



AMERICAS INVESTIGATIONS REVIEW 2023

The Americas Investigations Review is one of those reviews. It contains insight and thought leadership from 15 pre-eminent practitioners from the region. Spanning 83 pages, this particular review is part retrospective, part primer, part crystal ball – and 100 per cent essential reading.

Inside you'll read about some of the most important developments affecting international investigations in North and Latin America, supported throughout with footnotes and relevant statistics. This edition focuses on the US and Mexico in particular and has an overview on the exigencies of ESG and crypto-related investigations.

Visit globalinvestigationsreview.com
Follow [@GIRalerts](https://twitter.com/GIRalerts) on Twitter
Find us on [LinkedIn](https://www.linkedin.com/company/global-investigations-review)

Contents

 While reading, click this icon to jump back to the Contents at any time

Forensic techniques to investigate emerging trends	1
Jenna Voss, Masako Asaka and Umair Nadeem <i>Forensic Risk Alliance</i>	
Key considerations in US government investigations	20
Arian M June, Winston M Paes and Douglas S Zolkind <i>Debevoise & Plimpton LLP</i>	
In Re Boeing emphasises risk-based governance	43
Darryl Lew and Courtney Hague Andrews <i>White & Case LLP</i>	
On the horizon: more cyber investigations from a growing number of federal agencies	54
Michael Bahar, Garrett Gibson, Jay Patel and Ronald Zdrojeski <i>Eversheds Sutherland LLP</i>	
Non-trial resolutions as an overlooked ally in the Mexican fight against corruption	67
Diego Sierra, Raymundo Soberanis and Pablo Fautsch <i>Von Wobeser y Sierra, SC</i>	

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer–client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. Although the information provided was accurate as at August 2022, be advised that this is a developing area.

Preface

Welcome to the Americas Investigations Review 2023, one of Global Investigations Review's special reports. Global Investigations Review (for newcomers) is the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing. We tell them all they need to know about everything that matters, in their chosen professional niche.

Day in day out, we provide our readers with the most useful daily news, surveys and features; organise the liveliest events (GIR Live); and build innovative tools and know-how products to make working life more efficient.

In addition, with the aid of external contributors, we curate a range of comprehensive regional reviews that go deeper into developments than the exigencies of journalism allow.

Americas Investigations Review is one of those reviews. It contains insight and thought leadership from 15 pre-eminent practitioners from the region. Spanning over 80 pages, this particular review is part retrospective, part primer, part crystal ball – and 100 per cent essential reading. All contributors are vetted for their standing and knowledge before being invited to take part.

Inside you'll read about some of the most important developments affecting international investigations in North and South America, supported throughout with footnotes and relevant statistics. This edition focuses on the US and Mexico in particular and has an overview on the exigencies of ESG and crypto-related investigations.

As so often with our annual reviews, a close read yields many gems. On this occasion, for this reader, they included that:

- cryptocurrency investigations are on the rise – even before the arrival of bespoke regulation;
- the second part of Muhammad Ali's 'float like a butterfly sting like a bee' line ('the hands can't hit what the eye can't see') is a good metaphor for what the US Department of Justice (DOJ) expects from your compliance programme (see the chapter on *Re Boeing* for more);
- the DOJ also wants more cybersecurity-related whistleblowers; and
- Mexico is not one of the 23 OECD members that have now completed an anti-bribery case, but that might be about to change – assuming the right prosecutor comes along.

And much, much more

If you have any suggestions for future editions, or want to take part in this annual project, we would love to hear from you. Please write to insight@globalarbitrationreview.com.

David Samuels

Publisher, Global Investigations Review

August 2022

Key considerations in US government investigations

[Arian M June](#), [Winston M Paes](#) and [Douglas S Zolkind](#)*

[Debevoise & Plimpton LLP](#)

In summary

Guiding a client through a US government investigation requires advising on a myriad of complex strategic decisions. This article outlines certain critical considerations for companies and their counsel as they navigate criminal, civil and regulatory investigations, whether being led by the Department of Justice or an agency such as the Securities and Exchange Commission, the Commodity Futures Trading Commission or the Office of Foreign Assets Control.

Discussion points

- At the outset of a US government investigation, counsel should evaluate how the investigation began and how far it has progressed to assess how best to respond.
- Careful consideration must be given to undertaking an internal investigation if the company has not already done so.
- Cooperation (including self-reporting any new violations) carries significant benefits and risks, and must be tailored to the specific agency's expectations.
- Care must be taken to engage with the government and respond to requests without waiving the attorney-client privilege or other applicable privileges.
- Parallel investigations by multiple federal, state or foreign agencies carry unique challenges and require careful coordination.

Referenced in this article

- US Department of Justice, Justice Manual, Principles of Federal Prosecution of Business Organizations
- US Securities and Exchange Commission, Enforcement Manual
- US Commodity Futures Trading Commission, Enforcement Manual
- US Department of Treasury, Office of Foreign Assets Control, Enforcement Guidelines
- Memorandum from DOJ Deputy Attorney General Lisa O Monaco, 'Corporate Crime Advisory Group and Initial Revisions to Corporate Criminal Enforcement Policies'



In the early stages of a US government investigation, a company will often face daunting decisions that can have an outside impact on the course of the investigation for months or years to come. As discussed below, some of the important considerations are: (1) evaluating how the investigation began and how far it has progressed; (2) preserving potential evidence and other data; (3) deciding whether to launch an internal investigation; and (4) engaging with the investigating agency while protecting the attorney-client privilege.

How did the investigation begin?

US government investigations may be initiated in many different ways. Understanding how the investigation began can provide insight into how far it has progressed, which is a key factor to consider in deciding how best to respond.

Whistleblowers

The US legal system contains a variety of state and federal mechanisms that incentivise and shield individuals who come forward to report potential misconduct. In recent decades, the DOJ increasingly has used the False Claims Act (FCA)¹ to prosecute a broad range of false monetary claims submitted to the government, often relying on whistleblowers who are incentivised to bring lawsuits on behalf of the US government.²

The Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC) and Treasury Department also have effective whistleblower programmes. Under the Sarbanes-Oxley Act of 2002³ and Dodd-Frank Act of 2010,⁴ individuals may report voluntarily to the SEC 'original information' about potential violations of US securities laws. In fiscal year 2021, the SEC received a record-breaking number of whistleblower tips – more than 12,200 – from individuals in 99 foreign countries.⁵ The CFTC operates a virtually identical whistleblower programme under section 23 of the Commodity Exchange Act,⁶ which allows individuals to report potential violations of US commodities laws to the CFTC. The Treasury Department's whistleblower programme has been significantly bolstered by the recent passage of laws. On 1 January 2021, the Anti-Money Laundering Act of 2020 took effect, enhancing the Treasury

¹ 31 U.S.C. § 3729 et seq.

