CLIFFORD

CHANCE

# RESPONDING TO A U.S. GOVERNMENT INVESTIGATION IN THE DERIVATIVES, COMMODITIES, AND SECURITIES MARKETS

Provided in Conjunction with a Presentation to the
FUTURES INDUSTRY ASSOCIATION
September 30, 2021

## CONTENTS

# RESPONDING TO A U.S. GOVERNMENT INVESTIGATION IN THE DERIVATIVES, COMMODITIES AND SECURITIES MARKETS

## A. Preface

*The high stakes involved in U.S. investigations are clearly demonstrated by the very large civil and criminal penalties that authorities have imposed regularly in recent years for corporate misconduct. Although the nature and extent of any misconduct being investigated is a critical component, the penalties imposed are to an important degree also influenced by the response to an investigation. Long after any questioned conduct has ceased, been identified or is remediated, the response to a government investigation can have profound positive or negative consequences in its resolution. This guide describes the key stages of the investigative and resolution process and discusses various legal and practical factors to be considered in responding at each stage.*

*Questions concerning the subject matter or topics addressed in this guide may be directed to any of the authors listed in the contacts included at the end of this publication or to your local Clifford Chance resource.*

## B. Introduction

This guide is intended to provide corporate officers, directors, audit committees, and in-house counsel ("stakeholders") with an overview of the key factors to consider before, during, and in resolving an investigation involving one or more U.S. authorities. It provides detail concerning the significant benefits that can be attained by handling inquiries appropriately and in a timely manner, and the significant risks associated with failing to understand U.S. authorities' expectations or make appropriate compliance efforts. A proper investigative plan and response guided by experienced counsel can maximize efficiencies in responding to U.S. authorities, and can optimize outcomes at the resolution phase.

Unlike the prospect of responding to a civil lawsuit, investigations tend to be iterative processes. When the prospect of an investigation involving U.S. authorities presents itself, stakeholders should set forth an efficient plan for identifying and comprehensively understanding pertinent issues and responding effectively. It is important to begin an investigation with potential endpoints in mind. Generally speaking, the potential endpoints should be determined based on a variety of facts and circumstances, including the existence of any potentially meritorious defenses, the potential need to maintain productive relationships with the authorities, and the anticipated time, expense and consequences involved in investigating, in settling with the authorities and in litigating. Meanwhile, however, any investigative plan should be flexible enough to incorporate and respond to suggested modifications as facts develop, including from government regulators. At the outset of an investigation of alleged U.S.-related misconduct, a company should comprehensively consider, among other things: potential and desired outcomes, expectations of relevant agencies, and the structuring of investigative processes to minimize risky and constraining decisions, such as being untruthful with the investigating agency (or agencies).

Recent high-profile investigations have seen collaboration among U.S. enforcement agencies, including the U.S. Department of Justice ("DOJ"), the U.S. Securities and Exchange Commission ("SEC"), the U.S. Commodity Futures Trading Commission ("CFTC"), the Federal Energy Regulatory Commission, as well as the New York State Department of Financial Services and states' attorneys general and district attorneys' offices. Criminal prosecutors often coordinate closely with civil regulators in parallel proceedings, rather than waiting for referrals. This collaboration also extends across borders and among a multitude of non-U.S. regulators. Fines and penalties levied against corporate defendants have reached astronomical highs, with unclear mathematical correlation to specified violations or actual harm.

The first steps that a company should take to maximize its chances of achieving a desirable investigative outcome should occur long before the first sign of trouble. In addition to assessing the conduct subject to investigation and a respondent's remedial actions (including accountability for culpable individuals), authorities will assess whether a company's systems and controls were sufficient to detect the misconduct. Thus, companies should proactively and continuously evaluate their business supervisory, compliance and legal infrastructure, as well as their crisis management plans, to ensure that they are prepared to move quickly and appropriately at the first sign of trouble.

Stakeholders and counsel responding to government inquiries or facing the prospect of a likely government investigation can reap benefits of early and comprehensive responses and cooperation where appropriate and without sacrificing the independence of any internal investigation. By contrast, failure to react promptly and appropriately to suspected misconduct can be costly. Numerous resolutions demonstrate the significant penalties attributable to a respondent's failure to take an investigation or suspected misconduct seriously. And while prompt submissions to authorities are advisable, conveying information to authorities that is inaccurate or incomplete will itself lead to negative consequences. An appropriate investigative strategy and plan guided by experienced counsel can mitigate these risks.

## C. Stages of an Investigation

Broadly, an investigation can be considered to have three overarching phases: (1) commencement, (2) information gathering, and (3) resolution.

During the commencement phase of an investigation, corporations should strive to understand the potential sources and triggers of an investigation, including internal reporting, external requests and market awareness. Additionally, at the onset of an investigation, corporations should identify which government agencies might ultimately be involved and consider the respective agencies' expectations.

Next, during the information gathering phase, the target of an investigation should determine an optimal outcome and structure an investigation plan with that outcome in mind. Special consideration should be given to identifying potential sources of information, the scope of the inquiry, and issues concerning confidentiality and privileged communication.

Finally, in the resolution phase, corporations should carefully manage the outflow of information and ensure that all actions taken are directed at the desired outcome. The resolution strategy should be tailored to the specific agency or agencies involved and also reflect cognizance of any potential collateral consequences.

# D. Legal Framework: Reach of U.S. Law and Process

## 1. Jurisdiction

### (a) Generally

At the commencement of an investigation, a company should consider what laws may have been violated and the location of the misconduct in order to determine which U.S. authorities, if any, may have jurisdiction to prosecute the matter. In order to hear a claim in either the civil or criminal context, a court must first assert jurisdiction over the person and the conduct. Jurisdiction refers to a court's ability to exert its power and legal authority over the parties and matter at hand. Where conduct occurs outside the U.S., courts must separately find that the relevant U.S. law or laws to be applied are able to reach beyond U.S. territory. As a general matter, U.S. regulators and prosecutors take an expansive view of their territorial reach and are asserting increasingly aggressive jurisdictional claims in U.S. courts.

### (b) Personal Jurisdiction

Personal jurisdiction refers to the authority of a court to exercise its power over a particular person or entity. There are two types of personal jurisdiction—general and specific—but only one must be present.

General jurisdiction grants courts the ability to hear any and all claims against a party, and specific jurisdiction grants courts the power to hear claims relating to specific conduct of the parties. Courts exercising personal jurisdiction must do so in a manner consistent with federal due process.[1] Courts have expounded upon this rather nebulous standard and explained that, to prosecute a foreign individual or entity, there must be "a sufficient nexus between the defendant and the United States, so that such application would not be arbitrary or fundamentally unfair."[2]

#### (1) General Jurisdiction

General jurisdiction exists where a party has "continuous and systematic" contacts with the forum, regardless of whether those contacts relate to the lawsuit. The central inquiry in determining whether a court has general jurisdiction is not the conduct of the parties involved, but rather the geographical connection that an entity maintains with the forum. In 2014, the U.S. Supreme Court clarified that courts may assert general jurisdiction over a nonresident corporation only when its affiliations with the forum are "so continuous and systemic as to render [it] essentially at home in the forum State."[3] Under this formulation, absent "exceptional" circumstances, a corporation is only subject to general jurisdiction in the district or state where it is incorporated or where it has its principal place of business.[4]

Notably, courts obtain personal jurisdiction over individuals when they are physically present in the forum, even if only transiently.

1. *See* U.S. CONST. amend. V.
2. *United States v. Yousef*, 327 F.3d 56, 58 (2d Cir. 2003).
3. *Daimler AG v. Bauman*, 134 S. Ct. 746, 754 (2014).
4. *Id.* at 761 n.19; *see also BNSF Ry. v. Tyrrell*, 137 S. Ct. 1549, 1558 (2017); *Gucci Am., Inc.* v. *Li*, 768 F.3d 122 (2d Cir. 2014); *In re SSA Bonds Antitrust Litig.*, 420 F. Supp. 3d 219 (S.D.N.Y. 2019).

**(2) Specific Jurisdiction**

Specific jurisdiction requires that a party purposefully directs its activities toward the forum and that the lawsuit itself relates to that party's contacts with the forum. Typically, specific jurisdiction involves a fact-intensive inquiry into "Who did what? And where?"

Example Case: *In re SSA Bonds Antitrust Litig.*, 420 F. Supp. 3d 219 (S.D.N.Y. 2019)

In *In re SSA Bonds Antitrust Litig.*, the Southern District of New York held that the defendant foreign dealers were not subject to general jurisdiction in the U.S. because none of the defendants were domiciled or had a principal place of business in the U.S. As for specific jurisdiction, the plaintiffs did not sufficiently allege purposeful availment (i.e. that the defendants took intentional action to enjoy the privilege of doing business in the state), and the court found no factual support for allegations that the defendants' actions were directed at New York specifically (the "effects test"). Accordingly, the court did not find specific jurisdiction and concluded that exercising personal jurisdiction over any defendant in the matter would violate due process.[5]

## 2. Extraterritoriality Principles[6]

In addition to limits imposed by the requirement to establish jurisdiction, the Constitutional "presumption against extraterritoriality" imposes significant limits on the U.S. government's ability to prosecute individuals and entities for conduct outside of the United States.

The U.S. Supreme Court has consistently reaffirmed this presumption against extraterritoriality by holding that, unless a statute clearly indicates Congress intended an extraterritorial application, it has none. The Supreme Court's treatment of the Exchange Act provides a key example of an application of the presumption against extraterritoriality.

There are, however, certain circumstances where U.S. law unambiguously anticipates extraterritorial application. The CEA includes language stating that its swaps provisions will apply to conduct outside the U.S., provided that conduct (1) [has] a direct and significant connection with activities in, or effect on, commerce of the United States; or (2) contravene[s] such rules or regulations as the Commission may prescribe . . . to prevent the evasion of any provision of [the CEA]."[7] Other statutes that do not expressly have an extraterritorial reach may nevertheless reach conduct with only a very thin connection to the U.S. For example, the broad reach of the U.S. wire fraud statute criminalizes any scheme to defraud that affects "interstate or foreign commerce" and may be prosecuted in the United States where an electronic communication, such as a telephone call or email, in furtherance of the alleged scheme travels through the United States.[8] In enforcing crimes that invoke this statute, the DOJ has the ability to bring criminal

5. *In re SSA Bonds Antitrust Litig.*, 420 F. Supp. 3d at 235.
6. For further discussion of the limits on the U.S. government's ability to prosecute individuals and entities for conduct outside of the U.S., see the discussion in Sections II(B)(2) and III(c) of the Guide to United States, United Kingdom, and Hong Kong Derivatives and Commodities Market Enforcement Regimes, from which this resource is drawn. David Yeres, et al., GUIDE TO UNITED STATES, UNITED KINGDOM, HONG KONG DERIVATIVES AND COMMODITIES MARKET ENFORCEMENT REGIMES (Clifford Chance 2020) (hereinafter "Commodities Enforcement Guide").
7. 7 U.S.C. § 2(i).
8. 18 U.S.C. § 1343.

charges for violations of U.S. law despite the fact that the conduct at issue occurred almost entirely overseas.

Moreover, recent cases covering a wide range of sectors demonstrate that foreign nationals, even when operating outside the U.S., may fall within the ambit of U.S. criminal prosecution.

