Bribery and corruption reporting obligations: China

by *Geoffrey Atkins*, *Megan McEntee* and *Abraham Lee*, *Ropes & Gray* and *Practical Law China*.

Practice notes | **Maintained** | China

A note on the obligations that may arise for a corporate entity to report allegations or findings of bribery, corruption or related misconduct by personnel located in China. The note covers the US, UK, Chinese and Hong Kong regimes.

Scope of this note

Corruption is a significant risk for corporations doing business in *China*. Review this note if you have to decide whether it is required or otherwise advisable to report allegations or findings of misconduct to various government authorities. This may be the case if, for example, you:

- Have been notified of allegations involving bribery at your client's operations in China.
- Have taken (or are considering taking) steps to investigate these allegations.
- Have made or are preparing to make findings concerning the alleged misconduct.

This note addresses the legal requirements and practical considerations for in-house and outside counsel in deciding whether to report allegedly corrupt activities that occurred in China to government agencies in the US, UK, China, or Hong Kong. Consulting local counsel in these and other relevant countries is particularly important, as an increasing number of jurisdictions have passed mandatory reporting legislation and the enforcement landscape is rapidly evolving.

The note does not address in detail the substantive offences of bribery and corruption that arise under the regimes that most frequently apply to corporations operating in China. For a detailed description of the rules that apply under the Chinese, US and UK regimes, see Practice notes:

- *Bribery and corruption (China): overview*.
- *Bribery and corruption offences, enforcement and penalties: China*.
- *Anti-corruption regimes in China, the UK and the US: a comparative guide*.
- *The Foreign Corrupt Practices Act: Overview*.
- *Bribery Act 2010*.

Regime in the US

Corrupt activities undertaken by a company's subsidiary, employee, or other agent in China often require an organisation to consider disclosing the conduct to the US government. The bribery of foreign officials is prohibited by US law under the *Foreign Corrupt Practices Act of 1977* (FCPA). The FCPA's anti-bribery provisions prohibit improper payments to foreign officials to obtain or retain business or secure any improper advantage. The FCPA's accounting and internal controls provisions require companies whose securities are US-listed to maintain books and records that accurately and fairly reflect the company's transactions. These companies must also devise and maintain an adequate system of internal accounting controls. While the FCPA does not mandate self-disclosure, there may be reporting requirements in other contexts, and practical considerations may weigh in favour of reporting. For more detail on the individual provisions of the FCPA and links to other FCPA-related resources, see *Practice note, The Foreign Corrupt Practices Act: Overview*.

Reporting requirements in the US

In the US, there is no general obligation to disclose to the US government that a company's agent has committed bribery. However, certain entities may be required to report knowledge or suspicion of bribery if it relates to potential money laundering.

Requirements under US anti-money laundering legislation

US anti-money laundering legislation may require financial institutions to report actual or suspected bribery. Under 31 USC Section 5318(g) and its corresponding regulations, financial institutions must report certain suspicious activities. These institutions include banks, credit unions, securities brokers and insurance companies (*31 USC § 5312(a(2))*).

Financial institutions must:

- File a report of each deposit, withdrawal, exchange of currency, or transfer of USD10,000 or more (*31 CFR §§ 1010.311*).
- File suspicious activity reports (SARs) with the Treasury Department for any transaction over USD5,000 when the institution knows or suspects that:
  - the transaction involves funds derived from illegal activities or is intended to hide funds from illegal activities;
  - the transaction is designed to evade any requirements of the Bank Secrecy Act 1970, including structuring to evade reporting thresholds; or
  - the transaction has no apparent lawful purpose and no reasonable explanation.

(*31 CFR § 1020.320(a)(2)(i)-(iii)*.)

For further details of the SAR reporting requirements for financial institutions, see *Practice note, Suspicious Activity Reporting Requirements for Financial Institutions*.

Non-financial institutions do not have similar reporting requirements. However, the US *Department of Justice* (DOJ) has charged members of bribery conspiracies under US money laundering statutes (see for example, *United States v Duperval, 777 F. 3d 1324 (11th Cir. 2015)*). Additionally, if one or more conspirators use a financial institution to launder bribe payments, the financial institution may be obligated to file a SAR under the rules above.

Practical considerations when deciding to report to US authorities

There are several significant practical considerations that factor into the decision of whether to disclose allegedly corrupt behaviour by an agent in China to the US government.

Jurisdictional considerations

When deciding whether to disclose bribery in China, organisations should assess whether the US has jurisdiction. For example, the *FCPA* has a broad (but not unlimited) jurisdictional reach applying to US issuers (publicly traded companies required to file reports with the SEC) and domestic concerns (US citizens, residents, or any company organised under the laws of a US territory or having a principal place of business in the US) (*15 USC § 78dd-1(a)*). In addition, territorial jurisdiction may apply to foreign nationals and entities that breach the FCPA while in US territories (*78dd-3(a)*).