² See, eg, U.S. Dep't of Justice, 'Justice Department's False Claims Act Settlements and Judgments Exceed \$5.6 Billion in Fiscal Year 2021' (Feb. 1, 2022), available at <https://www.justice.gov/opa/pr/justice-department-s-false-claims-act-settlements-and-judgments-exceed-56-billion-fiscal-year> (discussing FCA recoveries in fiscal year 2021).

³ 15 U.S.C. § 7201 et seq.

⁴ 12 U.S.C. § 5301 et seq.

⁵ U.S. Securities and Exchange Comm'n, '2020 Annual Report to Congress – Whistleblower Program' (Nov. 16, 2021), available at https://www.sec.gov/files/2021_OW_AR_508.pdf.

⁶ 7 U.S.C. § 1 et seq.



Department's whistleblower award programme to encourage reporting on financial institutions' violations of the Bank Secrecy Act. And in March 2022, the Treasury Department established a new whistleblower programme pursuant to the Kleptocracy Asset Recovery Rewards Act. The Kleptocracy Asset Recovery Rewards Program offers up to US\$5 million to whistleblowers who provide information that leads to the seizure, restraint, forfeiture or repatriation of assets linked to foreign government corruption.⁷

Government officials report that whistleblowers continue to provide immense value to investigators. As insiders or individuals with knowledge of the workings of the target company, whistleblowers often have the ability to influence investigators' view of otherwise ambiguous conduct, particularly early on in a government investigation.

The most effective way for companies to mitigate whistleblower risks is to create and foster a compliance culture that encourages internal reporting and addresses complaints with as much transparency as possible. A robust compliance programme, coupled with easily accessible whistleblower and anti-retaliation policies, will provide comfort to employees by making it clear that improper conduct will not be tolerated and reassuring employees that their complaints will be handled sensitively and seriously. Companies should also establish an ethics policy that requires personnel to comply with all applicable legal duties and sets forth specific requirements in areas more prone to violations. Companies should ensure these programmes are implemented through robust and regular training, and provide routine surveys and checks to ensure the programme is meeting its desired goals.

Where a government investigation has been launched based on a whistleblower report, the target company is already at a significant disadvantage. The government is likely in possession of sensitive and potentially damaging information, including key documents or even recordings of meetings. Government investigators typically will not disclose to the company that the government has received a whistleblower report. In such circumstances, it would be prudent to undertake an internal investigation. However, special care must be taken to avoid even the appearance of retaliatory conduct. An investigation can be critical in developing additional facts and providing context to counterbalance the prevailing government narrative.

⁷ U.S. Dep't of Treasury, 'Kleptocracy Asset Recovery Rewards Program', <https://home.treasury.gov/about/offices/terrorism-and-financial-intelligence/terrorist-financing-and-financial-crimes/kleptocracy-asset-recovery-rewards-program> (last visited 27 June 2022).



Subpoena or other formal request

Companies often learn of a government investigation for the first time when they receive a formal written notice demanding the disclosure of documents and information. In criminal investigations, the DOJ typically issues these demands in the form of a grand jury subpoena. A corporation has no Fifth Amendment privilege against self-incrimination⁸ and therefore cannot refuse to produce records, even if it is the target of the investigation.

Many federal agencies are also statutorily authorised to issue administrative subpoenas compelling document production and testimony.⁹ These subpoenas are similar to grand jury subpoenas, except they are issued in an agency's name. Another investigative tool is the Civil Investigative Demand (CID), a compulsory procedure used to obtain documents, answers to interrogatories and oral testimony. CIDs are often used by the Federal Trade Commission and the DOJ's Antitrust and Civil Divisions.

Upon receipt of a subpoena or CID, a reasonable first step is often to begin a dialogue with the government agency. While it is not always necessary to retain outside counsel to handle this outreach, it may be wise to do so, especially if it is clear from the demands that the government is focused on a sensitive subject area or critical part of the business.

Key questions to try to answer are: What is the focus of the government's investigation? Is the investigation targeting the company or some other entity or person? How far along is the investigation? Answers to these questions will inform counsel's advice about what approach to take. Every situation is unique, but common approaches include negotiating with the government to narrow the subpoena, offering to provide a live presentation on the facts in lieu of a subpoena response in the first instance, or – if the demand seems unduly burdensome or baseless – trying to persuade the government to drop the demand, or pursuing a challenge in court. Depending on the circumstances, counsel may also advise the company to undertake an internal investigation to get to the bottom of what the government is investigating.

Awareness of government investigations in the same industry

Government agencies often focus their enforcement efforts on particular industries where many firms engage in similar practices that prosecutors or regulators believe to be problematic. Thus, when news breaks of a government investigation or corporate resolution in a particular industry, it can be a potent warning sign to other industry participants that they may soon be under investigation too, if they are not already.

⁸ See *Curcio v. United States*, 354 U.S. 118, 122 (1957).

⁹ See, eg, 15 U.S.C. § 78dd-2(d)(2) (DOJ); 15 U.S.C. § 77s(c) (SEC); 7 U.S.C. § 9(5)-(6) (CFTC).



Companies and their counsel should therefore pay close attention to enforcement trends in their industry. When they learn of an investigation or enforcement action involving a peer company, it can be wise to conduct an immediate risk assessment to evaluate the likelihood that employees at their company have engaged in similar conduct. If that risk assessment yields troubling results – or if a deeper dive otherwise seems prudent – serious thought should be given to retaining outside counsel to conduct an internal investigation. Such efforts will also put the company in a better position if it identifies misconduct and decides to self-report to the government, as the benefits of self-reporting and cooperating are greatest when a company acts proactively before it is contacted by the government.

Since late 2021, for example, multiple government agencies, including the SEC, CFTC and DOJ, and various state attorneys general, have indicated an intense focus on companies in the cryptocurrency space.¹⁰ These enforcement efforts serve as a warning sign to other market actors, and provide an opportunity for companies to get ahead of the curve.

Self-reporting

Some investigations begin when a company voluntarily discloses potential violations to a US government agency. Many companies self-report in the hopes of obtaining a more favourable resolution, but this should not be an automatic decision. Any organisation considering whether to self-disclose should carefully weigh the potential benefits and risks.

Benefits of self-reporting

In recent years, US agencies have actively promoted incentives for self-disclosure. For example, in 2017, the DOJ updated the Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy to require voluntary self-disclosure as a necessary prerequisite to full cooperation credit.¹¹ In early 2018, DOJ officials announced that the principles delineated in the Corporate Enforcement Policy

¹⁰ See, eg, U.S. Dep't of Justice, 'Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team' (Oct. 6, 2021), available at <https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team>; U.S. Securities and Exchange Comm'n, 'SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit' (May 3, 2022), available at <https://www.sec.gov/news/press-release/2022-78>; 'Testimony of CFTC Chairman Rostin Behnam Regarding "Examining Digital Assets: Risks, Regulation, and Innovation"' before the U.S. Senate Committee on Agriculture, Nutrition, and Forestry (Feb. 9, 2022), available at <https://www.cftc.gov/PressRoom/SpeechesTestimony/opabehnam20>.