### 3. Concurrent Jurisdiction and Associated Conflicts

There are several areas in which the CFTC and the SEC might assert overlapping jurisdiction. The CEA gives the CFTC jurisdiction over swaps, "commodities" and "commodity" futures. "Commodity" is very broadly defined by the CEA to include a specified list of agricultural products, as well as "goods and articles" and "all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt in . . . ."[9] While the exact limits of this authority have not been settled, CFTC enforcement has generally been coextensive with the wide range of products that currently have futures contracts. These include (i) traditional agricultural commodities (such as corn, sugar and wheat), (ii) industrial commodities (including energy products like oil and natural gas, precious metals like gold and silver, and industrial metals like copper and aluminum), and (iii) financial commodities (such as currencies, interest rates and certain cryptocurrencies). By contrast, the securities laws give the SEC jurisdiction over "securities," which are defined by law to include a range of instruments, such as shares of stock, warrants, options, bonds and notes, and investment contracts.[10]

These broadly defined categories create the potential for overlap in various areas. For example, reports in the first quarter of 2021 indicated that the CFTC has been investigating potential manipulation of silver prices, including potential manipulation that may have occurred through the purchase of ETF shares.[11] Similarly, the CFTC has likely been investigating potential manipulation in connection with the negative oil futures prices that were observed on April 20, 2020, and any such investigation may analyze potentially manipulative trading of crude oil ETFs.[12]

The CFTC and SEC have separate—but potentially overlapping—jurisdiction in this area. Any trading of futures or swaps, as well as wholesale interstate trading of physical commodities, are subject to the anti-manipulation provisions of the CEA and would be subject to the CFTC's civil enforcement jurisdiction. On the other hand, ETF share offerings which are registered under the U.S. securities laws are subject to the SEC's direct regulatory oversight and civil enforcement authority.[13] The CFTC's enforcement jurisdiction over trading of ETF shares would be less direct than that of the SEC, though the CFTC could seek to exercise enforcement jurisdiction over potentially manipulative trading of ETFs based on the price impact that such trading had on the prices of underlying commodities. It remains to be seen whether the CFTC would aggressively seek to assert jurisdiction over potentially manipulative trading in commodities ETFs, and if so, how the SEC would react.

---

9. 7 U.S.C. § 1a(9).
10. 15 U.S.C.§ 77b(a)(1).
11. Dave Michaels, *GameStop Mania Is Focus of Federal Probes Into Possible Manipulation,* The WALL STREET JOURNAL (Feb. 11, 2021), **https://www.wsj.com/articles/gamestop-mania-is-focus-of-federal-probes-into-possible-manipulation-11613066950**.
12. Ryan Dezember, *U.S. Oil Costs Less Than Zero After a Sharp Monday Selloff,* THE WALL STREET JOURNAL (Apr. 21, 2020), **https://www.wsj.com/articles/why-oil-is-11-a-barrel-now-but-three-times-that-in-autumn-11587392745.**
13. *See, e.g.*, 15 U.S.C. §§ 78i, 78j, 78l.

With respect to digital-assets businesses, the CFTC's actions have largely focused on retail fraudsters, but it has brought a handful of actions against more established digital-assets businesses as well. The SEC has also been active in this area, but crucially, neither the CFTC nor SEC has provided concrete guidance on which digital assets constitute commodities and which constitute securities. And in 2018, the Director of the SEC's Corporate Finance Division gave a speech in which he suggested that many digital assets start out as securities, but may ultimately achieve a sufficient level of decentralizations that they no longer qualify as such.[14] While the CFTC and SEC have made public statements highlighting cooperation between the two agencies in the digital-assets realm,[15] it remains to be seen whether these regulators' jurisdictional assertions will come into conflict, and how any such conflict might be resolved.This is particularly true because the CFTC has taken a broad view of its digital-assets jurisdiction while the SEC has failed thus far to define its own jurisdiction with precision. This is an area that will continue to evolve in the next few years.[16]

In practical terms, a target of an investigation involving a product or market in which the CFTC and SEC may have concurrent jurisdiction or where questions of jurisdiction are not fully resolved will often fail to persuade enforcement staff or supervisors to abandon their inquiry in the absence of controlling case law, particularly early in an investigation. However, a response strategy guided by experienced counsel should include consideration and advocacy of potential defects in the authority's jurisdictional theory, and the difficulties of prevailing at trial if the parties were not to reach a negotiated settlement.

## E. The Role of Internal Counsel and Compliance in Responding to Complaints or Investigations

Failure to react promptly and appropriately to suspected misconduct can be costly. Numerous high-profile CFTC and SEC investigations involving participants in the securities and commodities markets have highlighted the potential pitfalls of failing to take suspected misconduct seriously. On the other hand, reacting promptly but inappropriately carries its own risks. This is the tension that internal counsel and compliance face every time an allegation of misconduct is raised. Balancing these tensions is difficult, but there are some steps that internal counsel and compliance can take to protect the organization.

*First*, the importance of adequate communication among the stakeholders in an investigation cannot be overemphasized. From the beginning of an investigation, internal counsel, the relevant business, and compliance should work closely together

14. William Hinman, Dir., Division of Corporate Finance, Remarks at the Yahoo Finance All Markets Summit: Crypto. (June 14, 2018).
15. *See* Joint Statement from CFTC and SEC Enforcement Directors Regarding Virtual Currency Enforcement Actions (Jan. 19, 2018). The statement followed immediately after several enforcement actions the CFTC filed against virtual currency schemes that featured collaboration between the two agencies. *See* Remarks of Commissioner Brian D. Quintenz at FIA's 40th Annual Law and Compliance Conference (May 2, 2018) (citing enforcement actions against My Big Coin and CabbageTech to support the assertion that "the CFTC has worked closely with the SEC in bringing civil enforcement actions against fraud, market manipulation and disruptive trading involving virtual currency.")
16. Currently-pending and future enforcement actions, cases litigated in U.S. courts, and policy declarations will continue to shape these authorities' jurisdiction over digital-assets markets. For example, in December 2020 the SEC charged Ripple Labs Inc. and two of its executives with engaging in an illegal securities offering. The SEC alleged that Ripple's sale of XRP tokens was an unregistered offering, in contrast to sales of other digital assets that the SEC has not considered to be securities, such as Bitcoin. *See* Press Release, *SEC Charges Ripple and Two Executives with Conducting $1.3 Billion Unregistered Securities Offering* (Dec. 22, 2020), **https://www.sec.gov/news/press-release/2020-338**. And in a speech given on April 16, 2021 at Texas A&M's Bitcoin Conference, CFTC Commissioner Dawn Stump added that she was closely watching the SEC's ongoing enforcement action against Ripple because "the question of whether XRP is a security will be crucial," and it would "help to establish the scope of the SEC's authority in the digital assets space." During this speech, Commissioner Stump also pointed out that the CFTC's regulatory authority is limited to derivatives (such as futures and swaps) associated with underlying commodities, including digital asset commodities, as opposed to the underlying commodities themselves. However, Stump noted that the CFTC does have authority to investigate and prosecute civil enforcement actions in the cash commodity markets in cases of fraud or manipulation, including the Bitcoin cash market. *See* Remarks of Commission Dawn D. Stump Before Texas A&M's Bitcoin Conference (Apr. 16, 2021), **https://www.cftc.gov/PressRoom/SpeechesTestimony/opastump**.

to ensure that everyone who needs to know about the investigation has adequate information about what is being investigated and what needs to be done to conduct the investigation. Part of this process involves ensuring that whoever receives the initial inquiry—whether a customer complaint, regulatory or self-regulatory organization request or whistleblower complaint—knows who needs to receive this information. That list should include compliance, internal counsel, and senior business leaders. Critically, an investigation should: (1) have legal advisors involved at the outset to reduce the risk of non-privileged communications by businesspersons and management, and to avoid non-privileged interviews and investigations by the business; and (2) distribute a document preservation notice.

*Second*, it is critical that a timely determination is made as to whether an internal investigation is appropriate. Internal counsel and compliance play an important role as an initial gatekeeper for any complaints or regulatory demands. Because they have experience in these matters, they have the ability to identify whether a complaint may be baseless and whether a regulatory inquiry is routine. By exercising these gatekeeper functions, internal counsel and compliance may be able to help provide early closure to non-meritorious claims. On the other hand, internal counsel and compliance can also focus on meritorious claims to ensure that the company can take early steps that will maximize its cooperation credit, such as implementing quick remedial actions.

*Third*, once it is determined that an internal investigation is appropriate there should also be guidance on how the investigation will be conducted. Following receipt of a complaint or government inquiry—especially one that suggests possible serious misconduct—there is always the risk that the investigation will take on a life of its own. Therefore, internal counsel and compliance should ensure that there is an adequate plan in place for the initial inquiry. This initial plan needs to include clear information on who will conduct the investigation and the goals of the investigation. It should also identify a point person and a member of the legal team—either internal or external counsel—who will handle any contacts with the complainant or governmental authorities.

A critical aspect of this initial plan is ensuring that there is proper governance and supervision by internal counsel and compliance. Failure to have this supervision can be costly.

For example, in 2020, the CFTC reached a $127.4 million settlement with a multinational bank based in Canada, which resulted from the bank's failure to respond candidly in connection with a prior spoofing investigation by the CFTC. Among various charges, the bank was heavily penalized for compliance and supervision failures and agreed to pay $50 million to settle those charges. The CFTC found that despite the bank's general guidance on supervision stating that supervisors were responsible for "monitoring each trader" for compliance with business conduct standards, the bank did not have supervisory procedures for conducting such monitoring or attesting that it had occurred.[17] This penalty demonstrates that merely having written policies, procedures or guidance is not sufficient to avoid compliance and supervision liabilities; rather, the CFTC is looking for a detailed, consistent and effective approach that "instill[s] a meaningful culture of compliance among their personnel."[18]

17. CFTC No. 20-26 (Aug. 19, 2020).
18. Press Release, (Aug. 19, 2020). **https://www.cftc.gov/PressRoom/PressReleases/8220-20**.

Also in 2020, the CFTC, DOJ, and SEC reached a massive settlement of $920 million with a major U.S.-based multinational financial institution and other related entities to resolve spoofing charges.[19] The CFTC faulted the bank for failure to identify, investigate and stop the spoofing conduct, specifically criticizing its surveillance system for lacking "the ability to effectively identify spoofing conduct" prior to 2014.[20] The CFTC found that the bank failed to provide adequate supervision despite the rollout of an improved surveillance system and encountering "numerous red flags" such as internal alerts and trader complaints, as well as CME and CFTC inquiries.[21] Similarly, the SEC noted that the spoofing occurred over the course of several years despite policies prohibiting such conduct.[22]

Similarly, in 2017, the CFTC fined a U.S. investment bank $2.5 million for, amongst other violations, failing to adequately supervise an initial response to a regulatory inquiry.[23] According to the settlement, the bank failed to adequately supervise its employees and agents entrusted with investigating a CME inquiry into alleged pre-hedging of block trading. The CFTC alleged that, although the bank's compliance and legal departments were primarily responsible for responding to the inquiry, they relied on the operations support group to gather information for the bank's response and provided only "minimal oversight." This was problematic because the operations support group primarily handled operational and technical issues. The group also was not trained in investigatory procedures nor was it fully independent of the area under investigation.

