



AMERICAS
INVESTIGATIONS REVIEW
2022

Americas Investigations Review 2022

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2021
For further information please contact insight@globalinvestigationsreview.com

Published in the United Kingdom
by Global Investigations Review
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL
© 2021 Law Business Research Ltd
www.globalinvestigationsreview.com

To subscribe please contact subscriptions@globalinvestigationsreview.com

No photocopying: copyright licences do not apply.

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 September 2021, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to Law Business Research, at the address above. Enquiries concerning editorial content should be directed to the Publisher – david.samuels@globalinvestigationsreview.com

© 2021 Law Business Research Limited

ISBN: 978-1-83862-592-4

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

Contents

OVERVIEWS

The Evolution and Current Approach to Corporate Cooperation in US Enforcement Investigations 3
Virginia Chavez Romano, Tami Stark, Nida Jafrani and Ben Elron
White & Case LLP

How US Authorities Obtain Foreign Evidence in Cross-Border Investigations 25
Jason Linder, Michael P Heffernan and William D Sinnott
Mayer Brown LLP

Moving Forward after an Investigation 45
Frances McLeod, Jenna Voss and Umair Nadeem
Forensic Risk Alliance

COUNTRY-SPECIFIC: BRAZIL AND UNITED STATES

Brazil: Internal Investigations and Cooperation with Enforcement Authorities 65
Isabel Franco and Glaucia Ferreira
Azevedo Sette Advogados

Anti-corruption in Brazil: Current Status and the Next Steps 86
Carlos Ayres and Carolina Furquim
Maeda, Ayres & Sarubbi Advogados

Key Considerations in US Government Investigations..... 99

Arian M June, Winston M Paes and Douglas S Zolkind

Debevoise & Plimpton LLP

**United States: Use of Data to Detect Crimes and Evaluate
Corporate Compliance 123**

Palmina M Fava, Jessica S Heim, G Zachary Terwilliger and Meghan Natenson

Vinson & Elkins LLP

Preface

Welcome to the *Americas Investigations Review 2022*, a Global Investigations Review (GIR) special report. GIR strives to be the online home for all those who investigate, and resolve, suspected corporate wrongdoing for a living, telling them all they need to know about everything that matters – wherever it may take place.

Throughout the year, GIR’s team of journalists delivers daily news, surveys and features; organises the liveliest events (GIR Live) – covid-19 permitting; and provides our readers with innovative tools and know-how products.

In addition, assisted by external contributors, GIR curates a range of comprehensive regional reviews – online and in print – that go deeper into developments than the exigencies of journalism allow.

The *Americas Investigations Review*, which you are reading, is one of those reviews. It contains insight and thought leadership from 21 pre-eminent practitioners from the region. All contributors are vetted for their standing and knowledge before being invited to take part.

Across seven articles, and 142 pages, they capture and interpret the shifts of the past year in the region, supported with plenty of footnotes and statistics.

As so often with these reviews, a close read yields many nuggets. For this reader, they include that:

- foreign bribery is now a ‘core’ national security interest in the United States;
- ‘hold notices’ in Brazil routinely achieve the opposite effect;
- the OECD is so concerned about corruption in Brazil that it has established a special working group to monitor it. In the meantime, data from within Brazil is quite encouraging; and
- the US Securities and Exchange Commission and Department of Justice are at serious odds about the meaning of ‘cooperation’.

And much, much more.

Every article is splendid. I thoroughly commend all the authors.

If you have any suggestions for future editions of this review, or want to take part in it, we would love to hear from you.

Please write to insight@globalinvestigationsreview.com.

David Samuels

Publisher, Global Investigations Review

September 2021

Part 2

Country-specific: Brazil and United States

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 (e.g., Securities and Exchange Commission, Commodity Futures Trading Commission or 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 in order to assess how best to respond
- Considering an internal investigation if not already undertaken by the company
- 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

Guiding a client through a US government investigation requires advising on a myriad of complex strategic decisions at many points along the way. In this article, we discuss certain critical considerations that frequently arise, whether in criminal or civil investigations led by the Department of Justice (DOJ) or in regulatory investigations led by agencies such as the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC) and the Office of Foreign Assets Control (OFAC).