¹¹ See U.S. Dep't of Justice, Justice Manual § 9-47.120 (FCPA Corporate Enforcement Policy) (2018), <https://www.justice.gov/jm/justice-manual> (hereinafter Justice Manual).



would guide non-FCPA criminal corporate investigations as well.¹² In a June 2022 speech, Deputy Attorney General Lisa Monaco stated bluntly that '[t]he math is simple: self-disclosure can save a company hundreds of millions of dollars'.¹³

Likewise, the SEC has emphasised the importance of self-reporting in obtaining a successful resolution. In May 2022, the Director of the SEC's Division of Enforcement, Gurbir Grewal, made clear that 'when clients take steps to self-report potential violations, or to proactively cooperate with our investigations and remediate violations, the Commission is often willing to credit that cooperation, including through reduced penalties, or even no penalties at all'.¹⁴

In some cases, self-reporting may better enable an organisation to maintain direction and control over the course of the investigation. The company's information is most valuable to the government where (1) the government is not already aware of the misconduct, and (2) the government is unlikely to discover the misconduct by other means. In such circumstances, if a company can show the government that it is conducting a thorough investigation and making a full, voluntary disclosure, it has a better opportunity to frame the narrative before the government has cemented an inaccurate or excessively negative view.

Risks of self-reporting

Self-reporting may have serious consequences that should be thoroughly considered. Self-reporting risks 'throwing open the doors' to lengthy and costly organisational examinations. Enhanced government scrutiny may mean the matter quickly escalates beyond the bounds of the initial wrongdoing uncovered. This may be particularly risky where the misconduct turns out to be fairly confined and easily remediated by the company. When deciding to self-report, a company should be prepared to commit to a full-blown, well-resourced investigation and to report on all findings to the government, no matter what facts the investigation uncovers.

Further, counsel should consult the relevant agency's guidelines for what qualifies as 'voluntary self-disclosure'. Some agencies have stringent requirements. For example, the Office of Foreign Assets Control (OFAC) declines self-disclosure

¹² Remarks by John Cronan, Acting Ass't Att'y Gen., Crim. Div., U.S. Dep't of Justice, and Benjamin Singer, Chief, Securities and Financial Fraud Unit, Fraud Section, Crim. Div., DOJ, at the American Bar Association's 32nd Annual National Institute on White Collar Crime (Mar. 1, 2018), details of which are available at <https://www.law360.com/articles/1017798/doj-expands-leniency-beyond-fcpa-lets-barclays-off>.

¹³ U.S. Dep't of Justice, 'Deputy Attorney General Lisa O. Monaco Delivers Keynote Remarks at 2022 GIR Live: Women in Investigations' (June 15, 2022), available at <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-keynote-remarks-2022-gir-live-women>.

¹⁴ Gurbir S Grewal, Dir., SEC Div. of Enf't, Remarks at Securities Enforcement Forum West (May 12, 2022), available at <https://www.sec.gov/news/speech/grewal-remarks-securities-enforcement-forum-west-051222>.



credit where the disclosure ‘is materially incomplete’ or does not include ‘a report of sufficient detail to afford a complete understanding of an apparent violation’s circumstances’.¹⁵ Organisations should also recognise that voluntary self-disclosure is often merely one component needed to receive full cooperation credit. If a company is not prepared to meet all agency-specific cooperation obligations (which are discussed further below), the potential benefits of self-reporting could be obviated entirely.

Self-reporting may also draw the attention of other regulators, including other US agencies and global regulators, and may invite collateral litigation, such as shareholder derivative suits. Finally, there is no guarantee self-reporting will ultimately end in a successful resolution or reduced penalty.

Factors to consider in self-reporting

In weighing the potential risks and rewards of self-reporting, counsel should consider at least the following factors:

- Likelihood of detection: whether the misconduct will be detected by regulators through other means, such as a whistleblower or a regular audit or examination. Companies should also be cognisant of current enforcement trends; entities that operate in industries of high regulatory priority should be more wary of detection.
- Likelihood of prosecution: weighing the seriousness of the misconduct, including the frequency and pervasiveness of the violations, as well as the potential penalties at issue.
- Cooperation requirements: whether the organisation is prepared to meet potentially extensive cooperation obligations when opening the door to a US government agency.
- Commercial costs: inviting the government to initiate an investigation has real-world financial costs. Business operations are likely to be diverted as employees are called upon to meet the regulator requests.
- Reputational risk: self-reporting raises a high likelihood that the conduct could ultimately be disclosed publicly, even if the investigating agency declines to prosecute or pursue an enforcement action.

¹⁵ 31 C.F.R. pt. 501, app. A § (l)(l).



Data preservation

At the outset of a US government investigation, a company must promptly take reasonable steps to preserve evidence and other data. Failure to do so may violate legal requirements and additionally could lead to adverse inferences regarding the company's culpability.¹⁶

Broadly, counsel should take steps to identify the need for a legal hold on materials, determine the scope of the data required, and develop instructions for its preservation. The hold should be issued as soon as possible, identifying key custodians and instructing them not to delete or otherwise alter relevant data. Counsel should work with the company's IT department to confirm automated deletions are managed appropriately, data is properly collected and preserved, and responses and acknowledgements of hold responsibilities are tracked. Regulators provide differing guidance on preservation requirements, which may also be useful to keep in mind.¹⁷

Over the past two years, additional considerations have arisen as a result of the covid-19 pandemic, during which personal and professional data have become intermingled at many organisations. While working from home, many employees have conducted work on personal devices that exist outside corporate systems and are typically not protected with enterprise-grade security mechanisms. This shift has led to increased government scrutiny that such technology may be used to facilitate unlawful or inappropriate conduct (such as receiving and trading on insider tips, rate rigging, employment discrimination, or spoliation of evidence). While employees rely on ephemeral messaging apps as a functional equivalent of off-the-record phone calls, courts and law enforcement may adopt the position that, like email, the messages constitute business records that may be subject to retention and preservation requirements. This is particularly salient as US regulators are increasingly seeking business-related messages from employees' personal devices. Indeed, the SEC and CFTC are conducting sweeping investigations across the US securities industry regarding whether bank employees have used personal means of communication to discuss business matters, in violation of the record-keeping obligations imposed on broker-dealers under federal securities laws.¹⁸

¹⁶ See, eg, SEC Enforcement Manual § 3.2.9.4 [discussing duty to preserve records]; *U.S. v. Arthur Andersen, LLP*, 374 F.3d 281 (5th Cir. 2004) [affirming conviction of company for obstructing government investigation], rev'd on other grounds, *Arthur Andersen LLP v. U.S.*, 544 U.S. 596 (2005).