According to the CFTC, this failure to supervise was aggravated by the operations group's decision to only provide an "abridged version" of the relevant records to the legal and compliance departments that failed to disclose "a number of occasions" where certain traders traded futures contracts in the five minutes before the execution time of block trades. As a result, the CFTC found that the bank's "failure to stay adequately informed" regarding the activities of the operations support group contributed to its failure to detect the improper trading activity before the traders misled the CME during the interviews.[24]

The SEC has similarly pursued enforcement actions against companies for failure to supervise violations. In 2019, the SEC settled a complaint against a Los Angeles-based registered investment advisor failing to implement compliance policies and procedures and investigate red flags that had been raised about one of its advisers. According to the SEC's order, the adviser defrauded two clients for several years, misrepresenting the amount of management fees they paid, and misappropriated over $200,000 to support one of the adviser's own investments, a struggling restaurant. Notably, the company had multiple indications that the rogue adviser was violating the law: an outside compliance consultant that the adviser had hired to review its compliance had warned the company that the adviser may misappropriate client funds to improperly support his restaurant; and two different clients had complained about the adviser's handling of their accounts. Despite having policies and procedures in place that would have required an investigation into the red flags, the adviser failed to investigate. The settlement included a formal censure as well as a $220,000 civil penalty and $328,912

19. CFTC No. 20-69 (Sept. 29, 2020).
20. *Id. at* 7.
21. *Id.*
22. Exchange Act Release No. 90035, ¶ 11 (Sept. 29, 2020).
23. CFTC No. 17-25 (Sept. 22, 2017).
24. *Id.*

in restitution to clients. The adviser was sentenced to 30 months' incarceration and ordered to pay $1.2 million in criminal restitution.[25]

The SEC also charges companies for failing to have adequate policies and procedures in place to prevent and detect misconduct. For example, in 2018, the SEC settled charges with a major investment manager for failing to have compliance and surveillance procedures in place that were reasonably designed to prevent and detect misconduct that harmed its customers. Specifically, the SEC found that from 2009 to 2012 the investment manager's traders and salespersons convinced customers to overpay for Residential Mortgage Backed Securities by misrepresenting how much the company had paid to acquire the securities. These rogue employees also illegally profited from excessive and undisclosed commissions. As a result, the SEC found that the company failed to properly supervise these employees, to the detriment of its customers. The settlement included a formal censure as well as a civil penalty of $5.2 million as well as disgorgement (with interest) of more than $10.5 million paid to customers affected by the misconduct.[26]

Proper supervision of an internal investigation is also important from a privilege perspective.

The attorney-client privilege protects "(1) a communication between client and counsel that (2) was intended to be and was in fact kept confidential, and (3) was made for the purpose of obtaining or providing legal advice."[27] The privilege protects communications both to and from an attorney—whether internal or external—so long as the communication's purpose is related to the giving or receiving of legal advice.[28]

The attorney work-product doctrine provides qualified protection for materials prepared by, or at the behest of, counsel in anticipation of litigation. It applies to materials that are: "(1) a document or tangible thing, (2) that was prepared in anticipation of litigation, and (3) was prepared by or for a party, or by his representative."[29] The test for whether a document has been prepared in anticipation of litigation is whether "in light of the nature of the document and the factual situation in the particular case, [it] can fairly be said to have been prepared or obtained because of the prospect of litigation." [30] The potential litigation can be in any forum (i.e., judicial proceedings, arbitrations, administrative actions, etc.), and, as a result, documents prepared as part of a response to a government investigation are also protected.[31]

Courts analyzing whether internal investigations are protected by the attorney-client privilege or the work-product doctrine have typically focused on the role that attorneys played. When counsel has no role or a limited role in the process, courts are unlikely to deem the initial investigation privileged. For example, in *United States v. ISS Marine Services, Inc*., the United States District Court for the District of Columbia held that a

25. Release No. 5361 (Sep. 23, 2019).
26. Exchange Act Release No. 83408 (June 12, 2018).
27. *In re County of Erie*, 473 F.3d 413, 419 (2d Cir. 2007).
28. In evaluating privilege claims, courts will carefully consider the attorney's role and whether the communication was made for the purpose of securing legal advice. *Upjohn Co. v. United States*, 449 U.S. 383, 394 (1981). Where communications from counsel contain both business and legal advice, courts will generally make an inquiry into the "primary purpose" of the document in order to determine if the privilege applies. *Phillips v. C.R. Bard, Inc.*, 290 F.R.D. 615, 628 (D. Nev. 2013). In other words, a communication will only be deemed privileged if the purpose of the communication was "to discern the legal ramifications of a potential course of action." *Id.* (quoting *Henderson Apartment Venture, LLC v. Miller*, No. 2011 WL 1300143, at *9 (D. Nev. Mar. 31, 2011); *Premiere Digital Access*, Inc. v. Central Telephone Co., 360 F. Supp. 2d 1168 (D. Nev. 2005)).
29. *In re Veeco Instruments, Inc. Sec. Litig.*, No. 05-MD-01695, 2007 WL 724555, at *4 (S.D.N.Y. Jan. 24, 2007).
30. *Id.*
31. *In re LTV Sec. Litig.*, 89 F.R.D. 595, 612 (N.D.Tex.1981) ("Investigation by a federal agency presents more than a 'remote prospect' of future litigation and gives grounds for anticipating litigation sufficient for the work-product rule to apply.").

report on potentially fraudulent billing practices, which was prepared by non-attorneys and delivered to the Board of Directors—rather than counsel—was not privileged.[32] In doing so, the court rejected the defendant's argument that the report should be deemed privileged because the company initially consulted with outside counsel before beginning the process and then sent the report to counsel two months after it was completed.[33] According to the court, such "limited interaction with counsel at the beginning and end of an otherwise attorney-free internal investigation is an insufficient basis to support application of the attorney-client privilege."[34]

Conversely, when attorneys actively supervise the process, courts will typically deem internal investigation reports (or other reports prepared by non-attorneys) privileged. For example, in *In re Kellogg Brown & Root Inc*., the United States Court of Appeals for the District of Columbia considered whether a report that was created after a Kellogg Brown & Root ("KBR") employee alleged that the company was inflating costs and accepting kickbacks on government contracts was privileged.[35] The report was prepared in connection with an investigation that "was conducted under the auspices of KBR's in-house legal counsel," which relied on fact-gathering—including employee interviews—by non-attorneys.[36] The District Court initially ruled that such reports were not privileged because much of the investigation was conducted by non-attorneys and the investigation was conducted to comply with regulatory requirements.[37] Rejecting the District Court's decision, the Court of Appeals ruled that the investigation was privileged because it was supervised by attorneys and "obtaining or providing legal advice was one of the significant purposes of the internal investigation."[38]

Moreover, as a general matter, lawyers who are compliance officers are deemed to be functioning as compliance officers and thus their communications are not privileged. Thus, unless Compliance personnel are operating at the direction of Legal, their communications are not privileged.

*Fourth*, internal counsel should consider at the outset whether it is necessary to put in place a litigation hold. Under U.S. law, the duty to preserve evidence arises in three situations: (1) when a complaint is filed;[39] (2) when litigation is reasonably anticipated or foreseeable;[40] and (3) due to statutory notice.[41] When receiving an inquiry or complaint, internal counsel must evaluate the nature of the complaint to determine whether this standard is satisfied.

As a practical matter, erring on the side of caution is often the best course. If the complaint comes to the authorities' attention, failing to preserve such information may impair the credibility of the company and any internal investigation it has undertaken, increase settlement or penalty amounts, compromise cooperation credit, and/or potentially provide an independent basis for criminal sanctions or other severe penalties.

---

32. 905 F.Supp.2d 121, 132 (D.D.C. 2012).
33. *Id.*
34. *Id.*
35. 756 F.3d 754, 756 (D.C. Cir. 2014).
36. *Id.* at 757.
37. *Id.* at 758-759.
38. *Id.* at 759.
39. *Zubulake v. UBS Warburg LLC,* 220 F.R.D. 212, 217 (S.D.N.Y. 2003) (*Zubulake IV*).
40. *Id.* at 216 (holding that a party has a duty to preserve evidence when that party "should have known that evidence may be relevant to future litigation"); *see also Grabenstein v. Arrow Elec., Inc*., No. 10-CV-02348, 2012 WL 1388595, at *2 (D. Colo. Apr. 23, 2012) (same), *Keithley v. Home Store.com, Inc*., 2008 WL 3833384, at *5 (N.D. Cal. Aug. 12, 2008) (same) (citing *Zubulake IV*), *United States v. Koch Indus. Inc*., 197 F.R.D. 463, 482 (N.D. Okla. 1998) (recognizing defendant's pre-litigation duty to preserve evidence based on other parties' participation in litigation involving same circumstances).
41. *See e.g.,* 15 U.S.C. § 78q.

Therefore, an early priority should be to collect all relevant information as efficiently and cost-effectively as possible whilst protecting the credibility of the investigation. Collection efforts are dominated by issues relating to the proliferation of email and other electronically stored information ("ESI"). As such, internal counsel must be familiar with and mindful of regulatory requirements and case law in their jurisdiction and others to which the investigation may subsequently spread (to the extent that this can be ascertained) regarding the scope of ESI to be preserved and collected. Key issues include whether preservation/collection is limited to "readily available information", and what that means with respect to back-up tapes and archived data. In addition, it is imperative that counsel consider whether any of the data is subject to data protection statutes, such as the General Data Protection Regulation or California Consumer Privacy Act, which may limit the ability to transfer that data. If potential data protection issues are identified, then internal counsel should work to resolve them as early as possible.

*Fifth*, while not every investigation will require external counsel, internal counsel should recognize when it is necessary. This determination is ultimately the most critical task facing internal counsel. On the one hand, internal counsel and compliance have the advantage of significant institutional knowledge of a company, which they can often leverage to quickly conduct an investigation in a cost-effective manner. On the other hand, they also have other responsibilities and cannot necessarily devote the same attention to an investigation as outside counsel. In addition, outside counsel will often have more specialized knowledge of the specific legal issues that the company is investigating. Investigations by outside counsel are also more likely to be viewed as credible by regulators and will generally have stronger privilege protections.

This determination, therefore, will turn on balancing the facts. If the alleged misconduct involves an individual employee and does not implicate potential violations of law, internal counsel, with support from appropriate business functions such as the internal audit department, can investigate the allegations and recommend appropriate remedial and personnel actions to management. Conversely, where the potential misconduct is widespread, may involve officers or directors, potentially violates the law affects corporate governance, or subjects the company to government investigation and enforcement actions, the company should utilize external counsel to lead the investigation.

Once external counsel is engaged, however, the role of internal counsel and compliance does not disappear. Instead, it changes to one of management and communication. Internal counsel and compliance will always have more significant institutional knowledge about the company and relationships with stakeholders that will be crucial to a successful internal investigation. Internal counsel will also have a much better understanding of what is realistically achievable. Therefore, at this stage, internal counsel and compliance should work to create a strong partnership with external counsel that leverages their institutional knowledge within a company to allow external counsel to conduct an effective investigation.

As part of creating this partnership, it is best practice for internal counsel and compliance to work with external counsel at the outset of the engagement to create an investigative plan that is both feasible and sufficient. In crafting this plan, internal counsel should work with external counsel to consider: (1) potential and desired outcomes, (2) expectations of any relevant agencies, (3) expectations of the relevant

business unit, and (4) how to structure investigative processes to minimize unnecessary or premature risky and constraining decisions. A key example of where this may come up is in addressing potential risks of privilege waivers, which may provide short-term benefits in responding to a government investigation, but may make it impossible for the company to assert privilege in any follow-up investigations.

At the start of an investigation, stakeholders should set forth an efficient plan for bottoming out pertinent issues and responding effectively. While it is important to begin with an endpoint in mind, any investigative plan should be flexible enough to incorporate and respond to suggested modifications, including from government agencies.

After they have agreed upon a plan, internal counsel and compliance's role typically changes to one of adviser. In this role, they are best placed to work with external counsel and businesses within the company to help complete the investigation. This involves a myriad of tasks, such as helping with data collection, identifying potential witnesses or data sources, and ensuring that the business and external counsel both understand what is realistically achievable.