Possibility of eventual disclosure by whistleblowers

Companies should be aware of the risk that a whistleblower discloses the alleged bribery first. Section 806 of the *Sarbanes-Oxley Act of 2002* protects whistleblowers by prohibiting publicly traded companies from retaliating against employees who report instances of fraud to their employers, including fraud committed under the *FCPA* (*18 USC § 1514A*). The Sarbanes-Oxley Act of 2002 also requires the disclosure of information that has a material financial effect on public companies, which could in some instances necessitate the disclosure of corruption-related misconduct.

US law provides strong incentives to employees to report fraudulent behaviour by their employer. Under Section 922 of the *Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010*, whistleblowers may be rewarded between 10% and 30% of the amount recovered by the government, provided the whistleblower provided original information that led to a successful enforcement action with sanctions exceeding USD1 million (*15 USC § 78u-6*). The government has delivered on these promises; since the inception of the *Securities and Exchange Commission*'s (SEC) whistleblower program, the agency has awarded more than USD500 million in connection with successful actions. In June 2020, the SEC announced their largest ever whistleblower award of USD50 million to an individual whose direct observations of misconduct at an unnamed company led to a successful enforcement action. China has been a particularly fruitful source of tips. Since 2011, the SEC has received over 250 tips from whistleblowers in China.

The SEC's 2019 Annual Report to Congress detailing the results of the Whistleblower Program stated that the number of whistleblower tips has increased over time, with 200 FCPA-related tips in financial year 2019.

(For more information on the role played by whistleblowers in China, see *Practice note, Whistleblower protection: China*.)

Positive impact on charging decisions

While there is no affirmative requirement to self-report potential misconduct to US regulators, the DOJ maintains an FCPA Corporate Enforcement Policy that gives significant benefits to companies who self-disclose potential violations of the FCPA and meet additional prerequisites. In April 2016, the DOJ Fraud Section's *FCPA* Unit introduced a yearlong "Pilot Program" offering significant sentencing mitigation credit (up to a 50% reduction off the bottom end of the Sentencing Guidelines fine range or a declination) to businesses who met the programme's standards of:

- Voluntary self-disclosure
- Full co-operation
- Timely and appropriate remediation.

The Pilot Program specified that "full co-operation" involves proactive behaviour on behalf of the company, including rolling disclosures of key facts, provision of relevant overseas documents, and making company officers and employees available for interviews.

Shortly after the Pilot Program's inception, the DOJ publicly issued declination letters to US-based cloud computing and content delivery network company Akamai Technologies, Inc. and US-based building products manufacturer Nortek Inc., both of whom timely self-disclosed illegal payments made by their Chinese subsidiaries. Notably, the DOJ stated that credit would be "markedly less" for those who co-operate but do not self-disclose.

In November 2017, the DOJ announced a permanent FCPA Corporate Enforcement Policy that was incorporated into the United States Attorneys' Manual (renamed the "Justice Manual" in 2018), which provides internal guidance for all federal prosecutors. The revised policy adjusted the Pilot Program's requirements in several important ways:

- Establishing a presumption that the DOJ resolve cases through declinations when companies meet the Program's standards, absent aggravating circumstances such as involvement by executive management in the misconduct, significant profit resulting from the misconduct, pervasiveness of the misconduct, or recidivism.
- Directing the DOJ to accord a 50% reduction off the US Sentencing Guidelines range fine, where the company otherwise meets the detailed standards but aggravating circumstances are present.
- Providing additional detail on the criteria to assess the sufficiency of a company's compliance programme when assessing the sufficiency of remediation.

The DOJ made several updates to the Corporate Enforcement Policy in 2019. These included a clarification that to receive full self-disclosure credit companies need only disclose individuals "substantially involved in" the misconduct at issue. The updated Policy also extended a presumption of declination to companies that self-disclose in connection with a merger or acquisition, when misconduct is identified in the target company. The SEC has taken a similar position regarding the importance of self-disclosure.

Specifically, both DOJ and SEC have several means with which to offer companies co-operation credit:

- **Declinations.** In certain cases, the government may decline to prosecute a company that discloses an FCPA violation. For example, on 19 September 2019, global marketing solutions provider Quad/Graphics Inc. received a declination letter from the DOJ after an investigation into bribery by employees of the company's subsidiaries in China and Peru. The DOJ cited the Company's prompt voluntary disclosure, thorough investigation, and fulsome co-operation, including discontinuing the relationship with the employees and third-parties in China involved in the misconduct. Similarly, on 24 June 2020, the SEC declined to take any enforcement action against Usana Health Services, Inc., a multi-level marketing company that had conducted a voluntary internal investigation into certain of its operations in China. The SEC indicated that its decision was based in part on the Company's prompt, voluntary self-disclosure, thorough internal investigation, full cooperation with the SEC, and remediation of the matters underlying the investigation. As noted above, the DOJ's FCPA Corporate Enforcement Policy indicates that the DOJ should decline prosecution where a company meets the Policy's detailed requirements.
- **Non-prosecution agreements.** The government has rewarded some organisations' voluntary disclosures of misconduct with *non-prosecution agreements* (NPAs). For example, in 2016, the DOJ entered into an NPA with Kentucky-based manufacturer General Cable Corporation, despite alleged FCPA violations in China, Angola, Bangladesh, Indonesia and Thailand, due to the company's prompt reporting of the violations and co-operation with the DOJ's investigation. This co-operation included making foreign-based employees

available for interviews and terminating relationships with 57 third-party agents who participated in the misconduct.