First, we examine key considerations that must be confronted in the early stages of a government investigation. For instance, counsel must evaluate whether to launch an internal investigation; whether to self-report on potential violations of which the government is unaware; how to ensure that potential evidence and other data is preserved; and how to interact with, and be responsive to, government investigators without risking a waiver of the attorney–client privilege. Next, we discuss the process of cooperating with a government investigation and explore the benefits and risks of doing so. Finally, we discuss strategies for navigating parallel investigations, in which multiple federal, state or foreign agencies are examining the same conduct.

Key considerations at the outset of a US government investigation

In the early stages of a US government investigation, a company will often face daunting decisions that can have an outsize 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, DOJ increasingly has used the False Claims Act (FCA)¹ to prosecute a broad range of false monetary claims submitted to the government.

The SEC and CFTC also have effective whistleblower programmes. Under the Sarbanes-Oxley Act of 2002² and Dodd-Frank Act of 2010,³ individuals may report voluntarily to the SEC ‘original information’ about potential violations of US securities laws. In fiscal year 2020, the SEC received a record-breaking number of whistleblower tips – more than 6,900 – including from individuals in 78 foreign countries.⁴ The CFTC operates a virtually identical whistleblower programme under Section 23 of the Commodity Exchange Act,⁵ which allows individuals to report potential violations of US commodities laws to the CFTC. More recently, the Treasury Department enhanced its whistleblower award programme to encourage reporting on financial institutions’ violations of the Bank Secrecy Act, by passing the Anti-Money Laundering Act of 2020,⁶ which took effect on 1 January 2021.

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

1 31 U.S.C. § 3729 et seq.

2 15 U.S.C. § 7201 et seq.

3 12 U.S.C. § 5301 et seq.

4 U.S. Securities and Exchange Commission [SEC], ‘2020 Annual Report to Congress – Whistleblower Program’ (16 November 2020), available at https://www.sec.gov/files/2020%20Annual%20Report_0.pdf.

5 7 U.S.C. § 1 et seq.

6 31 U.S.C. § 5301 et seq.

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.

If a government investigation has been launched based on a whistleblower report, the target company is already at a significant disadvantage. The government is probably 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 these 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.

Subpoena or other formal request

A company often learns of a government investigation for the first time when it receives a formal written request demanding the disclosure of documents and information. In criminal investigations, DOJ typically issues these demands in the form of a grand jury subpoena. A corporation has no Fifth Amendment privilege against self-incrimination⁷ and, therefore, cannot refuse to produce records, even if it is the target of the investigation.

Many federal agencies in the United States are also statutorily authorised to issue administrative subpoenas compelling document production and testimony.⁸ 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 by DOJ's Antitrust and Civil Divisions.

On receipt of a subpoena or CID, a reasonable first step is often to begin a dialogue with the government agency. Although 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

⁷ See *Curcio v. United States*, 354 U.S. 118, 122 (1957).

⁸ See, e.g., 15 U.S.C. § 78dd-2(d)(2) (Department of Justice [DOJ]); 15 U.S.C. § 77s(c) (Securities and Exchange Commission [SEC]); 7 U.S.C. § 9(5)-(6) (Commodities Futures Trading Commission [CFTC]).

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 of 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 in which 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. 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. These 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.

Self-report

Some investigations begin when a company voluntarily discloses potential violations to a US government agency. Many companies self-report in the hope 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, DOJ updated the Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy to require voluntary self-disclosure as a necessary prerequisite to full cooperation credit.⁹ In early 2018, DOJ officials announced that the principles delineated in the Corporate Enforcement Policy would guide non-FCPA criminal corporate investigations as well.¹⁰ Likewise, the SEC has emphasised the importance of self-reporting in obtaining a successful resolution. In 2015, the then director of the SEC's Division of Enforcement made clear that 'there are significant benefits available to companies who self-report violations' and that companies must self-report to be eligible for a deferred prosecution agreement or non-prosecution agreement in FCPA cases.¹¹

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 when the government (1) is not already aware of the misconduct, and (2) is unlikely to discover the misconduct by other means. In these 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 opening the way 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 if the misconduct turns out to be fairly confined and easily remediated by the company.