In this role, internal counsel also plays an important liaison function. Internal counsel because they know the company and its employees will always be the first point of contact between an employee and external counsel. In that role, they are best placed to speak with employees to explain the investigation and external counsel's role. In playing that role, internal counsel's role is invaluable, as explanations by internal counsel can often help soothe a potential interview subject's nerves and facilitate a successful interview.

*Finally*, internal counsel will likely play a key role in the determination of the timing and content of any disclosures to shareholders or other relevant constituencies.

## F. Commencement Phase: Anticipating How a U.S. Investigation Can Begin

### 1. Sources and Triggers for Investigations

A variety of events may warrant conducting an internal inquiry. Investigations may be commenced through the direct intervention of a government agency, whether of its own volition or as a result of information supplied to it. Investigations can be triggered by third party allegations (for example, in a customer or counterparty compliant, in the press or in the context of ongoing regulatory investigations) or staff concerns (in the context of internal audit or compliance functions, exit interviews, disciplinary procedures, or by internal whistleblowing). An internal investigation may also be the prudent response to known regulatory enforcement in a discrete area which indicates broader risk issues.

### 2. Contact by Authorities

#### (a) Informal Requests and Subpoenas

Both the CFTC and the SEC have statutory authority to issue subpoenas for documents, as well as subpoenas requiring testimony by witnesses. Similarly, the DOJ can seek a subpoena from a grand jury, and can also issue its own administrative subpoenas, without intervention of a grand jury, in connection with investigations into violations of certain statutes. However, the CFTC, SEC

and DOJ all often begin investigations by making voluntary requests for information, rather than by issuing subpoenas.

Upon receipt of either a subpoena or a voluntary request, an organization must very quickly issue a litigation hold to ensure that relevant documents and information are not destroyed. Even an accidental destruction of relevant material following a government request would likely be viewed very negatively by the relevant authority, and could result in higher penalties in any negotiated settlement. A reckless or intentional destruction of relevant material following a government request could invite a criminal charge of obstruction of justice. It is therefore essential that a sufficiently broad litigation hold be issued. When drafting the litigation hold, the organization should consider:

1. The scope of documents subject to the hold;
2. The scope of distribution, which may include both individual employees and the IT or records department, and which may require translation into other languages; and
3. Whether it will be necessary to instruct relevant IT or records personnel to suspend normal document-destruction practices, identify the location of relevant information, and undertake collection efforts such as forensic imaging of electronic devices.

The organization should then develop a strategy for response. The organization should consider whether it may be unable to provide certain requested information, whether for a legal reason such as a data protection or confidentiality requirement, or a practical reason such as the non-existence of the information or any undue burden in providing it. It may be helpful at this stage to have outside counsel contact the requesting authority to determine whether there may be an opportunity to negotiate a staged or narrower production. When properly conducted, these discussions may allow the organization to gain valuable insight into the nature and scope of the authorities' interest.

Once the organization has a grasp of the potential theories of violation, it can make a more informed decision about the potential benefits and drawbacks of fully cooperating with a voluntary request or of resisting production of some or all of the requested information. Where the request comes from its primary regulator or it otherwise appears that a serious violation of law may have occurred, a company may find it beneficial to provide the most fulsome response practicable, in order to preserve it relationship with the authorities and its opportunity to receive maximal credit for cooperating with the authority's investigation. Conversely, where the organization believes that its legal exposure is very limited or perhaps nonexistent (whether because of jurisdictional, legal or factual defenses), it may prefer to provide the narrowest response possible—or even to decline to provide a substantive response if in receipt of only a voluntary request—in order to minimize the costs of its response.

With certain limited exceptions, an organization is legally bound to comply fully with a duly authorized and served subpoena from a government authority

acting within its jurisdiction. Nevertheless, even within this boundary, the organization can seek to negotiate a limited response, as well as a longer period for response or a staged response. It could also determine to provide additional cooperation to the government investigators beyond mere subpoena compliance, should it conclude such to be appropriate under the particular circumstances presented.

Whatever approach the organization takes in responding, it must ensure that any information provided is accurate and not misleading. Knowingly providing inaccurate or misleading information to the CFTC, SEC or DOJ constitutes a felony criminal violation. Even a mistaken provision of inaccurate information can expose an organization to higher penalties. For regulated entities, a mistaken provision of inaccurate information can also potentially support a charge for supervisory failures. For example, in 2017, the CFTC charged an investment bank with a failure to adequately supervise its response to a CFTC inquiry, based on the bank's Legal and Compliance functions passing along to CFTC information prepared by an operations function, which was incomplete and which Legal and Compliance had failed to vet.[42]

Finally, the organization should consider whether it will be necessary to seek to shield any of the information being provided form public disclosure. The U.S. Freedom of Information Act ("FOIA") requires government agencies to provide information upon request—including information that the government obtained from third parties. However, this requirement is subject to a number of exceptions, which prohibit the government from providing, for example, confidential information and trade secrets. If any such information is provided to the government, it should be clearly designated as confidential, and should be accompanied by a letter requesting that the materials be treated as confidential and not be provided to third parties.

### (a) Search Warrants and Dawn Raids

In certain circumstances, the DOJ may employ more drastic measures to obtain information from an organization, including through the execution of search warrants. A search warrant is a court order authorizing law enforcement authorities to enter and search premises and to take away specified documents or items as evidence. When executing search warrants against businesses, the authorities often conduct a "dawn raid," which is the informal term used to describe searches and seizures by authorities that are conducted without warning. As the term suggests, law enforcement conducting a dawn raid will usually appear at company offices early in the day, unannounced, so as to catch a company unprepared and minimize the risk that a respondent will destroy relevant evidence.

Execution of search warrants typically create high-pressure and stressful situations, so it is important for companies to prepare for these events in advance. It is not uncommon for companies to conduct mock dawn raids to stress-test existing protocols and procedures and train company employees. Thus, effective dawn raid response begins before a dawn raid actually occurs. For detailed guidance, please refer to the Clifford Chance Dawn Raids App,

42. *CFTC No. 17-25 (Sept. 22, 2017).*

which covers over 90 different authorities across Europe, Asia Pacific and the United States.[43] It includes specialist advice on numerous types of dawn raids such as antitrust, tax, fraud, anti-corruption, and employment, and is designed to provide the information needed to effectively deal with urgent situations.

To prepare for a dawn raid, a company should establish a response protocol and designate responsible employees to coordinate in the event of a raid. Where possible, employees selected to coordinate should be those with the lowest risk of being the target of an investigation.

One of the first steps a company should take when responding to a search warrant or dawn raid is to make proper notifications. This list of individuals to be notified will generally include executive leadership, in-house legal and compliance officers, public relations, and external counsel. In particular, companies should notify external counsel as soon as practicable to give counsel time to travel to the site of the investigation and intervene with law enforcement. A search warrant or dawn raid response plan should identify who needs to be notified and the proper contact information so that notification can be accomplished quickly and efficiently.

Once the search has commenced, the company should sequester investigators as soon as possible (*e.g.*, by asking them to wait in a conference room). This minimizes disruption to the company's business. In the meantime, if possible, the company should ask all non-essential personnel to leave the premises (*e.g.* by asking them to work from home or from a satellite location).

After sequestering investigators, counsel should conduct certain verification measures. One important aspect of this process is to ask for and review the investigators' credentials. For example, Federal Bureau of Investigation (FBI) agents are required to carry badges and government-issued photo identification, and they generally will provide this information with limited (if any) objection. Responsible employees should record the names and contact information of each investigator for later reference. Another important verification procedure is to analyze the warrant purported to authorize investigators to conduct the dawn raid. A defective search warrant (*e.g.* incorrect date or address) can be grounds to lawfully resist abiding by a search warrant, which is otherwise compulsory. The search warrant will also provide crucial details to responsible employees as to the scope of the permitted investigation.

Once this verification has concluded—and ideally after external counsel has arrived and the company has done what it can to narrow the scope of investigation—the actual search will begin. During this process, employees should carefully monitor and record each investigator's actions and progress. This will not only help speed up business recovery and continuity processes, but it will also inform stakeholders later in an investigation as to what information/evidence law enforcement may already possess. If possible, at least one employee monitor should be designated for each investigator so that a comprehensive record can be made. Monitors should remain respectful but

43. *See* Dawn Raids App, Clifford Chance, https://www.cliffordchance.com/insights/resources/apps/dawn-raids-app.html

keep detailed notes, including by taking photos of any issues that arise (*e.g.* damage done by an investigator).

While a government investigator generally has significant authority when executing a search warrant, counsel can still advocate on the company's behalf. This includes lodging objections where law enforcement exceeds the scope of the search warrant, asserting privilege, and seeking to protect sensitive business information (*e.g.* trade secrets).

Once a search is complete, stakeholders must quickly do damage control and take certain preparatory and protective measures. This includes executing a communication plan to preempt press rumors of misconduct, implementing a document hold to prevent spoliation of evidence, and potentially conducting an internal investigation. The end of a search is often only the beginning of a government investigation.

## 3. Internal Identification of Potential Issues

### (a) Discovery of Misconduct

Discovery of possible misconduct can occur while undertaking routine corporate inquiries such as internal audits and due diligence. In addition, employees and others connected with the company may be aware of or suspect a violation and make a report internally or to a governmental agency. Companies should be sensitive to increasing whistleblower activity.

### (b) Internal Reports

Internal reports of potential misconduct, whether to in-house counsel, human resources personnel, or employee supervisors, will require an assessment of whether the issue presents a violation of law, regulations, or company policy. Not all reports of misconduct within a company will necessitate an internal investigation conducted by outside counsel or the creation of a special investigative board committee. If the alleged misconduct involves an individual employee and does not implicate potential violations of law, in-house counsel, with support from appropriate business functions such as the internal audit department, can investigate the allegations and recommend appropriate remedial and personnel actions to management. Conversely, where the potential misconduct is widespread, may involve officers or directors, potentially violate law, affect corporate governance, or subject the company to government investigation and enforcement actions, the company should utilize external counsel to lead the investigation..

### (c) Investigations

During an investigation, a company may uncover evidence of a different but related category of misconduct. In these situations, the company should consider the potential scope of the issue as well as whether leniency may be available for the conduct.

### (d) Whistleblowers

Due to the increases in protections, an investigation is now more likely to be triggered by internal whistleblowers. Participants in the securities and commodities markets should be aware that both the securities and commodities laws provide for whistleblower protections. Section 23 of the CEA

provides for various protections—including a private right of action for retaliation that allows for reinstatement, back pay with interest, and compensation for special damages—and employers cannot discriminate against a whistleblower in retaliation for reporting misconduct to, or assisting in investigations of, the CFTC.[44] The CFTC has recently increased its commitments to anti-retaliation by amending its rules. Likewise, SEC whistleblowers are provided protection pursuant to the Sarbanes Oxley Act ("SOX") of 2002 and the Dodd-Frank Act ("DFA") of 2009. The DFA created the Whistleblower Protection Program (the Program), pursuant to which individuals who voluntarily report original information about potential violations of federal securities laws are protected from retaliation and entitled to a financial award if the information leads to a successful judicial or administrative enforcement action in which the SEC obtains monetary sanctions over US$1 million.[45] The procedures and protections available to whistleblowers under SOX and DFA differ, though both prohibit retaliation against whistleblowers. SOX is enforced by the Occupational Safety and Health Administration (OSHA), which is responsible for investigating claims and may pursue an administrative remedy.[46] Additionally, a SOX whistleblower may bring a retaliation claim in federal court if the Secretary of Labor "has not issued a final decision within 180 days of the filing of [a] complaint and there is no showing that such delay is due to the bad faith of the claimant."[47] Individuals claiming DFA protections, on the other hand, may immediately bring a claim in federal court. Also, in determining retaliatory conduct for whistleblowers, courts have refused to create a bright-line standard for what constitutes adverse employment action, meaning retaliation cases are likely to be difficult to dismiss and to defeat at the motion for summary judgment stage, especially given that the burden on the whistleblowers are not onerous. These reasons give whistleblowers more of an incentive to report violations to the CFTC, the SEC, and other agencies.