¹⁷ See, eg, Justice Manual §§ 9-5.004 (Guidance on the Use, Preservation, and Disclosure of Electronic Communications in Federal Criminal Cases), 9-47.120 (FCPA Corporate Enforcement Policy), 9-48.000 (Computer Fraud and Abuse Act); SEC Enforcement Manual §§ 3.2.9.4, 3.2.9.6 to 3.2.9.9; CFTC Enforcement Manual §§ 5.10, 9.1.

¹⁸ See, eg, Press Release, U.S. Securities and Exchange Comm'n, 'JPMorgan Admits to Widespread Recordkeeping Failures and Agrees to Pay \$125 Million Penalty to Resolve SEC Charge' (Dec. 17, 2021), available at <https://www.sec.gov/news/press-release/2021-262>; Harry Wilson, 'HSBC Under Investigation in U.S. Over Whatsapp Use', Bloomberg (Feb. 22, 2022), available at <https://www.bloomberg.com/news/articles/2022-02-22/hsbc-says-it-s-under-investigation-in-u-s-over-whatsapp-use>; Daniel Taub and Sridhar Natarajan, 'Goldman Probed by SEC Over Messages Sent Using Unapproved Services', Bloomberg (Feb. 25, 2022), available



In anticipating these issues, firms should consider how to locate and collect such data. Enhanced security and employee training may help address immediate concerns, while reassessing the location of servers and the manner in which data is stored may help mitigate foreign privacy concerns, particularly at global firms. Companies may find it helpful to consult with foreign legal counsel as to what is permissible in particular jurisdictions. Where particular employees are of concern, companies may also want to be especially mindful of how to balance collection and preservation with the risk of potentially informing custodians, who could in turn attempt to destroy data. Companies should craft a plan to retrieve data from furloughed or dismissed employees, and may consider implementing requirements for the return of devices and data in severance arrangements.

Whether to undertake an internal investigation

Once a company is put on notice of a US government investigation – whether through a subpoena, formal notice, leak or other means – and especially if the firm has not already rigorously investigated the subject matter – careful thought should be given to retaining outside counsel to lead a comprehensive internal investigation.

Benefits of an internal investigation

A company that proactively conducts an internal investigation will be better situated to navigate a government investigation. If the company expends the effort and resources to learn the facts, it can make informed decisions as to how to proceed and what posture to take with the government.

An internal investigation often opens the door to cooperation. In any government investigation, the nature and severity of the penalty will depend in part on whether, and how robustly, the company cooperated in the investigation. Whether or not to cooperate is a complex question, but if the company fails to carry out an internal investigation, the path to cooperation is significantly narrowed.

In the eyes of the government, internal investigations demonstrate the organisation's commitment to good corporate governance and a culture of compliance. The investigational findings may enable the company to proactively remediate the harm (potentially staving off future inquiries, litigation or reputational harm), while also demonstrating the company's good faith and diligence to the investigating agency.

at <https://www.bloomberg.com/news/articles/2022-02-25/goldman-probed-over-messages-sent-using-unapproved-services>; Daniel Taub, 'Citi Is Latest Bank to Be Probed Over Unapproved Messaging Services', Bloomberg (Feb. 28, 2022), available at <https://www.bloomberg.com/news/articles/2022-02-28/citi-is-latest-to-be-probed-over-unapproved-messaging-services>.



Additional factors to consider

Internal investigations can be extremely expensive, time-consuming and distracting to the business. A company should assess whether it can effectively respond to the government's requests without launching an investigation. It may also wish to conduct a preliminary inquiry using in-house lawyers to test the waters – this inquiry should be conducted in a manner that protects the attorney-client privilege. If no evidence of misconduct emerges during an initial inquiry, the company may decide not to devote further resources to an internal investigation conducted by outside counsel.

There are instances when the investigative agency may be opposed to the company conducting an internal investigation. This is especially true when the investigative agency has concerns about the company's or its counsel's ability to disclose all the facts and fully cooperate with the investigation. In these situations, the investigative agency may view an internal investigation as doing more harm than good by 'trampling the crime scene'. When conducted poorly or by inexperienced counsel, an internal investigation may be counterproductive by developing a self-serving record, or worse, creating the appearance of influencing witnesses. Thoughtful investigations are designed and executed to avoid future allegations from government agencies that the company followed a flawed, biased or incomplete process. When the government agency is aware that the company is conducting an internal investigation, it is good practice to be transparent and provide the government with an overview of the investigation so there is no misunderstanding about the scope of the investigation.

Privilege considerations

When engaging with government agencies and responding to their requests, special care must be taken to avoid inadvertently waiving privilege. In general terms, the attorney-client privilege shields confidential communications between an attorney and a client for the purpose of providing legal advice.¹⁹ The work-product privilege protects materials prepared by or at the direction of lawyers in anticipation of litigation.²⁰ In this section, we discuss a number

¹⁹ See *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981); *In re Brown & Root, Inc.*, 756 F.3d 754, 757 (D.C. Cir. 2014).

²⁰ See *Hickman v. Taylor*, 329 U.S. 495, 510–12 (1947).



of questions that should be top of mind when embarking on responding to a government investigation or conducting an internal investigation.

Who will lead the inquiry?

At the outset of an investigation, companies must determine who will direct and conduct the inquiry. Differences between in-house and outside counsel, as well as attorneys and non-attorneys, can lead to meaningfully different privilege protections.²¹ Privilege shields communications and work-product with legal purpose, and can therefore be compromised if an investigation is conducted by in-house counsel that performs both legal and non-legal functions. In cases where the need to preserve privilege is a strong consideration, companies are best served by retaining outside counsel.

In addition to preserving privilege, the use of outside counsel may bolster the credibility and quality of the investigation, particularly where underlying allegations concern a company's board or senior management. Even in routine matters where outside counsel are not regularly engaged, companies should consider whether in-house counsel possess sufficient technical and substantive experience with the core issues. Relatedly, if the investigation is delegated to a company's internal compliance, audit or human resources teams, in-house counsel should supervise and direct the investigation, so as to preserve privilege to the extent possible.

What is considered privileged information?

Privilege is determined through an analysis of the facts and circumstances surrounding a communication. Contrary to many organisations' expectations, including an attorney as an email recipient or inviting an attorney to a meeting will not necessarily shield the content of the communication. A conversation with counsel that primarily deals with business matters may not be protected regardless of the attorney's presence. Companies may therefore want to be sensitive to the context of their communications and consider clearly articulating the bases of applicable privileges in the communications themselves. Doing so will help develop the necessary record to support a privilege determination at a later date.