9 See Justice Manual § 9-47.120 (Foreign Corrupt Practice Act [FCPA] Corporate Enforcement Policy).

10 Remarks by John Cronan, Acting Ass't Att'y Gen., Crim. Div., DOJ, 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 (1 March 2018), details of which are available at <https://www.law360.com/articles/1017798/doj-expands-leniency-beyond-fcpa-lets-barclays-off>.

11 Andrew Ceresney, Dir., SEC Div. of Enf't, American Conference Institute's 32nd FCPA Conference Keynote Address (17 November 2015), available at <https://www.sec.gov/news/speech/ceresney-fcpa-keynote-11-17-15.html>.

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, OFAC declines self-disclosure credit if 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'.¹² 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 that self-reporting will 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 may 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 on to meet the regulator's requests; and

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

- 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.

Data preservation

At the outset of a US government investigation, a company must promptly take reasonable steps to preserve evidence and other data. A failure to do so may violate legal requirements and additionally could lead to adverse inferences regarding the company's culpability.¹³

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, so it may also be useful to keep this in mind.¹⁴

During the past year, 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, employees have conducted tremendous amounts of work on personal devices. These devices exist outside corporate systems and are typically not protected with enterprise-grade security mechanisms. This shift may lead to increased government scrutiny that this 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). Although 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,

13 See, e.g., 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).

14 See, e.g., DOJ, 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) (2018), available at <https://www.justice.gov/jm/justice-manual> [Justice Manual]; SEC Enforcement Manual §§ 3.2.9.4, 3.2.9.6 to 3.2.9.9; CFTC Enforcement Manual §§ 5.10, 9.1.

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.

In anticipating these issues, firms should consider how to locate and collect this data. Enhanced security and employee training may help to address immediate concerns, while reassessing the location of servers and the manner in which data is stored may help to 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 the 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 do 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.

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 a 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.¹⁵ The work-product privilege protects materials prepared by, or at the direction of, lawyers in anticipation of litigation.¹⁶ In this section, we discuss a number of questions that should be uppermost in the mind when embarking on responding to a government investigation or conducting an internal investigation.

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

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

Who will lead the inquiry?

At the outset of an investigation, a company 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.¹⁷ Privilege shields communications and work-product with legal purpose and, therefore, can be compromised if an investigation is conducted by in-house counsel that performs both legal and non-legal functions. If the need to preserve privilege is a strong consideration, a company is 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 when underlying allegations concern a company's board or senior management. Even in routine matters where outside counsel are not regularly engaged, a company 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 greatest possible extent.

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. A company 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 to develop the necessary record to support a privilege determination at a later date.

¹⁷ See *In re Kellogg Brown & Root, Inc.*, 756 F.3d at 757–59 (upholding privilege where 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 internal investigation led by compliance officer, who lacked purpose of providing legal advice).

The underlying facts of an investigation are generally not protected from disclosure.¹⁸ 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. 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 affect the investigation in the long run.

When should privilege be waived?

Despite government policies regarding privilege protections,¹⁹ 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.²⁰ Accordingly, disclosure of privileged documents and materials to government sources runs the risk that those materials will be discoverable by 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. DOJ, for example, explicitly states privilege waivers are not a prerequisite for cooperation, but disclosure of all relevant facts is.²¹ 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

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

19 See, e.g., Justice Manual § 9-28.710 (Attorney-Client and Work Product Protections).

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

21 See Justice Manual § 9-28.720 (Cooperation: Disclosing the Relevant Facts).

a later assertion by the company that the documents are still privileged. Nearly every circuit that has addressed attempts to selectively disclose privileged material has held that sharing information with the government amounts to a waiver of that information as to third parties as well.²²

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 forego cooperation when:

- it is factually unclear that 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; or
- 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 agency. There may also be differing guidelines based on the type of violation (for example, FCPA or FCA). This section explores the basic cooperation framework for DOJ, SEC, CFTC and OFAC.

²² 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*).

