-border data outflow and implementing robust pre-transfer data screening protocols are indispensable protective measures.

5. Key Trends and Future Outlook

5.1 The Year Ahead

With an increasingly robust legal framework and intensified government enforcement actions, 2027 is expected to remain a busy year for government enforcement in various areas. Companies in China are advised to pay close attention to updates and changes in regulatory enforcement trends, establish and operate well-founded compliance mechanisms and continuously strengthen their compliance status, especially in the high-risk areas of anti-corruption, anti-monopoly, anti-money laundering, securities fraud and data protection. Since the Chinese authorities announced collaborative efforts to launch a nationwide campaign targeting corruption within the healthcare industry in 2023, this industrial anti-corruption campaign has become a priority for China. Looking ahead, China's Fifteenth Five-Year Plan (2026–30) calls for stronger anti-monopoly and anti-unfair competition enforcement and closer co-ordination between administrative and criminal enforcement, while the Fifth Plenary Session of the 20th Central Commission for Discipline Inspection signals a continued focus on corruption in key sectors and on new, concealed and cross-border forms of corruption. As the regulatory compliance landscape in China is expected to become increasingly stringent, best practices dictate a dual approach: proactive measures to prevent non-compliance issues and reactive strategies to effectively manage potential external 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