²¹ See *In re Kellogg Brown & Root, Inc.*, 756 F.3d at 757–59 (upholding privilege where the investigation was led by in-house counsel and interviews were conducted by non-attorney, compliance employees because providing legal advice was a 'significant purpose' of the investigation); *Wultz v. Bank of China Ltd.*, 304 F.R.D. 384, 393 (S.D.N.Y. 2015) (distinguishing *Kellogg Brown & Root*'s attorney-led investigation from the internal investigation led by a compliance officer, who lacked the purpose of providing legal advice).



The underlying facts of an investigation are generally not protected from disclosure.²² A witness could therefore be asked about the existence of an attorney-client relationship, for example, without delving into any privileged communications. A witness could similarly be asked to discuss the facts of an event, provided the questioning does not veer towards divulging what the witness discussed with counsel. Facts therefore do not become privileged just because a client has discussed them with or learned them from their counsel. The dividing line between attorney-client communications and underlying facts is often case specific.

Companies should expect scrutiny from regulators on their assertions of privilege. In order to respond to investigators effectively, counsel must have a clear and defined basis for withholding materials. Failing to do so may cause them to lose credibility in the eyes of the regulators and may negatively impact the investigation in the long run.

When should privilege be waived?

Despite government policies regarding privilege protections,²³ companies can feel pressure to produce privileged and protected documents in exchange for potential leniency. However, disclosing privileged communications to anyone outside a company, including the government, almost always waives attorney-client privilege.²⁴ Accordingly, disclosure of privileged documents and materials to government sources runs the risk that those materials will be discoverable to third parties, including other government agencies or private plaintiffs. In short: leniency in one case may result in liability in another.

Counsel should strategically consider ways in which they can satisfy government information requests to obtain leniency, without waiving privilege. The DOJ, for example, explicitly states that privilege waivers are not a prerequisite for cooperation, but disclosure of all relevant facts is.²⁵ Using this guidance, one way to effectively collaborate with regulators is to share information in reports or presentations that exclusively contain facts uncovered during an internal investigation and withhold any work-product opining on those facts. Such a disclosure would avoid waiving privilege while simultaneously establishing robust cooperation with investigators. Even if government investigators promise to maintain confidentiality of the privileged documents disclosed to them, courts are likely to consider the privilege waived and will not countenance a later assertion by the company that the documents are still privileged. Nearly every circuit that has addressed attempts to selectively disclose privileged material

²² See *Upjohn Co.*, 449 U.S. at 395–96.

²³ See, eg, Justice Manual § 9-28.710 [Attorney-Client and Work Product Protections].

²⁴ See, eg, *In re Qwest Commc'ns Int'l Inc.*, 450 F.3d 1179, 1192–93 (10th Cir. 2006).

²⁵ See Justice Manual § 9-28.720 [Cooperation: Disclosing the Relevant Facts].



has held that sharing information with the government amounts to a waiver of that information as to third parties as well.²⁶

Cooperation considerations

In most instances, companies will benefit from cooperating with the government. However, there are rare circumstances that may warrant a more defensive approach. An organisation may choose to forgo cooperation where:

- it is factually unclear a violation occurred: the company does not believe the government's evidence is credible. The company has conducted its own internal investigation and has substantial reason to believe no violation, including a lesser violation, occurred;
- it is legally unclear a violation occurred: the investigating agency may be engaging in impermissible 'rulemaking by enforcement' and the legal basis for liability is unclear or unsupported by the company's assessment;
- the government's demands are intolerable: the investigating agency's penalty expectations are so severe or disproportionate to the misconduct that it would be impossible for the company to tolerate.

If an organisation decides to cooperate with the government, it should familiarise itself with the relevant agency's cooperation guidelines so as to maximise the likelihood of earning credit.

Cooperation credit guidelines

Each US government agency has different expectations for cooperation. Before engaging with the government, counsel should consult cooperation guidelines and policies for the relevant US agency. Agencies may also have differing guidelines based on the type of violation (for example, FCPA or FCA). This section explores the basic cooperation framework for the DOJ, SEC, CFTC and OFAC.

Department of Justice

The DOJ Justice Manual instructs that federal prosecutors consider a set of 11 factors when investigating and deciding whether to criminally charge a company. These factors, commonly known as the 'Filip Factors', include 'the corporation's willingness to cooperate'.²⁷ Cooperation credit is predicated on the company's

²⁶ See *In re Pac. Pictures Corp.*, 679 F.3d 1121, 1127 (9th Cir. 2012) (collecting cases); but see *Diversified Indus., Inc. v. Meredith*, 572 F.2d 596, 611 (8th Cir. 1978) (en banc).

²⁷ Justice Manual § 9-28.300 (Factors to Be Considered).



identification of all individuals ‘substantially involved in or responsible for the misconduct at issue’.²⁸ The company must provide the government with ‘complete factual information’ about these identified individuals.²⁹ However, the policy also acknowledges the practical difficulties of meeting this standard; accordingly, organisations may still earn cooperation credit where ‘despite its best efforts to conduct a thorough investigation, a company genuinely cannot get access to certain evidence’.³⁰

In the civil context, cooperation credit is awarded on a sliding scale, at the discretion of the DOJ attorneys handling the matter.³¹ To earn maximum cooperation credit, the organisation must (1) conduct a ‘timely self-analysis’, (2) proactively and voluntarily disclose the wrongdoing, and (3) ‘identify . . . all individuals substantially involved in or responsible for the misconduct’.³² However, even if the company does not qualify for maximum credit, an organisation may still receive some credit for providing ‘meaningful assistance to the government’s investigation’.³³ The DOJ will consider the factors ‘traditionally applied’ when assessing the extent of cooperation credit earned, including the timeliness, diligence, speed and proactive nature of the cooperation.³⁴

In October 2021, Deputy Attorney General Monaco announced major changes to the DOJ’s corporate enforcement policies, including enhancements to certain DOJ policies softened under the Trump administration.³⁵ First, Monaco indicated a return to the ‘Yates Memorandum’ standard on individual liability, which requires companies to disclose all relevant facts regarding all persons involved in corporate misconduct – both inside and outside the company – in order to obtain cooperation credit. The reimposition of this requirement may increase the burden that companies experience with investigations and provide prosecutors with additional leverage. Second, Monaco rescinded prior guidance that ‘monitorships are disfavored or are the exception.’³⁶ The DOJ is now ‘free to require the imposition of independent monitors whenever it is appropriate to do so’.³⁷ Finally, prosecutors must now consider all prior misconduct – and not just similar misconduct – in deciding whether to charge a corporation.³⁸ The Monaco Memorandum thus signals a more aggressive approach to corporate investigations and prosecutions. As a result, careful attention is required as companies decide whether and how to cooperate or self-disclose, and how to navigate DOJ investigations.