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’.²³ Cooperation credit is predicated on the company’s identification of all individuals ‘substantially involved in or responsible for the misconduct at issue’.²⁴ The company must provide the government with complete factual information about these identified individuals.²⁵ However, the policy also acknowledges the practical difficulties of meeting this standard; accordingly, organisations may still earn cooperation credit when ‘despite its best efforts to conduct a thorough investigation, a company genuinely cannot get access to certain evidence’.²⁶

In the civil context, cooperation credit is awarded on a sliding scale, at the discretion of the DOJ attorneys handling the matter.²⁷ 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’.²⁸ However, even if it does not qualify for maximum credit, an organisation may still receive some credit for providing ‘meaningful assistance to the government’s investigation’.²⁹ 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.³⁰

These policies, announced in 2018,³¹ softened the prior guidelines for cooperation credit embodied in a 2015 policy document called the Yates Memorandum, which required even more stringent disclosures regarding individuals’ involvement in

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

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

25 *id.*

26 *id.*

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

28 *id.*

29 *id.*

30 *id.*

31 See Rod J Rosenstein, Deputy Att’y Gen., DOJ, Remarks at American Conference Institute’s 35th International Conference on the Foreign Corrupt Practices Act (29 November 2018), available at <https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0>.

the misconduct.³² Industry professionals have speculated that DOJ, under the Biden administration, may revive the Yates Memorandum's emphasis on all-encompassing individual accountability.

As a practical matter, DOJ has shown it is willing to grant full cooperation credit when an organisation takes serious proactive measures. For example, in April 2020, Pentax Medical, a medical supply company, entered into a deferred prosecution agreement for misbranding medical devices. Pentax received full cooperation credit for 'conducting a thorough internal investigation, making regular factual presentations to [DOJ], proactively identifying issues and facts that would likely be of interest to [DOJ], advising [DOJ] about facts and issues that were not the focus of the subpoena, and collecting, analyzing, and organizing voluminous evidence and information for [DOJ]'.³³

Securities and Exchange Commission

In 2001, the SEC issued a Report of Investigation and Commission Statement, commonly known as the Seaboard Report, laying out the framework for earning cooperation credit.³⁴ 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 with law enforcement authorities.³⁵ From there, the Seaboard Report lays out a series of 13 considerations the SEC will weigh 'in determining whether, and how much, to credit self-policing, self-reporting, remediation and cooperation – from the extraordinary

32 See Memorandum from DOJ Deputy Att'y Gen. Sally Yates on Individual Accountability for Corporate Wrongdoing (9 September 2015), <https://www.justice.gov/archives/dag/file/769036/download>.

33 Pentax Medical Company Deferred Prosecution Agreement (7 April 2020), available at <https://www.pentaxmedical.com/pentax/download/fstore/uploadFiles/Pdfs/Downloads/20200407%20DPA%20PENTAX%20Medical%20Final.pdf>.

34 See SEC, 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) [Seaboard Report], available at <https://www.sec.gov/litigation/investreport/34-44969.htm>.

35 See Spotlight on Enforcement Cooperation Program, SEC (20 September 2016), <https://www.sec.gov/spotlight/enforcement-cooperation-initiative.shtml>.

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'.³⁶

The SEC accords significant benefits to companies that fully cooperate with the Seaboard Report framework. For instance, in February 2021, the SEC settled charges against a gas exploration company (Gulfport Energy Corporation) for failure to disclose certain compensation perks provided to its chief executive officer. The SEC declined to impose a civil penalty in light of the company's 'significant cooperation' and 'remedial efforts', including 'replacing key personnel, developing an internal audit function, enhancing existing policies and procedures, and instituting new review and tracking processes'.³⁷

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 its Enforcement Manual.³⁸ CFTC guidance emphasises that 'ordinary cooperation' is insufficient for credit; rather, a company's conduct during an investigation should be 'sincere, robustly cooperative, and indicative of a willingness to accept responsibility for the misconduct'.³⁹ 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).⁴⁰ The CFTC will also take into account any 'uncooperative conduct', such as failing to adequately respond to requests or to preserve relevant information, or minimising the misconduct at issue.⁴¹

36 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 (Seaboard Report), available at <https://www.sec.gov/litigation/investreport/34-44969.htm>.