### 4. Awareness of Changes in Law/Regulation, Enforcement Priorities and Investigations of Other Market Participants and Responsive Risk Assessments

Often, government agencies and prosecutors will conduct industry-wide investigations of entities that undertake similar business activities or offer similar products where a violation is suspected at a peer company, especially where the violation may involve collusive conduct. Counsel should monitor developments and trends in agencies' enforcement priorities and conduct appropriate due diligence where an investigation of a peer company involves a product or business function that the company shares. Often, similar structural characteristics or incentives exist in companies in a given industry that independently lead employees to undertake similar actions. An initial risk assessment is therefore highly advisable where a peer company is under investigation for conduct that could plausibly occur at the company. Similarly, organizations should consider conducting risk assessments whenever there is a potentially relevant change in law or regulation.

44. 15 U.S.C. § 78u–6(h)(1)(A).
45. *See* 15 U.S.C. § 78u-6. Dodd-Frank also imposed a similar regime under the Commodity Exchange Act. See 7 U.S.C. § 26.
46. See 29 C.F.R. § 1980.104(e).
47. 18 U.S.C. § 1514A(b)(1)(B).

In all instances, a risk assessment should seek to determine whether the company's control environment is properly calibrated to account for the salient legal risks and whether the proper proportion of compliance resources are devoted to the most consequential risks. The risk assessment should also consider whether supplemental policies or training are advisable. The necessity of conducting a risk assessment is particularly acute where the investigated conduct could involve external coordination or communications, because investigators could come into possession of materials involving the company through investigation of others. A risk assessment should be guided by counsel that is familiar with potentially applicable U.S. law.

## G. Commencement Phase: Analyzing U.S. Agencies' Priorities

### 1. Cooperation Expectations of U.S. Authorities

After a company learns that a governmental authority has begun an investigation, the company must decide how cooperative it will be with the authority. That decision is laden with numerous considerations, and a decision either way involves many potential benefits and drawbacks.

#### (a) DOJ

The standards that guide the U.S. Department of Justice's criminal prosecution of companies are set out in the Justice Manual (formerly known as the U.S. Attorneys' Manual) "Principles of Federal Prosecution of Business Organizations." That section of the Justice Manual lists ten factors—often called the "Filip Factors," so-named after former Deputy Attorney General ("DAG") Mark Filip—which DOJ attorneys consider in determining whether to charge a company. These factors include the company's "willingness to cooperate in the investigation of its agents" and its "efforts . . . to cooperate with the relevant government agencies."[48] In other words, whether and the extent to which a company cooperates with the DOJ directly affects the DOJ's likely treatment of that company.[49]

The potential benefits of cooperation are significant. The Justice Manual explains that "[c]ooperation is a mitigating factor, by which a corporation . . . can gain credit in a case that otherwise is appropriate for indictment and prosecution."[50] Such credit can lead to reduced charges and penalties, or avoidance of charges altogether. Failure to cooperate appropriately, on the other hand, can result in significant penalties and in cases of egregious misconduct, other consequences such as charges of obstruction of justice.

Although the Justice Manual does not formally define "cooperation," it identifies how a company can be eligible for cooperation credit. Of utmost importance, "the company must identify all individuals involved in or responsible for the misconduct at issue, regardless of their position, status or seniority, and provide to the Department all facts relating to that misconduct."[51]

48. U.S. Dep't of Justice, JUSTICE MANUAL, § 9-28.300, **https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations#9-28.300** (hereinafter "Justice Manual"); Mark Filip, U.S. Dep't of Justice, Principles of Federal Prosecution of Business Organizations (Aug. 28, 2008), **https://www.justice.gov/sites/default/files/dag/legacy/2008/11/03/dag-memo-08282008.pdf**.
49. U.S. Dep't of Justice, Evaluation of Corporate Compliance Programs (June 2020), **https://www.justice.gov/criminal-fraud/page/file/937501/download**.
50. Justice Manual, *supra* note 47 at § 9-28.700.
51. *Id.*

These relevant facts include: "[H]ow and when did the alleged misconduct occur? Who promoted or approved it? Who was responsible for committing it?"[52]

Pursuant to DOJ policy, "any company seeking cooperation credit in criminal cases must identify every individual who was substantially involved in or responsible for the criminal conduct."[53] Pursuant to this policy, companies must "identify all wrongdoing by senior officials" to earn any cooperation credit in a civil case, with maximum credit available only after the company "identif[ies] every individual person who was substantially involved in or responsible for the misconduct."[54]

Cooperation can take many forms, including: producing relevant documents, making employees available for interviews, proffering findings from internal investigations, and assisting in the analysis and synthesis of potentially voluminous evidence. Further, to achieve cooperation under current DOJ policy, corporations must also attempt to identify all culpable individuals, timely produce all relevant information, and agree to continued cooperation even after resolving any charges against the company. The amount of credit earned will depend on the proactive nature of the cooperation and the diligence, thoroughness, and speed of any internal investigation. But the Justice Manual also clarifies that waiver of attorney-client privilege or work-product protection is not required for credit (to avoid placing undue pressure on companies to waive these protections provided by law) so long as the relevant facts concerning misconduct are disclosed.[55]

Notwithstanding the increased responsibility on the part of companies to make "extensive efforts" in their internal investigations, counsel should be aware that the DOJ has, in the past, often conducted its own parallel investigation "to pressure test" a company's efforts, and if the DOJ concludes through its own investigation that the internal investigation's efforts "spread corporate talking points rather than secure facts related to individual culpability," companies will "pay a price when they ask for cooperation credit."[56] Thus, any attempt to cooperate and seek credit should be taken on diligently and with the full commitment of all involved, while maintaining independence and keeping in mind at all times the company's objectives and best interests.[57]

**(1) DOJ Antitrust Division Leniency Program**

A company engaged in cartel conduct that is the first to self-report and fully cooperate with the DOJ's investigation will receive full leniency.[58] The company and its cooperating employees will not be criminally prosecuted.

52. *Id*. at § 9-28.720.
53. Rod J. Rosenstein, Deputy Att'y Gen., U.S. Dep't of Justice, *Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act* (Nov. 29, 2018), **https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0**. The Justice Manual has been updated to reflect these priorities. Justice Manual, *supra* note 47 at §§ 9-28.210, 9-28.300, 9-28.70.
54. *Id.*
55. Justice Manual, *supra* note 47 at § 9-28.710.
56. Marshall L. Miller, Principal Deputy Ass't Att'y Gen., Crim. Div., U.S. Dep't of Justice, *Remarks before the Global Investigation Review Program* (Sept. 17, 2014), **https://www.justice.gov/opa/speech/remarks-principal-deputy-assistant-attorney-general-criminal-division-marshall-l-miller**.
57. Southern District of New York Judge Colleen McMahon's 2019 decision in *United States v. Connolly* highlights potential pitfalls of too-closely aligning an internal investigation with government priorities. In *Connolly*, the court found that a respondent bank had become a *de facto* arm of the government because federal prosecutors and the CFTC exerted control over the way the investigation was conducted. 2019 WL 2120523 (S.D.N.Y. May 2, 2019). While McMahon concluded that compelled testimony in *Connolly* did not warrant overturning the conviction at issue, and subsequent courts have not followed *Connolly*, the decision underscores that counsel must always balance the risks and rewards of any cooperation.
58. U.S. Dep't of Justice, *Corporate Leniency Policy* (1993), **https://www.justice.gov/atr/corporate-leniency-policy**.

Although leniency applicants can still incur liability for civil damages, such liability is limited to actual damages, rather than the usual treble damages provided for by U.S. antitrust laws. A "second in the door" company can still obtain favorable treatment from the DOJ, if it cooperates and provides information valuable to the DOJ's investigation.

The Antitrust Division first developed its Corporate Leniency Program in 1978, but made significant changes to the program in 1993. Under the revised Corporate Leniency Program, the first company to contact the Antitrust Division and report its involvement in a criminal antitrust violation will receive full amnesty from criminal liability for itself and its cooperating employees, as long as the company meets the criteria outlined in the Leniency Program.

A company is eligible for "Type A" leniency if it self-reports an antitrust violation before the DOJ has opened an investigation and: (1) the Antitrust Division has not yet received information about the misconduct from any other source at the time the company comes forward; (2) the company took "prompt and effective" action to terminate its involvement in the illegal activity upon discovering it; (3) the company reports the misconduct with "candor and completeness" and provides "full, continuing, and complete cooperation" throughout the Antitrust Division's investigation; (4) the company admits to a criminal antitrust violation as a "truly corporate act," rather than "isolated confessions of individuals executives or officials"; (5) the company makes restitution to injured parties "where possible"; and (6) the company did not "coerce" another party to participate in the anticompetitive conspiracy and clearly was not the "leader" or "originator" of the misconduct.

A company who does not satisfy the requirements for "Type A" leniency may still qualify for "Type B" leniency. If a company contacts the Antitrust Division after it has opened an investigation, the company may still receive leniency if it is the first company to contact the Division and self-report its involvement in the anticompetitive conspiracy. However, the company will only receive leniency if at the time it self-reports the misconduct, the Antitrust Division does not yet have evidence against the company that is "likely to result in a sustainable conviction." Like Type A applicants, Type B applicants must also take "prompt and effective action" to terminate their involvement in the misconduct, provide "full, continuing, and complete cooperation" with the Division's investigation, confess to a criminal antitrust violation as a truly "corporate act," and make restitution to injured parties where possible.

If these criteria are met, the Division will grant the Type B applicant amnesty from prosecution if it also determines that doing so would not be "unfair to others" based on factors such as: (1) when the company came forward and self-reported the misconduct; (2) how much information and evidence the Division possessed at the time the company self-reported; (3) the company's role in the misconduct; and (4) whether the company "coerced" another party to participate in the misconduct or was the "leader" or "originator" of the conduct.

The Corporate Leniency Program creates a strong incentive for companies to report potential antitrust violations to the Division as soon as possible. The Division grants leniency to only one participant in a given anticompetitive conspiracy. Companies are therefore in a "race" against their co-conspirators, and possibly even their own employees, who may also apply to the Division for leniency individually. The Division has noted that in many cases, the second company to seek leniency has been beaten to the Division's door by only a matter of hours.

The Antitrust Division has established a marker system that permits companies to report a possible violation prior to completing a full investigation of the conduct. A marker secures the company's position as the first to come forward and report a violation, while the company gathers more information. To obtain a marker, counsel for the company must contact the Division and: (1) report that the company has discovered information indicating that it engaged in a criminal antitrust violation; (2) disclose the general nature of the conduct; (3) identify the industry, product, or service involved with enough specificity to allow the Division to determine whether a marker is available; and (4) identify the company.

Division guidance makes clear that because companies are encouraged to seek leniency at the first indication of wrongdoing, the evidentiary standard for securing a marker is relatively low.