Even where a company does not voluntarily disclose, the government may still reward co-operation and remediation with an NPA. For example, in 2019, the DOJ entered into an NPA with global retail-chain Walmart Inc., related to alleged FCPA violations. Notably, the company did not receive voluntary disclosure credit despite disclosing conduct related to activities in China, Brazil, and India because such disclosure occurred only after the DOJ had already begun investigating the company's misconduct in Mexico. The company was still able to secure the NPA, however, because of the company's "significant remedial measures" and continued co-operation with the government.

- **Deferred prosecution agreements.** Similarly, the government has also offered *deferred prosecution agreements* (DPAs) as an alternative to criminal indictment, in recognition of corporations' voluntary disclosure and co-operation. For example, in April 2018, Panasonic Avionics Corporation entered into a DPA to resolve allegations that it made payments to "consultants" in China and elsewhere in Asia that resulted in a violation of the books and records provision of the FCPA. The agreement noted that while Panasonic Avionics did not make a timely disclosure of the misconduct, it did co-operate with the DOJ's investigation. Similarly, in August 2020, Herbalife Nutrition Ltd. ("Herbalife") entered into a three-year DPA, paying a criminal fine that was discounted by 25% off the otherwise applicable Sentencing Guidelines fine range. Despite Herbalife's failure to self-report the misconduct, it was credited for its full subsequent co-operation.
- **Reduced fine amounts.** The government frequently cites self-reporting, co-operation with an investigation, and remediation efforts when assessing the amount of a penalty. For example, in September 2018, United Technologies Corporation, a Connecticut-based manufacturer, paid USD13.9 million to the SEC to settle allegations that the company paid bribes to officials in China and Azerbaijan. The SEC cited the company's efforts of self-reporting the misconduct, including providing timely reports of its investigative findings, producing key document binders and English language translations of documents, and making foreign witnesses available. These measures were credited with determining the appropriate remedy. By contrast, Ericsson, a telecommunications company headquartered in Sweden, paid total penalties over USD1 billion in an FCPA case in 2019, in which the DOJ's press release explicitly cited failure to voluntarily disclose misconduct as a consideration in justifying the penalty amount.
- **Sentencing guideline credit.** As discussed above, the Revised FCPA Corporate Enforcement Policy requires prosecutors to accord a 50% reduction off of the US Sentencing Guideline penalty ranges where a declination is inappropriate (for example, due to the presence of "aggravating circumstances" as defined in the Policy) but the company meets the standards for self-disclosure, co-operation, remediation, and disgorgement. However, only a 25% reduction will be given where the company fails to self-disclose but otherwise meets the criteria above.

Importantly, voluntary disclosure may not always result in a positive outcome for the company. Some have suggested that regulators overemphasise the value of disclosing misconduct. Many factors influence regulator charging and penalty decisions beyond voluntary disclosure, including the scope and nature of the misconduct, subsequent co-operation, remedial measures, and the nature of the misconduct itself.

Presence of a corporate compliance programme

A strong corporate compliance programme can affect a company's potential liability in several ways, and is often a factor in evaluating whether to voluntarily disclose misconduct. The Second Edition of *A Resource Guide to the U.S. Foreign Corrupt Practices Act* (Resource Guide), jointly released by the DOJ and SEC in April 2020, highlights that the adequacy and effectiveness of a company's compliance program factors into three key areas of decision making in criminal resolutions:

- The form of resolution or prosecution, if any.
- The monetary penalty, if any.
- The compliance obligations to be included in any resolution.

The Resource Guide also outlines certain "hallmarks of effective compliance programs" that the DOJ and SEC consider when making a determination as to the quality of a corporate compliance programme. The hallmarks include:

- Commitment from senior management and a clearly articulated policy against corruption.
- Code of conduct and compliance policies and procedures.
- Oversight, autonomy, and resources.
- Risk assessment.
- Training and continuing advice.
- Incentives and disciplinary measures.
- Third-party due diligence and payments.
- Confidential reporting and internal investigation.
- Continuous improvement: periodic testing and review.
- Mergers and acquisitions: pre-acquisition due diligence and post-acquisition integration.
- Investigation, analysis, and remediation of misconduct.