37 Press Release, SEC, 'SEC Charges Gas Exploration and Production Company and Former CEO with Failing to Disclose Executive Perks' (24 February 2021), <https://www.sec.gov/news/press-release/2021-33>.

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

39 Div. of Enf't, CFTC, Enforcement Advisory: Cooperation Factors in Enforcement Division Sanction Recommendations for Companies (2017), available at <https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfadvisorycompanies011917.pdf>.

40 See *id.*

41 *id.* at 6-7.

In December 2020, the CFTC settled charges against Vitol Inc, an energy and commodities trading firm. The CFTC recognised Vitol's 'substantial cooperation' as a factor supporting a reduced penalty. Specifically, Vitol had 'voluntarily provided material information . . . obtained by Vitol through an internal investigation', 'proactively identified information of interest', 'produced expeditious and prioritized responses . . . on a voluntary basis', and 'assisted [the CFTC] in analyzing trading data'.⁴²

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.⁴³ Specifically, OFAC considers the 'nature and extent' of an entity's cooperation by assessing, among other things, (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.⁴⁴

In April 2021, OFAC reached a settlement with SAP SE, a German software company, to resolve violations relating to the export of software from the United States to Iran. OFAC considered SAP's 'substantial[]' cooperation to be a mitigating factor, including SAP's efforts to 'arrang[e] interviews with SAP employees'.⁴⁵

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 parallel investigations, counsel must keep a number of additional considerations in mind.

42 *In the Matter of: Vitol Inc.*, CFTC Docket No. 21-01, Order Instituting Proceedings Pursuant to Section 6(c) and (d) of the Commodity Exchange Act, Making Findings, and Imposing Remedial Sanctions, (3 December 2020).

43 See 31 CFR pt. 501, app. A.

44 *id.* §§ (III)(G)(1)-(6).

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

Parallel investigations by multiple US federal agencies

For several decades, the US federal government has made efforts to increase inter-agency cooperation.⁴⁶ In 2018, 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’.⁴⁷

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.

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.

46 See Memorandum from DOJ Att’y Gen. Janet Reno on Coordination of Parallel Criminal, Civil, and Administrative Proceedings (28 July 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 (30 January 2012), in Justice Manual § 27, available at <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’).

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

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.⁴⁸ Parallel proceedings have led to massive global penalties in recent years.⁴⁹ 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.

In addition to the general concerns accompanying parallel 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

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

49 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, DOJ, 'Airbus Agrees to Pay over \$3.9 Billion in Global Penalties to Resolve Foreign Bribery and ITAR Case' (31 January 2020), available at <https://www.justice.gov/opa/pr/airbus-agrees-pay-over-39-billion-global-penalties-resolve-foreign-bribery-and-itar-case>.

Data Protection Regulation.⁵⁰ A key difference is the extent of the government's reach into personal data. For example, 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 United States, 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, whereas English privilege law does not.⁵¹ 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 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 if another country's agencies are prepared to resolve the matter.

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 the terms of a resolution versus seeking a declination and appealing to supervisors within the agency.

50 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 119, 4.5.2016, pp. 1–88 (European Union).

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



ARIAN M JUNE

Debevoise & Plimpton LLP

Arian M June is a litigation partner in the Washington, DC, office of Debevoise & Plimpton LLP. Recognised as one of 25 Influential Black Women in Business by *The Network Journal* (2020) and by *Benchmark Litigation's* 40 and Under Hotlist (2020), Ms June's practice focuses on government and internal investigations, securities enforcement defence, whistleblower response, sensitive investigations, crisis management and white-collar criminal defence.

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.

Ms June advises clients on various facets of the Dodd-Frank Act, with particular emphasis on designing corporate policies and procedures to comply with the Dodd-Frank Whistleblower regulations, investigating corporate whistleblower reports and mitigating whistleblower-related risks. In addition to her white-collar practice, Ms June also advises boards of corporations, educational institutions and other organisations in sensitive investigations, including board-directed independent inquiries of allegations involving sexual misconduct, racial intolerance and related matters.