²⁸ Justice Manual § 9-28.700(A) (The Value of Cooperation).

²⁹ *id.*

³⁰ *id.*

³¹ See Justice Manual § 4-3.100(3) (Pursuit of Claims Against Individuals).

³² *id.*

³³ *id.*

³⁴ *id.*

³⁵ Memorandum from DOJ Deputy Att’y General Lisa O. Monaco, ‘Corporate Crime Advisory Group and Initial Revisions to Corporate Criminal Enforcement Policies’ (Oct. 28, 2021), available at <https://www.justice.gov/dag/page/file/1445106/download> (hereinafter the Monaco Memorandum).

³⁶ Monaco Memorandum, at 3.

³⁷ *id.*

³⁸ *id.*



Recent cases involving Glencore and Stericycle may be illustrative of the DOJ's approach moving forward.

In May 2022, Glencore International AG and Glencore Ltd pleaded guilty and agreed to pay over US\$1.1 billion to resolve investigations by authorities in the US, UK and Brazil into violations of the FCPA and a commodity price manipulation scheme.³⁹ According to the DOJ, Glencore did not receive full cooperation credit due to, among other things, delays in producing evidence, undertaking remedial measures and disciplining employees involved in the misconduct.⁴⁰ Additionally, because Glencore's new compliance enhancements have not been fully implemented or tested, an independent compliance monitor was imposed for a term of three years.⁴¹

In the prior month, April 2022, Stericycle, Inc agreed to pay over US\$84 million to resolve parallel FCPA investigations by authorities in the US and Brazil.⁴² In contrast to Glencore, the company received full cooperation credit, resulting in a 25 per cent penalty reduction, for 'proactively disclosing' evidence, 'providing information obtained through its internal investigation', 'making detailed factual presentations', 'voluntarily facilitating interviews in the United States of foreign-based employees', and 'producing voluminous relevant documents', 'including documents located outside the United States, accompanied by translation'.⁴³ The Department also noted that Stericycle had 'engaged in extensive remedial measures'.⁴⁴ Nevertheless, the DOJ imposed a two-year monitorship, suggesting that even such efforts may be insufficient to prevent the imposition of an independent compliance monitor.⁴⁵

Securities and Exchange Commission

In 2001, the SEC issued a Report of Investigation and Statement, commonly known as the Seaboard Report, laying out the framework for earning cooperation credit.⁴⁶ The report identifies four broad measures of cooperation, including (1) self-policing prior to the discovery of misconduct, (2) self-reporting the misconduct once discovered, (3) remediation efforts, and (4) cooperation

³⁹ id.

⁴⁰ Press Release, U.S. Dep't of Justice, 'Glencore Entered Guilty Pleas to Foreign Bribery and Market Manipulation Schemes' (May 24, 2022), available at <https://www.justice.gov/opa/pr/glencore-entered-guilty-pleas-foreign-bribery-and-market-manipulation-schemes>.

⁴¹ id.

⁴² Press Release, U.S. Dep't of Justice, 'Stericycle Agrees to Pay Over \$84 Million in Coordinated Foreign Bribery Resolution' (Apr. 20, 2022), available at <https://www.justice.gov/opa/pr/stericycle-agrees-pay-over-84-million-coordinated-foreign-bribery-resolution>.

⁴³ id.

⁴⁴ id.

⁴⁵ id.

⁴⁶ See U.S. Securities and Exchange Comm'n, Release Nos. 44969 and 1470, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions (2001), <https://www.sec.gov/litigation/investreport/34-44969.htm> (hereinafter the Seaboard Report).



with law enforcement authorities.⁴⁷ From there, the report lays out a series of 13 considerations the Commission will weigh ‘in determining whether, and how much, to credit self-policing, self-reporting, remediation and cooperation—from the extraordinary step of taking no enforcement action to bringing reduced charges, seeking lighter sanctions, or including mitigating language in documents we use to announce and resolve enforcement actions’.⁴⁸

Nevertheless, SEC Director of Enforcement Grewal has made clear that there is ‘no exhaustive checklist of what constitutes cooperation’, even if behaviour described in the Seaboard Report, such as self-reporting and remediation, ‘fall within the cooperation rubric’.⁴⁹ Director Grewal additionally warned that dilatory and obfuscatory tactics used by defence counsel (eg, in the course of document production or witness interviews) erode trust and may impair the company’s opportunity to obtain cooperation credit.⁵⁰

Grewal has pointed to the SEC’s January 2020 settlement with HeadSpin, Inc, a private technology company, as ‘an excellent example’ of the ‘types of remedial actions and cooperation [that] might be credited by the Commission after a company uncovers fraud’. The SEC had alleged violations of the anti-fraud provisions of federal securities laws, claiming that HeadSpin, through its chief executive officer (CEO), had falsely inflated financial metrics, which propelled the company’s valuation of over US\$1 billion.⁵¹ Once the board of directors became aware of the potential fraud, however, it undertook extensive remedial measures, including conducting an internal investigation, removing the CEO, hiring new senior management, revising its valuation, repaying investors, and implementing new compliance processes and procedures. HeadSpin neither admitted nor denied the allegations and the SEC imposed no financial penalties.

Commodity Futures Trading Commission

In recent years, the CFTC has issued several pieces of enforcement guidance on self-reporting, cooperation and remediation, which are incorporated into the agency’s Enforcement Manual.⁵² CFTC guidance emphasises that ‘ordinary cooperation’ is insufficient for credit; rather, the company’s conduct during an investigation should be ‘sincere, robustly cooperative and indicative of a

⁴⁷ See U.S. Securities and Enforcement Comm’n, Spotlight on Enforcement Cooperation Program (Sept. 20, 2016), <https://www.sec.gov/spotlight/enforcement-cooperation-initiative.shtml>.

⁴⁸ Seaboard Report.

⁴⁹ Gurbir S Grewal, Dir., SEC Div. of Enf’t, Remarks at Securities Enforcement Forum West (May 12, 2022), available at <https://www.sec.gov/news/speech/grewal-remarks-securities-enforcement-forum-west-051222>.

⁵⁰ id.

⁵¹ Press Release, U.S. Securities and Exchange Comm’n, ‘Remediation Helps Tech Company Avoid Penalties’ (Jan. 28, 2022), available at <https://www.sec.gov/news/press-release/2022-14>.