Importantly, the Resource Guide notes that the hallmarks are not dispositive, and different factors will warrant more or less emphasis depending on the type of business at issue (for example, size of enterprise and industry group). The DOJ reiterated the importance of these factors in the June 2020 update of its guidance on Evaluation of Corporate Compliance Programs, where several changes seek to ensure that compliance programs are dynamic and continuously updated to fit new circumstances. For example, in a section pertaining to third-party risk, the guidance looks to whether the company engages in "risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process."

The government's consideration of these factors was already evident in previous enforcement actions. For example, in 2012, the SEC and DOJ prosecuted Garth Peterson, a managing director at Morgan Stanley who secretly arranged payments to the chairman of a Chinese state-owned entity. However, the government chose not to prosecute Morgan Stanley itself, citing the company's internal controls "which provided reasonable assurances that its employees were not bribing government officials" (see *Article, Corporate crime and investigations column: August 2012: Morgan Stanley shows Wall Street how "adequate procedures" is done*). Similarly, in a 2016 case involving JPMorgan Securities, the company received an NPA that noted that an independent compliance monitor was unnecessary due to the state of the company's compliance programme.

There is also potential to argue that corporate compliance programmes may provide a substantive defence to corporate criminal liability. Unlike the adequate procedures defence under the UK *Bribery Act 2010* (BA 2010, as described further in *Availability of adequate procedures defence*), a comprehensive and effective compliance programme is not an explicit defence to liability under the *FCPA*. Applying general principles of corporate criminal liability, most US courts addressing the question have stated that strong compliance policies do not remove an agent's conduct from the scope of employment for purposes of assessing corporate liability. However, dicta in several US circuits suggest that comprehensive and rigorously enforced policies can potentially provide a substantive defence to liability by cabining the scope of an agent's authority.

Additional practical considerations

Organisations should consider the following additional factors when deciding whether to disclose bribery or corruption in their China operations to US authorities:

- **Resulting disclosure to other governments.** As other countries develop more sophisticated anti-bribery legislation, disclosure to the US government may result in disclosure to countries with less predictable enforcement regimes such as China.
- **Obligations under pre-existing agreements with the government.** Is the organisation under a pre-existing DPA or corporate integrity agreement? These agreements may contain monitoring and self-reporting mandates for any subsequent violations.
- **Details of the misconduct.** Was the conduct pervasive throughout the organisation? Did it occur long ago, and has the conduct been fixed? Organisations should consider all factors that may persuade regulators not to pursue the matter aggressively.
- **Broader government inquiries.** Is the matter part of a broader government inquiry (for example, an industry-wide enforcement effort)? This could have divergent implications, depending on the facts. The government may wish to send an industry-wide message concerning corrupt conduct and so may be less receptive to pleas for leniency. However, if other organisations from the industry have publicly resolved similar matters involving more egregious conduct, this may provide an opportunity to distinguish the organisation's own conduct and request a more favourable resolution.
- **Exposure to related litigation.** An entity may be exposed to follow-on shareholder lawsuits based on the underlying bribery allegations in an *FCPA* case, often involving penalties that are higher than those paid to the government. In one case, Nature's Sunshine Products, Inc. paid a civil penalty of USD600,000 to settle charges that they made improper payments to Brazilian customs officials. Nature's Sunshine subsequently settled a related securities fraud class action for USD6 million.
- **Implications of China's blocking statute.** On 26 October 2018, China enacted the *Law on International Criminal Judicial Assistance* (2018 ICJAL), which requires any institution, organisation, or individual within China to receive approval by Chinese governmental authorities before providing any materials or assistance to foreign countries' criminal proceedings. Because the language of the 2018 ICJAL specifically forbids private parties from transmitting information internationally without first obtaining approval from Chinese authorities, organisations facing potential FCPA violations may encounter hurdles when attempting to co-operate with U.S. governmental entities. (For more information on the 2018 ICJAL, see *Article, China's international criminal judicial assistance law and the impact on MNC internal investigations*.) Nonetheless, organisations may still receive the benefit of full co-operation with the DOJ as long as they attempt to take the appropriate steps to obtain approval from Chinese authorities. The DOJ recently amended the Justice Manual to acknowledge that there may be circumstances in which a

company "genuinely cannot get access to certain evidence or is legally prohibited from disclosing it to the government".

Regime in the UK

It is a criminal offence under the *BA 2010* to offer, give, request or receive a bribe (*sections 1, 2 and 6*). This is not limited to the bribery of foreign officials, as the BA 2010 covers the bribery of any person or organisation. Of particular note to companies incorporated in the UK is the corporate offence of failing to prevent bribery: if an employee, subsidiary or agent of a UK company engages in bribery anywhere in the world, then the UK company can be held criminally liable for failing to have adequate controls in place to prevent the bribery (*section 7*).

The BA 2010 does not obligate a company to report corrupt activity to UK law enforcement agencies. However, companies that identify instances of corrupt activity within their operations may consider with their legal advisors on making a voluntary disclosure to law enforcement, followed by fulsome co-operation, in the hope of achieving a more favourable outcome in any resulting criminal proceedings.