**WINSTON M PAES**

Debevoise & Plimpton LLP

Winston M Paes is a litigation partner in the New York office of Debevoise & Plimpton LLP. He is a seasoned trial lawyer and advises clients on white-collar criminal defence, regulatory enforcement, internal investigations and complex civil litigation. Mr Paes is ranked as a leading lawyer in *Chambers USA* (2021), where clients describe him as ‘fantastic’ and ‘a brilliant, strategic lawyer who has tremendous respect from his time in the government’. He is also recognised by *The Legal 500: US* (2021).

Prior to joining the firm, Mr Paes served for nine years as an Assistant US Attorney in the Eastern District of New York, the final two years of which he spent as Chief of the Business and Securities Fraud Section. As Section Chief, Mr Paes supervised a team of 20 experienced federal prosecutors focused on white-collar matters. Under his leadership, the EDNY significantly expanded its white-collar practice and prosecuted a number of the Department of Justice’s most high-profile matters. Before his appointment as a Section Chief, Mr Paes also served as the Deputy Chief of the Business and Securities Fraud Section and Supervisor of its Medicare Fraud Task Force.



DOUGLAS S ZOLKIND

Debevoise & Plimpton LLP

Douglas S Zolkind is a litigation counsel in the New York office of Debevoise & Plimpton LLP. 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.

Prior to joining Debevoise, Mr Zolkind was an Assistant United States Attorney in the US Attorney's Office for the Southern District of New York (SDNY), serving as a senior member of the Criminal Division's Public Corruption Unit. Prior to joining SDNY, Mr Zolkind was a litigation associate at another international law firm.

At SDNY, Mr Zolkind led investigations, prosecutions and trials in cases involving foreign bribery and the Foreign Corrupt Practices Act (FCPA), wire fraud, money laundering, business and political corruption, bank fraud, securities offences and cybercrime. He handled many high-profile white-collar matters, including an FCPA trial against a Macao-based real estate tycoon involving corruption at the highest levels of the United Nations, and an FCPA trial against a former cabinet-level Hong Kong official involving efforts by a Chinese energy company to bribe top officials in Chad and Uganda.

Debevoise & Plimpton

Debevoise & Plimpton LLP is a premier law firm with market-leading practices, a global perspective and strong New York roots. Approximately 800 lawyers work in 10 offices across three continents, within integrated global practices, serving clients around the world.

The firm's white collar and regulatory defence group has excelled in some of the most high-profile, difficult corporate crises. The group's depth of experience and global reach means it works strategically and effectively with international clients to anticipate and respond to risks, swiftly identifying the root of any problem.

The team's experience includes defending against criminal prosecutions and civil enforcement actions, securities-related litigation, conducting internal investigations, negotiating complex global settlements and facilitating cooperation with government regulators. The team also routinely counsels clients regarding preventive measures, compliance programmes and the collateral consequences of criminal proceedings.

Respected by enforcement agencies, the group's lawyers are renowned for their investigative skill, seasoned judgement and consistently clear and persuasive presentation of the facts. This makes the team a powerful advocate for clients, and leads to considerable success in matters involving investigations by the Securities and Exchange Commission, US Department of Justice, New York Attorney General, UK Serious Fraud Office, and other authorities around the world.

The group combines this unique understanding of the enforcement landscape with a deep appreciation for client business issues. As leading trial lawyers, but skilled negotiators, a successful outcome for the client is frequently achieved before a trial begins, and government cases are sometimes dropped altogether.

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

Arian M June
ajune@debevoise.com

Winston M Paes
wmpaes@debevoise.com

Douglas S Zolkind
dzolkind@debevoise.com

The Americas Investigations Review 2022 contains insight and thought leadership from 21 pre-eminent practitioners from the region. Across 142 pages, it provides an invaluable retrospective on what's been happening, and where, in the corporate criminal space.

All articles come complete with footnotes with, where appropriate, relevant statistics.

This edition has a particular focus on Brazil and the United States and includes, among other things, overviews on the expectations of the US Department of Justice regarding corporate data systems and how to learn the lessons from an investigation.

Visit globalinvestigationsreview.com
Follow @GIRalerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-592-4