The Antitrust Division will not prosecute an applicant who meets the requirements of the leniency program for the antitrust violation that it reports or for "acts or offenses integral to that violation."[59] However, a conditional leniency letter only binds the Antitrust Division, not other agencies or sections of the DOJ. It does not protect applicants from prosecution by other agencies for non-antitrust crimes.

### (b) CFTC

In January and September 2017, the CFTC issued updated guidance on its cooperation and self-reporting programs. In January 2017, CFTC released a pair of "Enforcement Advisories" detailing the factors the Enforcement Division will consider in rewarding cooperation credit to companies and individuals. In September 2017, CFTC issued another "Enforcement Advisory," this time addressing changes to the agency's self-reporting program. The Advisory clarifies the "concrete benefits" a company will receive in return for self-reporting, cooperation, and remediation. More recently, in March 2019, the CFTC followed up on the 2017 Advisories with an Enforcement Advisory addressing "Self Reporting and Cooperation for CEA violations Involving Foreign Corrupt Practices,"[60] and in September 2020, the CFTC issued guidance for Enforcement Division staff to consider in evaluating corporate compliance programs in connection with enforcement matters.[61]

---

59. U.S. Dep't of Justice, *Frequently Asked Questions about the Antitrust Division's Leniency Program and Model Leniency Letters* 7 (2017), **https://www.justice.gov/atr/page/file/926521/download** (Appendix H).
60. U.S. Commodity Futures Trading Comm'n, *Advisory on Self Reporting & Cooperation for CEA Violations Involving Foreign Corrupt Practices* (Mar. 6, 2019), **https://www.cftc.gov/sites/default/files/2019-03/enfadvisoryselfreporting030619.pdf.**
61. *See* James McDonald, Director of the Division of Enforcement, U.S. Commodity Futures Trading Comm'n, *Guidance on Evaluating Compliance Programs in Connection with Enforcement Matters* (Sept. 10, 2020), **https://www.cftc.gov/media/4626/EnfGuidanceEvaluatingCompliancePrograms091020/download**.

The CFTC has recognized the cost-benefit analysis companies go through when they discover misconduct and consider whether to voluntarily report it and explained that the updated policies are intended to "shift this analysis in favor of self-reporting."[62]

Significantly, the CFTC has also stated that it wants its self-reporting program to "line up with other self-reporting programs, most notably at the Department of Justice."[63] One objective of this effort is to limit the extent to which companies subject to oversight by more than one regulator have to deal with "multiple, sometimes conflicting, self-reporting and cooperation programs."[64] Consistent with this approach, the updated self-reporting guidance aims to provide "greater transparency" regarding what the Enforcement Division requires of companies seeking mitigation credit for voluntarily self-reporting misconduct, and the benefits of doing so.[65]

The updated CFTC self-reporting program stops short of the DOJ Antitrust Division Leniency Program's promise of full amnesty for the first company to self-report misconduct. Instead, the CFTC's new guidance promises that if a company or individual self-reports, fully cooperates, and remediates, the Enforcement Division will recommend that the Commission consider a "substantial reduction" from the otherwise applicable civil penalties.

The new guidance does indicate that in certain cases, the Enforcement Division may recommend that the Commission decline to prosecute a company that has self-reported misconduct. However, the guidance indicates the Division will only do so in "extraordinary circumstances" such as when "misconduct is pervasive across an industry and the company or individual is the first to self-report."

To obtain credit, a company must report to the CFTC's Enforcement Division "prior to an imminent threat of exposure of the misconduct" and "within a reasonably prompt time after the company or individual becomes aware of the misconduct." A self-reporting company must disclose "all relevant facts" known to it at the time, including relevant facts about individuals involved in the misconduct. To encourage early disclosure of misconduct, the updated guidance states that the Division will still recommend full self-reporting credit where the company used "best efforts" to: (1) ascertain relevant facts at the time of disclosure; (2) fully disclose the facts known to it at the time; (3) continue to investigate the conduct; and (4) disclose additional relevant facts as they came to light.

The January 2017 Enforcement Advisories provided a detailed overview of factors the Enforcement Division considers in granting cooperation credit. The September 2017 Advisory on self-reporting states that to receive

62. James McDonald, Director of the Division of Enforcement, U.S. Commodity Futures Trading Comm'n, *Speech Regarding Perspectives on Enforcement: Self-Reporting and Cooperation at the CFTC* (Sept. 25, 2017), **http://www.cftc.gov/PressRoom/SpeechesTestimony/opamcdonald092517**; *see also* U.S. Commodity Futures Trading Comm'n, *Enforcement Advisory: Cooperation Factors in Enforcement Division Sanction Recommendations for Companies* (Jan. 19, 2017), **http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/** enfadvisorycompanies 011917.pdf (Appendix A); U.S. Commodity Futures Trading Comm'n, *Enforcement Advisory: Cooperation Factors in Enforcement Division Sanction Recommendations for Individuals* (Jan. 19, 2017), **http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfadvisoryindividuals011917.pdf** (Appendix B); U.S. Commodity Futures Trading Comm'n, *Enforcement Advisory: Updated Advisory on Self Reporting and Full Cooperation* (Sept. 25, 2017), **http://www.cftc.gov/idc/groups/public/@lrenforcementactions/ documents/legalpleading/enfadvisoryself reporting0917.pdf** (Appendix C).
63. *Id.* James McDonald, Director of the Division of Enforcement, U.S. Commodity Futures Trading Comm'n, *Speech Regarding Perspectives on Enforcement: Self-Reporting and Cooperation at the CFTC (Sept. 25, 2017),* **http://www.cftc.gov/PressRoom/SpeechesTestimony/opamcdonald092517**.
64. *Id.*
65. *Id.*

self-reporting credit, a company must also adhere to the terms of the January 2017 cooperation guidance. CFTC considers three broad factors of cooperation:

First, the value of the company's cooperation to the Commission's investigation or enforcement action. In this regard, the CFTC will consider: (1) the materiality of the company's assistance; (2) the timeliness of the company's cooperation; (3) the nature of the company's cooperation, such as whether the company independently investigated the misconduct and provided information that was "truthful, specific, complete, and reliable"; and (4) the quality of the cooperation, based on the extent to which the company investigated the misconduct and the completeness of the information reported.

Second, the value of the company's cooperation to the Commission's broader law enforcement interests. In this regard, the CFTC will consider: (1) whether granting cooperation credit would encourage cooperation by other entities; (2) the significance of the matter under investigation; (3) the extent to which the company's cooperation conserved the Enforcement Division's time and resources; and (4) the extent to which granting cooperation credit would otherwise enhance the Commission's ability to detect and pursue violations of the CEA.

Third, the level of the company's culpability and history of past misconduct, balanced against the company's acceptance of responsibility, mitigation, and remediation. In this regard, the CFTC will consider: (1) the circumstances of the misconduct, including its pervasiveness and the level of involvement by management or officers at the company; (2) prior misconduct by the company; and (3) steps taken by the company to mitigate harm, remediate and prevent future misconduct, and accept responsibility for the misconduct.

As for remediation, to obtain the greatest available cooperation credit, the CFTC requires "timely and appropriate remediation of flaws in compliance and control programs." Formal guidance on this issue indicates that the nature and extent of this obligation will be "fact and circumstance dependent." However, in all cases, a company or individual will be required to disgorge all profits resulting from violations and pay restitution to injured parties "where applicable."

In a Statement from January 2018, then-Director of Enforcement James McDonald remarked on the success in implementing the CFTC's updated self-reporting and cooperation program. While announcing spoofing resolutions with banks, for amounts ranging from $1.6 million to $30 million, McDonald noted that "the fines would have been substantially higher but for each bank's substantial cooperation, and for one of the banks, its additional self-reporting of the conduct."[66]

The 2019 Advisory builds on its predecessors, representing the Enforcement Division's latest effort to define the benefits of and to incentivize voluntary cooperation with the CFTC. The 2019 Advisory targets foreign corrupt

66. James McDonald, Director of the Division of Enforcement, U.S. Commodity Futures Trading Comm'n, *Statement on Recent Civil Settlements and Cooperation* (Jan. 29, 2018), **https://www.cftc.gov/PressRoom/SpeechesTestimony/mcdonaldstatement012918**.

practices such as bribes used "to secure business in connection with regulated activities like trading, advising, or dealing in swaps or derivatives," or corrupt practices "used to manipulate benchmarks that serve as the basis for related derivatives contracts.[67]

Under this Advisory, individuals and entities "not registered (or required to be registered) with the CFTC" will receive a "presumption that [the Enforcement Division] will recommend to the Commission a resolution with no civil monetary penalty, absent aggravating factors" if they (i) "timely and voluntarily disclose" violations of the CEA "involving foreign corrupt practices," (ii) fully cooperate with the CFTC, (iii) undertake "appropriate remediation" as described in the prior advisories, and (iv) disgorge all unlawful profits. Aggravating factors that would foreclose a presumption of no penalty include involvement of "executive or senior level management" in the wrongdoing, "the misconduct was pervasive within the company," or the company or individual was recidivist.

On the other hand, this no-penalty presumption will not apply to individuals and entities registered with the CFTC because such registrants have "existing, independent reporting obligations to the Commission requiring them, among other things, to report any material noncompliance issues under the CEA, which would include any foreign corrupt practices that violate the CEA." Nevertheless, these registrants may still receive credit for self-reporting in accordance with the 2017 Advisories.

The 2020 guidance provided a framework for enforcement staff to evaluate corporate compliance programs in connection with an enforcement matter. This guidance instructed staff to consider a number of non-exhaustive factors in evaluating whether the corporate compliance program was reasonably designed and implemented to accomplish three goals relating to the underlying misconduct at issue: (1) prevention; (2) detection; and (3) remediation.[68]

### (c) SEC

The SEC has long had a cooperation program that aims to encourage cooperation from individuals and companies that are involved in SEC investigations and enforcement actions. The cooperation program applies to all potential violations over which the SEC has oversight, including insider trading, market manipulation, financial fraud, and even FCPA violations. Effective cooperation can lead to a deferred prosecution agreement or in limited circumstances a non-prosecution agreement.

With regards to cooperation by corporate entities, the SEC's cooperation framework can be traced to a report issued in October 2001 in which the agency explained why it decided not to take enforcement action against a public company it had investigated for irregularities in its financial statements.[69] The report, commonly known as the Seaboard Report, described the framework through which the SEC evaluates a company's cooperation and

67. James McDonald, Director of the Division of Enforcement, U.S. Commodity Futures Trading Comm'n, *Remarks of CFTC Director of Enf't James McDonald at the ABA National Institute on White Collar Crime* (Mar. 6, 2019), **https://www.cftc.gov/PressRoom/SpeechesTestimony/opamcdonald2**.
68. *See* James McDonald, Director of the Division of Enforcement, U.S. Commodity Futures Trading Comm'n, Guidance on Evaluating Compliance Programs in Connection with Enforcement Matters (Sept. 10, 2020), **https://www.cftc.gov/media/4626/EnfGuidanceEvaluatingCompliancePrograms091020/download.**
69. *See 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*, Exchange Act Release No. 44969 (Oct. 23, 2001).

eligibility for leniency. Specifically, the report outlined four factors the SEC would consider.

First, the SEC considers the company's self-policing prior to the discovery of the misconduct. In this regard, the SEC will assess the company's compliance procedures and whether it has a culture of compliance starting at the executive level. Notably, this factor evaluates the company's pre-existing compliance program, notwithstanding its failure to prevent misconduct.