There is also a stringent and sophisticated anti-money laundering regime in the UK that requires companies in the financial services sector, as well as lawyers and accountants, to report any suspicions of money laundering or terrorist financing to law enforcement. Failure by these parties to make such a report is a criminal offence. In addition to these positive reporting obligations, companies and individuals (in any sector) may wish to report knowledge or suspicion of money laundering in order to obtain a defence to a substantive money laundering offence.

Moreover, there are other reporting obligations that specifically apply to the financial services and extractive sectors.

Reporting obligations in the UK

Reporting to the Financial Conduct Authority

Financial services firms have specific duties to make disclosures to the *Financial Conduct Authority* (FCA). The following rules from the FCA Handbook (identified by the FCA in its April 2016 *Financial Crime: a guide for firms* as being particularly relevant to financial crime) are of particular note:

- A firm must deal with its regulators in an open and co-operative way, and disclose anything about which the regulator would reasonably expect notice (*PRIN 2.1.1R*).
- A firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements under the regulatory system, and for countering the risk that the firm might be used to further financial crime (*SYSC 3.2.6R* and *SYSC 6.1.1R*).
- Authorised firms are required to conduct their business with integrity and due care, skill and diligence (*PRIN 2.1.1R*).

The FCA does not enforce the *BA 2010*; its primary concern in this context is whether firms have in place appropriate systems and concerns to adequately address the risk that they may be used for the purposes of financial crime. However, it is possible that information provided to the FCA may be shared with the Serious Fraud Office (SFO), or other criminal or regulatory enforcement authorities in the UK. For more information on the FCA's financial crime responsibilities, see *Practice note, A guide to key resources for financial institutions: financial crime*.

Requirements under UK anti-money laundering statutes

Entities within the "regulated sector" (as defined by Schedule 9 of the *Proceeds of Crime Act 2002* (POCA) and Schedule 3A of the *Terrorism Act 2000* (TACT)) are required to report suspicions of money laundering or involvement in terrorist financing to the National Crime Agency (NCA) under Part 7 of POCA and under Part 3 of TACT. The term "regulated sector" includes financial institutions such as banks, credit providers, investment advisors, private equity firms and money service businesses, as well as high-value dealers, trust service providers, accounting firms, law firms and estate agency businesses.

If an entity in the regulated sector knows or suspects that a person is engaged in, or attempting, money laundering or terrorist financing, it must file a Suspicious Activity Report (UK SAR) with UK law enforcement. As in the US, this requirement may relate back to corruption if the laundered funds originated as a bribe. Failure to file a UK SAR by an entity within the regulated sector when there is suspicion of money laundering is a criminal offence under Part 7 of POCA (*section 330, POCA*).

Information submitted to the NCA may be shared with other law enforcement agencies, including the SFO. Entities within the regulated sector regularly disclose bribery issues through UK SARs.

When reporting a suspicion of money laundering, entities must be mindful of the offence of "tipping-off". This offence is committed when a person working within the regulated sector knows or suspects that another person's suspected involvement with money laundering is the subject of investigation (or contemplated investigation) and makes a disclosure to a person likely to prejudice an investigation (*section 333A(1), POCA*). Accordingly, it is essential that the subject of the UK SAR is not informed of the fact that it has been filed with the NCA.

Making a disclosure to law enforcement can also serve as a defence to a substantive money laundering offence, such as being concerned in an arrangement which a person (operating in any sector) knows or suspects facilitates, by whatever means, the acquisition of, retention, use or control of criminal property by or on behalf of another person (*sections 328 and 338*, *POCA*).

For a general overview of reporting obligations under POCA, see *Practice note, An overview of the UK anti-money laundering and counter-terrorist financing regime*. For specific details of how POCA applies to bank staff, see *Practice note, Reporting obligations under the Proceeds of Crime Act 2002: guide for financial institutions*.

Reporting requirements in the extractive sector

Since 1 January 2015, companies that are either listed on EU-regulated markets, or are listed companies in the logging or extractive industries, have been subject to additional reporting requirements concerning any payments made to governments. This rule was introduced by the *Transparency Directive* (2004/109/EC), with parallel rules contained in the *Accounting Directive (2013/34/EU)*. These companies are not necessarily registered or incorporated in the EEA. For further details, see *Practice notes, Transparency Directive: overview* and *Accounting Directive: overview*.

The aim of these reporting requirements is to increase transparency in these industries and to reduce corruption risk by holding governments of resource-rich countries accountable. Relevant companies are required to disclose payments made to government entities worldwide, in accordance with *The Reports on Payments to Governments Regulations 2014* (*SI 2014/3209*).

Listed companies should also consult with their legal advisors on what, if any, public disclosures they are required to make under the rules of the relevant listing authority about their involvement in any bribery, corruption or money-laundering.

Practical considerations when deciding whether to report to the UK authorities

There are several significant practical considerations when considering whether to make a voluntary disclosure of corrupt behaviour by an agent in China to the UK authorities.