⁵² See CFTC Enforcement Manual, § 7 (Consideration of Self-Reporting, Cooperation, and Remediation).



willingness to accept responsibility for the misconduct'.⁵³ Broadly, the CFTC will consider (1) the value of the cooperation to the investigation, (2) the value of the cooperation to the CFTC's broader law enforcement interests, and (3) the culpability of the company (and other relevant factors).⁵⁴ The CFTC will also take into account any 'uncooperative conduct', such as failing to adequately respond to requests, failing to preserve relevant information or minimising the misconduct at issue.⁵⁵

For example, in January 2022, the CFTC reached a settlement with Blockratize, Inc for operating an unregistered and non-designated contract market.⁵⁶ According to the settlement order, Blockratize's cooperation 'significantly conserved the time and resources' of CFTC staff; the company voluntarily produced documents, presented analysis of its technology, and provided the staff with 'complete presentations of the facts of its operations, including identifying key persons and key documents'. The Commission recognised Blockratize's 'substantial cooperation' in the form of a reduced civil monetary penalty of US\$1.4 million.

US Department of Treasury, Office of Foreign Assets Control

OFAC's Enforcement Guidelines lay out a series of factors the agency considers when assessing the quality of cooperation.⁵⁷ Specifically, OFAC considers the 'nature and extent' of an entity's cooperation by assessing, among other items, (1) whether the organisation voluntarily self-disclosed the violation, (2) whether the organisation provided 'all relevant information' to OFAC, (3) whether the company investigated and disclosed other potential violations caused by the same underlying conduct, and (4) the nature and timeliness of responses to OFAC's requests.⁵⁸

In April 2021, OFAC reached a settlement with SAP SE, a German software company, to resolve violations related to the export of software from the US to Iran. OFAC considered SAP's 'substantial' cooperation to be a mitigating factor, including SAP's efforts to 'arrang[e] interviews with SAP employees'.⁵⁹ The DOJ likewise credited SAP for its 'voluntary disclosure to DOJ, extensive cooperation and strong remediation costing more than \$27 million', and agreed to a non-

⁵³ Div. of Enf't, CFTC, Enforcement Advisory: Cooperation Factors in Enforcement Division Sanction Recommendations for Companies (2017), <https://www.cftc.gov/sites/default/files/idc/groups/public/@enforcementactions/documents/legalpleading/enfadvistorycompanies011917.pdf>.

⁵⁴ id.

⁵⁵ id. at 6–7.

⁵⁶ Press Release, U.S. Commodity Futures Trading Commission, 'CFTC Orders Event-Based Binary Options Markets Operator to Pay \$1.4 Million Penalty' (Jan. 3, 2022), available at <https://www.cftc.gov/PressRoom/PressReleases/8478-22>.

⁵⁷ See 31 CFR pt. 501, app. A.

⁵⁸ id. §§ (III)(G)(1)–(6).

⁵⁹ Press Release, U.S. Dep't of Treasury, 'OFAC Settles with SAP SE for Its Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations' (Apr. 29, 2021), available at https://home.treasury.gov/system/files/126/20210429_sap.pdf.



prosecution agreement, no fine and disgorgement of US\$5.14 million in ill-gotten gains.⁶⁰

Navigating parallel investigations

We live in an era of heightened attention to white-collar enforcement, both domestically and globally. It is increasingly common for companies to face concurrent investigations by multiple US and foreign government agencies covering the same conduct. To successfully navigate such parallel investigations, counsel must keep a number of additional considerations in mind.

Parallel investigations by multiple US federal agencies

For several decades, the US federal government has made efforts to increase inter-agency cooperation.⁶¹ In 2018, the DOJ issued an 'anti-piling on' policy, instructing DOJ attorneys to 'coordinate with one another [as well as with other federal, local, state, or foreign authorities] to avoid the unnecessary imposition of duplicative fines, penalties, and/or forfeiture'.⁶²

Despite the government's pronouncements, parallel investigations are often marked – from a practitioner's perspective – by a distinct lack of coordination among agencies. US federal agencies have different guidelines and standards, different priorities and different personalities. It is crucial for the target company to understand how each regulator operates and what each regulator expects for a successful resolution.

Companies should also be prepared to assume responsibilities to centrally coordinate the investigation rather than counting on agencies to organise among themselves. Counsel should expend the effort to come up with a comprehensive plan for responding to requests, including – where feasible – combining responses and document productions.

⁶⁰ Press Release, U.S. Dep't of Justice, 'SAP Admits to Thousands of Illegal Exports of its Software Products to Iran and Enters into Non-Prosecution Agreement with DOJ' (Apr. 29, 2021), available at <https://www.justice.gov/opa/pr/sap-admits-thousands-illegal-exports-its-software-products-iran-and-enters-non-prosecution>.

⁶¹ See Memorandum from DOJ Att'y Gen. Janet Reno on Coordination of Parallel Criminal, Civil, and Administrative Proceedings (July 28, 1997), <https://www.justice.gov/archives/ag/ag-memo-coordinate-parallel-criminal-civil-administraative> (encouraging DOJ attorneys to 'coordinate an investigative strategy'); Memorandum from DOJ Att'y Gen. Eric M. Holder on Coordination of Parallel Criminal, Civil, Regulatory, and Administrative Proceedings (Jan. 30, 2012), in Justice Manual § 27, <https://www.justice.gov/jm/organization-and-functions-manual-27-parallel-proceedings> (encouraging DOJ criminal and civil attorneys to 'coordinate together and with agency attorneys in a manner that adequately takes into account the government's criminal, civil, regulatory and administrative remedies').

⁶² See Letter from Rod J. Rosenstein, Deputy Att'y Gen., DOJ, to Heads of Dep't Components & U.S. Att'ys, DOJ (May 9, 2018), <https://www.justice.gov/opa/speech/file/1061186/download>.



The organisation should take a proactive role in pushing for a global resolution. Negotiating a global resolution can be challenging given the varied degree of coordination among agencies, and developing a solid understanding of the underlying policies and inter-agency dynamics is vital. The benefits of a coordinated settlement are enormous – greater legal certainty, a sense of closure and relief, and the avoidance of unnecessary duplication in penalties and disclosure.

Parallel US federal-state investigations

In recent years, US state regulators and attorneys general have become increasingly aggressive enforcers, especially in the areas of consumer protection, antitrust, and financial and healthcare fraud. Companies should recognise that the US federal government and state agencies often have overlapping investigative authority, and it is common for state investigators to piggyback onto federal investigations. These types of parallel proceedings may be particularly challenging as federal and state governments have different agendas and legal constraints.

Parallel US-foreign investigations

Parallel investigations involving US and foreign authorities are increasingly frequent, and US agencies have developed a collaborative relationship with foreign counterparts.⁶³ Such parallel proceedings have led to massive global penalties in recent years.⁶⁴ US-foreign coordination may come in different forms. Formally, it may involve mutual legal assistance treaties, memoranda of understanding or subject-specific agreements. Informally, coordination may involve ad hoc decisions to share investigative strategies and access to witnesses and information.