Second, the SEC considers self-reporting of misconduct once discovered. In this regard, the SEC will assess the effectiveness of the company's own review of the nature, extent, origins and consequences of the misconduct, as well as how promptly and completely the company disclosed the misconduct, not only to the SEC but also to any other relevant parties including other regulatory agencies, self-regulatory organizations, and the public at large.

Third, the SEC considers remediation of the misconduct and its consequences. In this regard, the SEC will assess what steps the company took to address the violation, including disciplining violators (including dismissal if appropriate), upgrading internal controls and implementing policies and procedures designed to prevent further instances of the misconduct, and providing restitution to customers and other individuals who suffered harm as a result of the violation.

Fourth, the SEC considers cooperation with law enforcement authorities. In this regard, the SEC will assess the completeness of the company's cooperation, including providing SEC investigators with all information relevant to its investigation of the misconduct, as well as disclosures relating to the company's remediation efforts.

Even 20 years after its release, the framework described in the Seaboard report continues to govern the SEC's cooperation program and the considerations outlined in the report are regularly included in the SEC's enforcement orders.

As for individuals, the SEC issued a policy statement in 2010 that established a framework for evaluating cooperation by individuals in its enforcement activity.[70] As with corporate entities, the framework for individuals includes four primary considerations.

First, the SEC considers the assistance provided by the cooperator. In this regard, the SEC will assess how useful the cooperation provided was to the SEC's investigation; the timeliness of the cooperation (i.e. whether the individual was first to report and whether it was before or after knowledge of an SEC investigation into the matter); whether the information initiated an SEC investigation; the nature of the cooperation (i.e. whether it was truthful, complete, and reliable); the time and resources conserved as a result of the individual's cooperation; whether the assistance was voluntary; the types of assistance provided by the individual; whether information was provided that would otherwise not have been discovered by investigators; whether the individual encouraged or authorized others to cooperate that may not otherwise; and any other unique circumstances.

Second, the SEC considers the importance of the underlying matter. In this regard, the SEC will assess whether the subject matter is an SEC priority; the type of violation; the age and duration of the misconduct; the number of violations and whether they were isolated or repetitive; the amount of harm (or potential harm) caused by the violations; the type of harm (or potential harm) resulting from the underlying violation; and the number of individuals or entities harmed.

Third, the SEC considers the interest in holding the individual accountable. In this regard, the SEC will assess the severity of the individual's misconduct in light of their knowledge, education, training, experience, and position of responsibility when the violation occurred; the culpability of the individual, both generally and in relation to others who participated in the misconduct; the degree to which the individual took steps to prevent or address the violation, both internally and by notifying law enforcement; the efforts undertaken by the individual to remediate the harm including restitution and assistance in recovering unlawful profits; and other penalties the individual has faced (e.g. any involving state and federal authorities).

Fourth, the SEC considers the profile of the individual. In this regard, the SEC will consider whether the individual has had a history of compliance, particularly with securities laws or regulations; the degree of acceptance of responsibility; and the risk of recidivism, including the opportunity to commit future violations due to their position or status, in light of any existing or proposed safeguards imposed on the individual.

It is worth mentioning that the SEC's investigations can begin with an informal or formal inquiry. Informal inquiries, which are conducted by the Staff without formal authorization from the SEC Commissioners, are voluntary requests.[71] While there is no requirement that a company comply with this voluntary request, failure to cooperate will likely lead to a formal investigation.[72] Formal inquiries are conducted after the Staff receives a Formal Order of Investigation from the SEC Commissioners. The Formal Order gives the Staff subpoena power.[73] The SEC can move from an informal inquiry to a formal investigation at any time, and does not have to inform the subject of the investigation that the Staff is seeking a formal investigation. Typically, the Staff will move to a formal investigation because they believe that the subject of the investigation is not cooperating or that the Staff is not receiving sufficient information to conduct their investigation through voluntary requests.[74]

When an SEC investigation occurs, first, there is a fact-finding stage. During this stage, the Staff—either through an informal inquiry or formal investigation—will review documents provided by a company and interview the relevant company employees and other witnesses, or take their testimony under oath. In this phase, the Staff will determine if they believe that the company violated

70. *Policy Statement Concerning Cooperation by Individuals in its Investigations and Related Enforcement Actions*, Exchange Act Release No. 34-61340 (Jan. 19, 2010).
71. *Id*. at § 2.3. There are five Commissioners who are appointed by the President with the advice and consent of the Senate, who supervise the SEC.
72. *Id*. at § 2.3.2.
73. *See id*. at § 5.6.
74. *See id*. at § 2.3.4.

the U.S. securities laws. If the Staff believes that there were no violations of the U.S. securities laws, they will generally close the investigation.[75]

Second, once the Staff has completed its fact-finding investigation, if the Staff believes that there is a violation of U.S. securities law, the company will receive a "Wells Notice." A Wells Notice is a written notice by which the Staff provides limited information about the basis for the Staff's conclusions and the specific laws that the Staff believe were violated. When a company receives a Wells Notice, it has an opportunity to submit a written response that outlines why it believes the SEC should not pursue an enforcement action against it. The Commissioners will review the Wells Notice and any response from the company to determine whether to institute an enforcement action against the company. Notably, information contained in a response to a Wells Notice may be used against the respondent, so careful consideration of the contents of a response is critical.

### (d) Referral to the DOJ

Although civil regulators such as the CFTC and SEC do not have authority to bring criminal charges against entities or individuals, they can refer criminal violations of U.S. securities and commodities laws to the DOJ for prosecution.

In a January 2012 memorandum, the DOJ provided that "there may be matters that come to the attention of the Department's civil attorneys or attorneys of other agencies in the first instance that would be appropriate for the Department's prosecutors to investigate and pursue to ensure culpable individuals and entities are held criminally accountable. Early and effective communication and coordination will help avoid many problems and enhance the overall result for the United States."[76]

In November 2017, Deputy Attorney General Rod Rosenstein gave remarks in which he indicated that DOJ is seeking further coordination with both domestic regulators as well as foreign law enforcement agencies.[77] Rosenstein stated that the DOJ is mindful of respondents' concerns with regard to multiple overlapping penalties when the DOJ pursues parallel enforcement actions with domestic enforcement agencies, and the DOJ was "considering proposals to improve coordination in those situations and to help avoid unwarranted payments."[78]

Following on these remarks, on May 9, 2018, Deputy Attorney General Rod Rosenstein announced a new non-binding DOJ policy regarding "Piling On"—the simultaneous imposition of multiple penalties for the same underlying misconduct by different regulatory or criminal authorities. Rosenstein explained, "our new policy discourages 'piling on' by instructing Department components to appropriately coordinate with one another and with other enforcement

75. If the SEC determines that there is no violation of U.S. securities law, but believes that there is a violation of another federal law or international law, they may refer the matter to another U.S. or foreign regulator for additional investigation.
76. *See* U.S. Dep't of Justice, *Coordination of Parallel Criminal, Civil, Regulatory, and Administrative Proceedings* (2012), **https://www.justice.gov/usam/organization-and-functions-manual-27-parallel-proceedings**.
77. Rod J. Rosenstein, Deputy Att'y Gen., U.S. Dep't of Justice, *Remarks at the Clearing House's 2017 Annual Conference* (Nov. 8, 2017), **https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-remarks-clearing-house-s-2017-annual**.
78. *Id.*

agencies in imposing multiple penalties on a company in relation to investigations of the same misconduct.[79] He further noted:

> In highly regulated industries, a company may be accountable to multiple regulatory bodies. That creates a risk of repeated punishments that may exceed what is necessary to rectify the harm and deter future violations.
>
> Sometimes government authorities coordinate well. They are force multipliers in their respective efforts to punish and deter fraud. They achieve efficiencies and limit unnecessary regulatory burdens.
>
> Other times, joint or parallel investigations by multiple agencies sound less like singing in harmony, and more like competing attempts to sing a solo.[80]

Of particular importance for multi-national corporations is the directive that DOJ attorneys should "coordinate with other federal, state, local, and foreign enforcement authorities seeking to resolve a case with a company for the same misconduct."[81] The DOJ will consider a number of factors when applying the policy, including the "egregiousness of the wrongdoing; statutory mandates regarding penalties; the risk of delay in finalizing a resolution; and the adequacy and timeliness of a company's disclosures and cooperation with the Department."[82] While the actual impact of the new policy has yet to be seen, members of the defense bar have already voiced their skepticism over whether the policy will result in a notable reduction in DOJ penalties. Where the policy may have the most significant impact is in cases where foreign entities are subject to enforcement actions in their home and other non-U.S. jurisdictions.

### (e) DOJ Charging Decisions

Potential resolutions can range from a decision not to charge a corporation to a guilty plea to felony charges. In a Non-Prosecution Agreement ("NPA"), in exchange for cooperation, the DOJ will agree not to prosecute the corporation. In a Deferred-Prosecution Agreement ("DPA"), criminal charges are filed along with an agreement to dismiss the charges within a specific time period if the defendant fulfills the DPA requirements. The DOJ generally requires an admission of wrongdoing to resolve an investigation of a corporation.

The Justice Manual directs prosecutors to consider a number of factors (the previously mentioned Filip Factors) in determining whether to bring charges, negotiate a plea agreement, or enter into some other form of settlement agreement, with cooperation being emphasized above the rest.

Since at least September 2015, when then-DAG Sally Yates issued a DOJ policy memorandum concerning individual accountability for corporate wrongdoing (the "Yates Memo"), the DOJ has focused on individuals' misconduct when resolving corporate enforcement matters." Under the Yates Memo, prosecutors cannot enter into a settlement agreement with a corporation without first preparing a written plan to investigate and prosecute

79. Rod J. Rosenstein, Deputy Att'y Gen., U.S. Dep't of Justice, *Remarks to the New York City Bar White Collar Crime Institute* (May 9, 2018), **https://www.justice.gov/opa/speech/deputy-attorney-general-rod-rosenstein-delivers-remarks-new-york-city-bar-white-collar.**
80. *Id.*
81. *Id.*
82. *Id.*

individuals. Prosecutors must alternatively prepare a written memorandum justifying a decision not to charge an individual and must obtain approval from a senior Department official.[83] In November 2018, the then-DAG delivered a speech revising the Yates memo's approach to individual accountability.[84] In particular, under the new policy, the DOJ announced that it would end the Yates Memo's "all or nothing" approach and permit corporations to receive credit for their cooperation if they identify individuals who were significantly involved in or caused the criminal conduct.[85]

## H. Information Gathering Phase: Conducting the Investigation

### 1. Planning the Endgame

Every internal investigation should begin with an end game—the ultimate objective—and a plan to get there along the most efficient path. Identifying a desired outcome (e.g., bringing authorities to accept that misconduct has not occurred where the facts support such a finding, or obtaining a negotiated settlement where misconduct is apparent early on) facilitates the process of anticipating potential issues. Corporations facing investigation must develop a single strategy that works across the various government agencies and jurisdictions at issue, since taking a materially different position in one jurisdiction can come back to be used against you by another authority.

### 2. Scope and Depth of the Investigatory Request

Corporate counsel should analyze the operative request (whether subpoena, document request, or informal request) to determine which entities, employees, and records may be relevant.

In the rush to get to the bottom of what has happened, it is all too easy for those conducting investigations to become beholden to a pre-determined process and to lose sight of what they set out to achieve. Setting and communicating clear objectives, as well as defining and continuously reviewing the scope and terms of the inquiry, are critical first steps towards achieving an appropriate and proportionate outcome.

A company can likely negotiate with the relevant authority regarding the scope of documents covered by the request and the production date in order to ensure the company and its advisors can undertake a proportionate and reasonable response.