Jurisdictional considerations

An organisation should consider whether the UK is likely to have jurisdiction over the discovered misconduct. The *BA 2010* generally has jurisdiction over:

- Offences committed in whole or in part in the UK.
- Offences committed by individuals or entities with a close connection to the UK, regardless of where the conduct occurs.
- In the case of the corporate offence of failing to prevent bribery: an offence is committed irrespective of whether the acts or omissions which form part of the offence take place in the UK or elsewhere.

(*section 12*.)

As defined, "close connection" includes British citizens, citizens of British territories, and entities incorporated under the law of any part of the UK (*section 12(4), BA 2010*).

For more information on the jurisdictional reach of the BA 2010, see *Practice note, Bribery Act 2010: jurisdictional reach*.

Influence on charging decisions

It cannot be assumed that self-reporting will mean that a corporate entity is not prosecuted or lead to a lower penalty than would otherwise be imposed. However, the SFO has frequently emphasised the benefits of voluntary disclosure. According to the SFO's Guide to Corporate Self-Reporting, the SFO may take into account a voluntary disclosure as a public interest factor tending against prosecution, if the disclosure forms part of a genuinely proactive approach adopted by the corporate management team when the offence is brought to their notice. This approach should include self-reporting and remedial actions, including the compensation of any victims. Prosecutors also consider whether a corporation has provided sufficient information to the government, including making witnesses available and disclosing the details of any internal investigation.

Self-reporting can also have a bearing on whether prosecutors consider offering a DPA. DPAs were introduced in the UK in 2014. In February 2014, the SFO and CPS jointly issued the *DPA Code of Practice* (DPA Code), which sets out the issues to be considered by prosecutors when deciding whether a DPA is appropriate. The DPA Code specifically identifies self-reporting as a factor in favour of offering a DPA. It also makes clear that considerable weight is given to the existence of:

- A genuinely proactive approach adopted by an organisation's management when the offending conduct is brought to their attention.
- Full co-operation with the SFO's investigation. This could include a request for copies of any witness statements and reports prepared during any internal investigation. However, the Court of Appeal has confirmed that it may be possible for a company to resist disclosure on the basis of legal professional privilege (see *SFO v ENRC [2018] EWCA Civ 2006*). For further guidance on privilege under English law, see *Practice note, Legal professional privilege in civil litigation: an overview*.
- Proactive corporate compliance programme, both at the time of the offence and at the time of reporting.

SFO Director Lisa Osofsky has reiterated statements made by her predecessor, Sir David Green, who made clear that the SFO will not simply take self-reports at face value. In particular, in November 2018, she stated that the SFO was prepared to seek accounts of internal witness interviews if the interviewee was later charged with a crime.

The timing of the disclosure to the UK authorities may also be important. Failure to report the wrongdoing within a reasonable time after discovering the offence is a public interest factor in favour of prosecution. The SFO may have information about wrongdoing from other sources (including SARs). Therefore, companies who have discovered misconduct should rapidly begin the process of deciding whether to disclose.

There is growing precedent available in the UK to assist companies in evaluating the advantages and disadvantages of self-reporting in the UK. Since their introduction in 2014, the SFO has so far entered into nine DPAs, reflecting some effort by the SFO to highlight the benefits of co-operation.

The largest DPA in the UK to date was entered into by Airbus SE (Airbus) in January 2020 following an investigation into allegations that the company had used external consultants to bribe customers to buy civilian and military aircraft. Airbus agreed to pay a financial penalty of EUR983.97 million plus the SFO's costs of EUR6.9 million, as part of a EUR3.6 billion global resolution, which also included separate settlements with prosecutors in France and the US.

In July 2020, a DPA was entered into by G4S Care & Justice (UK) Ltd (G4S), following an investigation into allegations that G4S had made various misrepresentations about profits made under private government contracts between 2011 and 2013. G4S agreed to pay a financial penalty of £38,513,277 in addition to the SFO's costs of £5,952,711. Following the publication of guidance on its approach to compliance programmes which foreshadowed the greater use of monitors, and in line with the expectation that the use of monitorships would increase under Lisa Osofsky's directorship at the SFO, an external and independent "Reviewer" (a monitor in all but name) will be appointed at G4S, to provide what Ms Osofsky referred to as "unprecedented, multi-year scrutiny and assurance".

Most recently, in October 2020, the SFO announced it had entered into its latest DPA, with Airline Services Ltd. The company admitted to three counts of failing to prevent bribery arising from its use of an agent to win contracts worth a total of £7.3 million. As a result, ASL is required to pay a financial penalty of £1,238,714, disgorgement of £990,900 and a contribution of £750,000 to the SFO's legal costs.

The judge approving the ASL DPA again emphasised the importance of self-reporting and co-operation, indicating that while corporate offending will be met with the imposition of penalties "over and above the disgorging of profit wrongly made", that the discount in the case provides "a positive and substantial incentive towards self-reporting and co-operation". In this case, the misconduct became known following an internal investigation instigated by ASL, the findings of which were swiftly disclosed to the SFO.