The Biden administration has expressed a strong commitment to cooperating with international authorities to fight global corruption. The US Strategy on Countering Corruption, released in December 2021, described the administration's planned approach to strengthening relationships with foreign

⁶³ See, eg, Kenneth A. Blanco, Acting Assistant Att'y Gen., DOJ, Remarks at the American Bar Association National Institute on White Collar Crime (Mar. 10, 2017), <https://www.justice.gov/opa/speech/acting-assistant-attorney-general-kenneth-blanco-speaks-american-bar-association-national>; U.S. Securities and Exchange Comm'n, SEC's Cooperative Arrangements with Foreign Regulators (Oct. 20, 2012), available at https://www.sec.gov/about/offices/oia/oia_coopfactsheet.htm.

⁶⁴ For example, in 2020, Airbus SE agreed to pay a record-breaking settlement of over US\$3.9 billion in combined penalties with US, French and UK regulators to resolve bribery charges. Press Release, U.S. Dep't of Justice, 'Airbus Agrees to Pay over \$3.9 Billion in Global Penalties to Resolve Foreign Bribery and ITAR Case' (Jan. 31, 2020), available at <https://www.justice.gov/opa/pr/airbus-agrees-pay-over-39-billion-global-penalties-resolve-foreign-bribery-and-itar-case>.



authorities and bolstering anti-corruption institutions.⁶⁵ As part of this initiative, the US government announced its intention to 'elevate and expand the scale of diplomatic engagement and foreign assistance' in combating corruption.⁶⁶ We expect this initiative will lead, in time, to greater coordination between US and foreign authorities on anti-corruption and anti-money laundering efforts, sanctions and related criminal investigations.

Coordinating cross-border resolutions raises some distinct issues, particularly surrounding data privacy. Global organisations responding to discovery requests should remain especially mindful of the ways in which they might get caught between the conflicting pressures of permissive US data privacy laws and non-US restrictive data protections. The US enforcement landscape is wholly distinct from other jurisdictions. A patchwork of state and federal laws comprises a complex framework, which is generally far less protective than foreign omnibus statutes, such as the European Union's General Data Protection Regulation.⁶⁷ A key difference is the extent of the government's reach into personal data. For example, the DOJ can, and regularly does, use search warrants and subpoenas to obtain text messages, emails and other communications from business and personal devices, such as data stored in messaging apps and in the cloud.

In addition, privileges that are well-established in the US, such as those shielding attorney-client communications and work-product, may look very different in other jurisdictions. For example, US privilege law generally protects notes of employee interviews conducted during an internal investigation, while English privilege law does not.⁶⁸ Because of such material differences in privilege laws, consulting with local counsel can be indispensable.

Companies should also consider the distinct legal regimes they are dealing with, as less than careful coordination can lead to sub-optimal outcomes. For example, a company may self-report to the DOJ to earn cooperation credit; should it also self-report to a foreign jurisdiction that provides no benefit for doing so? Cooperating in one jurisdiction may force the company into cooperating in other jurisdictions as well. In addition, different legal systems move at different speeds. An investigation may linger in one country's judicial system, even where another country's agencies are prepared to resolve the matter.

⁶⁵ The White House, United States Strategy on Countering Corruption (Dec. 2021), available at <https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf>.

⁶⁶ id.

⁶⁷ Parliament & Council Regulation 2016/679, 2016 O.J. (L 119) (EU).

⁶⁸ See generally *Re the RBS Rights Issue Litigation* [2016] EWHC (Ch) 3161.



Conclusion

There is no one-size-fits-all approach to advising a client facing a US government investigation. Much depends on the nature of the investigation, the scope and stage of the inquiry, the potential consequences of an enforcement action, and the potential risks of collateral consequences such as reputational damage and civil litigation. This article has sought to describe certain key considerations that should be given serious attention in all manner of white-collar and regulatory investigations. Ultimately, counsel must provide strategic advice and constantly assess, as an investigation progresses, the pros and cons of cooperating with the government versus challenging the government's assertions, undertaking a voluntary internal investigation versus merely responding to requests, and negotiating over the terms of a resolution versus seeking a declination and appealing to supervisors within the agency.

* *Debevoise associate Allison Miller and summer law clerk Natalie Tsang assisted in the preparation of this article.*



Arian M June

Debevoise & Plimpton LLP

Arian M June is a litigation partner based in the firm's Washington, DC, office and is a member of the white-collar and regulatory defence group. Recognised as one of 25 Influential Black Women in Business by *The Network Journal* (2020) and by *Benchmark Litigation* and *Chambers USA* for her expertise in white-collar criminal defence, Ms June's practice focuses on government and internal investigations, securities enforcement defence, whistleblower response, sensitive investigations and crisis management. She has represented financial institutions, publicly traded companies, investment advisers and senior executives in complex regulatory matters, including allegations of securities fraud, insider trading, accounting and corporate disclosure issues, violations of the Bank Secrecy Act, cyber-intrusions and sales practices violations, including matters involving foreign exchange products and the distribution of life insurance products.

**Winston M Paes**

Debevoise & Plimpton LLP

Winston M Paes is a litigation partner and a member of the white-collar and regulatory defence group. He is a seasoned trial lawyer and advises clients on complex matters concerning white-collar criminal defence, regulatory enforcement, internal investigations and civil litigation. Mr Paes is ranked as a leading lawyer in *Chambers USA* (2022), where clients have described him as 'fantastic' and 'a brilliant, strategic lawyer who has tremendous respect from his time in the government'.

**Douglas S Zolkind**

Debevoise & Plimpton LLP

Douglas S Zolkind is a litigation counsel based in the New York office and a member of the firm's white-collar and regulatory defence group. He has extensive trial experience and focuses his practice on white-collar criminal defence, government investigations and internal investigations. He defends corporate and individual clients in criminal and regulatory enforcement matters around the world.



Debevoise & Plimpton

Debevoise & Plimpton LLP is a premier law firm with market-leading practices, a global perspective and strong New York roots. Our clients look to us to bring a distinctively high degree of quality, intensity and creativity to resolve legal challenges effectively and cost efficiently.

Deep partner commitment, industry experience and a strategic approach enable us to bring clear commercial judgment to every matter. We draw on the strength of our culture and structure to deliver the best of our firm to every client through true collaboration.

Approximately 800 lawyers work in 10 offices across three continents, within integrated global practices, serving clients around the world. Our lawyers prioritise developing a deep understanding of the business of our clients. We then pursue each matter with both intensity and creativity to achieve optimal results.

801 Pennsylvania Avenue NW
Washington, DC 20004
United States
Tel: +1 202 383 8000

[Arian M June](#)
ajune@debevoise.com

[Winston M Paes](#)
wmpaes@debevoise.com

919 Third Avenue
New York, NY 10022
United States
Tel: +1 212 909 6000

[Douglas S Zolkind](#)
dzolkind@debevoise.com

www.debevoise.com