In all cases, the judgments approving the DPAs emphasised the importance of full co-operation on the part of the relevant companies as a key precondition to any settlement. In the case of G4S, a 40% reduction was applied to the financial penalty to reflect the company's delayed, but subsequently full, co-operation with the SFO. In other cases where companies have demonstrated "extraordinary co-operation", the discount applied has been as high as 50%.

The importance of self-reporting has also been emphasised in cases involving the offence of failing to prevent bribery under section 7 of the *BA 2010*. In February 2016, Sweett Group PLC (Sweett) was fined £2.25 million as part of a prosecution related to payments made in connection with securing and retaining contracts in the United Arab Emirates between December 2012 and December 2015. The SFO declined to enter into a DPA largely as a consequence of the timing of the company's self-report to the SFO (which coincided with impending press reports in relation to the conduct in question) and failures to provide full co-operation throughout the investigation.

Availability of adequate procedures defence

It is a defence against the corporate offence of failing to prevent bribery if an organisation can prove that it "had in place adequate procedures designed to prevent persons associated with [the organisation] from undertaking such conduct" (*section 7(2), BA 2010*). This analysis is highly fact sensitive and will be based heavily on factors including the size and complexity of the organisation, and the sectors and geographies in which it does business. For an overview of how to create an anti-corruption policy that helps to demonstrate that a company had adequate procedures in place to prevent bribery, see *Practice note, Bribery Act 2010: anti-corruption policies*, which includes information based on the UK Ministry of Justice's *Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing (section 9 of the Bribery Act 2010)*.

Regime in China

There are two main sources of anti-corruption law in China:

- *Criminal Law of the PRC 1997* (1997 Criminal Law, last revised in 2017). This contains anti-bribery provisions relating to Chinese and foreign officials, as well as the criminal offence of commercial bribery.
- *Anti-unfair Competition Law 2019* (2019 AUCL). This covers the administrative offence of commercial bribery, which is treated less seriously than the criminal offence. The 2017 re-enactment of the AUCL updated the scope, elements and other aspects of commercial bribery (for more information, see *Practice note, Chinese anti-unfair competition law: Commercial bribery*). Note that further revisions to the law were made in 2019 that did not affect the anti-corruption sections.

While China has historically been inconsistent in its enforcement of this legislation, guidance has elaborated on how these statutes are expected to be applied. There is generally no obligation under Chinese law to report corrupt activity to Chinese authorities. However, there are narrow circumstances in which reporting obligations could be interpreted as applying, and there are prudential considerations that are relevant to the decision to disclose. For a detailed examination of the liability that can arise under Chinese anti-bribery legislation, see *Practice note, Bribery and corruption offences, enforcement and penalties: China*.

Reporting obligations in China

In August 2014, Chinese authorities issued the *Interim Regulations on the Disclosure of Enterprise Information 2014*, which contain an obligation for entities to disclose penalties imposed by Chinese regulators. There is some speculation that this may require foreign corporations to disclose any actions brought against them by the *State Administration for Market Regulation* (SAMR) or its local branches, which conduct civil enforcement actions involving allegations of commercial bribery. In practice, however, the SAMR and its local branches usually publish their enforcement actions in the official enterprise credit information disclosure system (for more information on the disclosure system, see *Practice note, Understanding the 2013 Company Law reforms: China: Enterprise information disclosure system*). Before April 2018, the predecessor authority of the SAMR was the *State Administration for Industry and Commerce* (SAIC). (For more information, see *Practice note, Understanding the 2018 government institutional reform: China: Market supervision: a mega-sized regulator*.)

(For more information on these reporting obligations, see *Practice note, Understanding the 2013 Company Law reforms: China: Ongoing notification obligations*.)

Practical considerations when deciding whether to report to Chinese authorities

There are several significant practical considerations that should factor into the decision of whether to disclose to Chinese authorities allegedly corrupt behaviour by an agent in China.

Potential to mitigate punishment

Under the *1997 Criminal Law*, if an individual or corporate entity accused of bribery voluntarily confesses to the authorities before prosecution begins, they may be eligible for mitigated punishment or a waiver of punishment (*Article 390*). Guidance issued by Chinese authorities that took effect in January 2013 confirmed this position (*Interpretation of the Supreme People's Court and Supreme People's Procuratorate on Certain Issues concerning Specific Application of the Law in Handling Criminal Cases involving Bribery 2012* (2012 Bribery Interpretation, with effect from 1 January 2013)).

Persons convicted of bribery may still be eligible for leniency in sentencing post-prosecution if they confess to the criminal conduct (*Article 8, 2012 Bribery Interpretation*) or expose other crimes committed by the bribe taker (*Article 9, 2012 Bribery Interpretation*). However, full mitigation such as a suspended sentence or exemption from punishment is not available in several circumstances, including when:

- The bribe giver provided bribes to more than three people.
- The bribe giver was previously subject to an administrative or criminal penalty for bribery.
- The bribes were provided to carry out illegal activities.
- The bribery resulted in severe consequences.

(*Article 10, 2012 Bribery Interpretation*.)

In August 2015, China amended the 1997 Criminal Law to revise the sentencing mitigation provision, allowing the waiver of punishment only when the briber-giver meets at least one of the following conditions:

- They committed no more than a relatively minor crime.
- They made "significant meritorious contributions" through their co-operation.

- They helped uncover a "major case".

This effectively raised the bar for bribe-givers to be exempted from punishment. For more information, see *Legal update, Criminal Law amendment: Changes to China's anti-bribery regime*.

In April 2016, the *Supreme People's Court* (SPC) and the *Supreme People's Procuratorate* (SPP) issued the *Interpretations on Certain Issues Concerning the Application of Law in Handling Criminal Cases Involving Embezzlement and Bribery 2016* (2016 Criminal Bribery Offences Interpretation). This document further clarified the circumstances under which punishment may be mitigated by voluntary disclosure. For example, it defined "relatively minor crime", and also clarified what it means to provide substantial assistance in a "major case", such as providing new evidence that helps officials in an on-going or new investigation, or providing evidence that is used to capture a fugitive or illegally acquired property. For more information, see *Legal update, SPC and SPP issue interpretation on Criminal Law provisions on bribery and corruption*.

With regard to administrative actions, local branches of the SAMR may also use their discretion to consider certain mitigating factors when issuing punishment (see *Guiding Opinions of the SAMR on Regulating the Discretionary Power of Administrative Punishments in Market Supervision and Administration 2019* (市场监管总局关于规范市场监督管理行政处罚裁量权的指导意见)). For example, a guideline issued by the Beijing branch of the SAIC in December 2017 stated that the agency may grant "light penalties" (that is, constituting less than 30% of the range between the lowest and highest permitted penalty) when the bribe-giver voluntarily reports misconduct (*Article 24(4), Implementation Measures for Administrative Punishment Discretion of Beijing Administration for Industry and Commerce (Trial) 2017* (北京市工商行政管理局行政处罚裁量权实施办法(试行))).

Regime in Hong Kong

Hong Kong's *Prevention of Bribery Ordinance, Cap 201* (POBO) is enforced by the Independent Commission Against Corruption (ICAC), which investigates alleged corrupt practices, and the Department of Justice, which is responsible for prosecuting corruption charges. There is no general obligation to report corrupt activity under Hong Kong law, although alternative reporting mechanisms may ultimately compel an organisation to report potential corruption.

Reporting obligations in Hong Kong

Requirements under Hong Kong anti-money-laundering statutes

Financial institutions may have obligations to report knowledge or suspicion that property in its possession constitutes proceeds from bribery. Hong Kong's anti-money laundering and anti-terrorist financing scheme is comprised of several ordinances, including the:

- *Drug Trafficking (Recovery of Proceeds) Ordinance, Cap 405*.
- *Organised and Serious Crimes Ordinance, Cap 455*.
- *United Nations (Anti-Terrorism Measures) Ordinance, Cap 575*.
- *Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance, Cap 615*.

These provisions are breached if an individual fails to disclose any knowledge or suspicion that property represents the proceeds of an indictable offence. Many POBO violations are likely also to constitute indictable offences under Hong Kong's money laundering legislation. Financial institutions and other entities subject to Hong Kong's money laundering legislation should consider possible obligations to report relevant information related to potential bribery.

Requirements that listed companies disclose corrupt behaviour

The *Hong Kong Stock Exchange* (HKEx) encourages reporting on environmental, social and governance (ESG) matters, including an issuer's corruption compliance. This includes information on the issuer's anti-corruption policies and compliance and material non-compliance with relevant standards, rules and regulations on bribery, extortion, fraud and money laundering. In December 2015, the HKEx amended its Listing Rules to take ESG reporting from a best practice to a requirement that corporations "comply or explain".

Practical considerations when deciding whether to report to Hong Kong authorities

Hong Kong law does not provide that self-reporting of bribery by an organisation leads to a reduction in the sentence of an offender, although it does grant leniency for corporate self-disclosure of other crimes. (For example, anti-trust violation, see *Hong Kong Competition Commission, Leniency Policy for Undertakings Engaged in Cartel Conduct*). Individuals who commit a bribery offense may also be granted leniency or in certain exceptional circumstances even immunity from prosecution when they voluntarily self-disclose. For more information about immunity and leniency under the Hong Kong regime, see *Country Q&A, Financial crime in Hong Kong: overview: Immunity and leniency*.

Any evaluation of whether to report conduct to Hong Kong authorities should include careful consideration of whether the conduct is likely to be pursued by other governments, and the benefits of self-disclosure arising from disclosing the conduct to the Hong Kong authorities.

END OF DOCUMENT