A request with a long look-back period, or even without any time limit, could involve a time and resource-intensive review and production exercise.

### 3. Governing Structure

Another initial point of consideration is who will be responsible for leading the investigation: the board, management, or outside counsel.

In establishing a governance structure and reporting lines for the investigation, a company should consider:

83. Sally Quillian Yates, U.S. Dep't of Justice, *Individual Accountability for Corporate Wrongdoing* (Sept. 9, 2015), **https://www.justice.gov/archives/dag/file/769036/download**.
84. Rod J. Rosenstein, Deputy Att'y Gen., U.S. Dep't of Justice, *Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act* (Nov. 29, 2018), **https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0**.
85. *Id.*

Expectations of the relevant authority, who may take a skeptical view of management-led inquiries, rather than an investigation by outside counsel;

Who is known to be involved or potentially involved in the subject matter of the investigation and establishing reporting lines accordingly;

Attorney-client and work-product issues—the governance structure and reporting lines should be established so as to ensure maximum protection of potentially privileged materials.

### 4. Establishing an Investigation Plan

When a company first suspects wrongdoing, it should consider the type and scope of investigation necessary, in light of the severity of the potential violation. For example, internal reports of potential misconduct, whether to in-house counsel, human resources personnel, or employee supervisors, will require an assessment of whether the issue presents a violation of law or regulation, or merely a violation of company policy. Not all reports of misconduct within a company will necessitate an internal investigation conducted by outside counsel or the creation of a special investigative board committee. If the alleged misconduct involves an individual employee and does not implicate potential violations of law, in-house counsel, with support from appropriate business functions such as the internal audit department, can investigate the allegations and recommend appropriate remedial and personnel actions to management. Conversely, where the potential misconduct is widespread, may involve officers or directors, potentially violates the law affects corporate governance, or subjects the company to government investigation and enforcement actions, the company should utilize external counsel to lead the investigation.

At the outset of a U.S. investigation, a company should comprehensively consider, among other things: (1) potential and desired outcomes, (2) expectations of relevant agencies, and (3) structuring investigative processes to minimize risky and constraining decisions. It is critical for the company to develop and memorialize an action plan at the outset of the investigation that defines the parameters of the investigation. Broadly, the plan should aim to define:

1. The relevant time period to be investigated;
2. The geographic scope of the investigation;
3. Which entities of the company (e.g., subsidiaries, affiliates, or departments) will be covered, as well as an explanation of why particular entities are not included; and
4. The subject matter of the investigation.

Broadly, an investigation can be considered to have three overarching phases: (1) commencement, (2) information gathering, and (3) disposal.

During the commencement phase of an investigation, corporations should strive to understand the potential sources and triggers of an investigation, including internal reporting, external requests, or market awareness. Additionally, at the onset of an investigation, corporations should identify which government agencies might be involved and consider the respective agencies' expectations.

Next, during the information gathering phase, the target of an investigation should determine an optimal outcome and structure an investigation plan with that outcome in mind. Special consideration should be given to identifying potential sources of information, the scope of the inquiry, and issues concerning confidentiality and privileged communication.

Finally, in the disposal phase, corporations should carefully manage the outflow of information and ensure that all actions taken are directed at their desired outcome.

The disposal strategy should be tailored to the specific agency involved and also reflect cognizance of any potential collateral consequences.

Because the relevant authority may be interested in how the company has set the parameters of an internal investigation, the investigation plan should be drafted with the possibility of disclosure in mind.
When constructing the investigation plan, key considerations for information gathering include:

1. Documents—The investigation plan should set out what documents will be collected, how they will be processed, and who will be responsible for collection and processing.
2. Any concerns or considerations related to data privacy should also be addressed in the investigation plan.
3. Interviews—The investigation plan should list individuals that have been interviewed as part of a preliminary investigation or will be interviewed as part of a full investigation.
4. The plan should also provide a rationale for why it has been decided that certain individuals will not be interviewed.
5. Witness interviews may have various purposes, including: scoping the investigation, understanding the facts and issues at play, and assessing the accountability of individuals as well as possible defenses for the company and its employees.
6. Third Parties—The plan should describe whether the investigation will require consultation with or assistance from third parties such as forensic accountants, foreign counsel, or industry experts, as well as the scope of any such anticipated consultation.
7. Reporting—The plan should describe generally how the company intends to report its investigation findings and whether it will be necessary to issue an interim report.
8. Anticipated time frame for completion of the investigation.
9. Anticipated costs of the investigation.
10. Anticipated potential remediation.

During an investigation, a company may uncover evidence of a different but related category of misconduct. In these situations, the company should consider the potential scope of the issue as well as whether leniency may be available for the conduct.

Critically, once an investigation is ongoing, whether initiated by a government authority or an exchange, a respondent must ensure that all responses to information requests are complete and accurate.

A 2020 CFTC settlement, discussed above, clearly illustrates the risks of insufficient cooperation in an investigation of a respondent's market conduct. In 2018, a bank settled with the CFTC, agreeing to pay a penalty of $800,000 to resolve spoofing charges. The CFTC cited the bank's substantial cooperation with its investigation as a factor in agreeing to settle for the relatively small sum.[86] In 2020, the CFTC discovered that the bank's spoofing activities were broader than the Commission had originally understood and concluded that the bank had not been candid in response to the initial investigation.[87] The CFTC concluded that, among other things, the bank had failed to identify to investigators certain of its precious metals traders, certain accounts through which it traded precious metals futures contracts and certain COMEX user IDs that its traders used to trade precious metals.[88] The CFTC also found that the bank had made false statements to COMEX regarding the existence of a central repository of COMEX user IDs that its traders used, in addition to false statements to the National Futures Association concerning the bank's use of software to monitor manipulative or deceptive trading practices, including spoofing. The CFTC also described in its order the bank's failure to correct misleading statements made by its employees in sworn testimony.[89]

The subsequent investigation ended in a $127.4 million settlement with the CFTC resulting from the bank's failure to respond candidly in the prior investigation. $50 million of this penalty was attributable to the bank's compliance and supervision failures, as the bank did not have supervisory procedures for conducting required monitoring of traders or attesting that such monitoring had occurred.

Similarly, in a separate 2020 CFTC settlement, discussed above, the Commission faulted a different bank for failing to "respond to certain of the Division's requests for documents in a timely manner" and responding "incompletely or unsatisfactorily to certain of the Division's information requests in a manner that resulted in the Division being misled" and failing to "timely inform the Division of relevant information."[90]

Previously, in 2017, an investment bank entered into a $2.5 million settlement with the CFTC to resolve allegations that it violated the CEA by failing to supervise its employees and keep adequate records, discussed above.[91] From 2009 to 2010, the CME investigated whether traders at that bank executed U.S. Treasury Futures transactions on the CME before entering into block trades with these counterparties.[92] In November 2010, the CME interviewed certain traders about the suspected misconduct. The traders allegedly provided "misleading answers" to the CME by suggesting that the trades were unrelated to the block trades or that

86. CFTC No. 18-50 (Sept. 28, 2018).
87. CFTC No. 20-28 (Aug. 19, 2020).
88. *Id.* at 3.
89. CFTC No. 20-26 (Aug. 19, 2020).
90. CFTC No. 20-69 (Sept. 29, 2020).
91. CFTC No. 17-25 (Sept. 22, 2017).
92. *Id.* at 2.

the trades actually occurred after the block trades and that the reported execution times for the block trades were inaccurate.[93] The traders also claimed that it would have been impossible for them to trade ahead of a counterparty's block trade because the time between receiving the customer's block trade inquiry and executing the block trade was very brief.[94] However, according to the CFTC's Order of Settlement, the traders "did in fact trade futures contracts" in this way and engaged in other questionable conduct such as eavesdropping on calls between counterparties and salespersons about block futures trades without announcing their presence and then using the information learned to hedge expected risk from those block trades.[95]

The CFTC alleged that the bank violated CFTC Regulation 166.3, which requires entities registered with the CFTC to "diligently supervise the handling by its partners, officers, employees and agents" of "all commodity interest accounts . . . relating to its business as a Commission registrant."[96] Typically, the CFTC brings Regulation 166.3 claims against firms who failed to prevent their employees from committing misconduct (such as manipulative trading practices). However, here the CFTC took an expansive and unprecedented approach in applying this provision to find the bank liable for its inadequate response to the CME investigation.

According to the CFTC, the bank failed to adequately supervise its employees and agents entrusted with investigating the CME's claims of trading ahead on block trades. Although the compliance and legal departments were primarily responsible for responding to the inquiry, they relied on the bank's operations support group to gather information for the bank's response and provided only "minimal oversight."

This lack of oversight allegedly led to certain material omissions and misstatements. For example, the CFTC alleged that the operations support group provided only an "abridged version" of relevant trading activity to the legal and compliance departments that failed to disclose "a number of occasions" where certain traders traded futures contracts in the five minutes before the execution time of block trades. Rather, in responding to the CME's inquiries, the business unit generated an internal spreadsheet identifying several potential instances of "pre-hedging" but did not share it with legal and compliance personnel. Overall, the CME found that the bank's "failure to stay adequately informed" regarding the activities of the operations support group contributed to its failure to detect the improper trading activity before the traders misled the CME during the interviews.[97]

## 5. Information Preservation, Retrieval, and Review

### (a) Information Preservation

As soon as it becomes apparent that an investigation will be necessary, the company should distribute a litigation hold to prevent the intentional or accidental destruction of relevant documents and information. Failure to do so could be eventually viewed as an obstruction of justice.

93. *Id.* at 2–3.
94. *Id.*
95. *Id.*
96. *Id.* at 6 (quoting 17 C.F.R. § 166.3 (1983)).
97. *Id.*

Necessary steps to issuing a litigation hold include:

1. Determining the scope of documents that will be subject to the hold;
2. Determining who should receive the hold notices, which may include both individual employees and the IT or records department of a particular entity;
3. Collaborating with IT/records departments to suspend normal document destruction practices, identify the location of stored data/information, and implement proactive data-capturing measures such as forensic imaging of employee computers and other electronic devices;
4. Considering the need for translations of the hold; and
5. Considering whether data privacy laws/restrictions are implicated.

**(b) Information Collection/Retrieval**

With document preservation measures in place, the investigators should work to collect documents within the scope of the investigation plan.

Investigators should anticipate whether there will be barriers to document collection, which may include:

1. Local employment laws;
2. Company policies or codes of conduct;
3. The need to collect documents in the possession of third parties;
4. Data privacy laws (particularly in cases involving documents located outside the United States).

**(c) Collection of Electronic Data**

Collection will ordinarily require making forensic copies of files identified as containing potentially relevant data and maintaining backups. In addition to electronic files, it is also important to preserve and collect the underlying metadata contained in those files. Often, the process of collecting, processing, and hosting electronic materials is performed by a third-party data vendor. Even when such steps are performed by a vendor, the document collection process should be documented by the investigation team.

**(d) Document Review**

When the collection stage results in a large volume of documents for review, it is important to adopt methods of efficiently identifying relevant documents.

**(1) Search Terms**

Search terms should be applied in a way that is sufficiently broad to capture responsive documents, but narrow enough to eliminate documents that do not require examination by the review team.

**(2) Predictive Coding**

Predictive coding is a developing review tool that can significantly reduce the number of documents that need to be manually reviewed. The company should consider the view of the relevant agency on whether and when the use of predictive coding is acceptable.

#### (3) Manual Review

After potentially reducing the universe of relevant documents through search terms and predictive coding, it is usually necessary to have a human review team tag and code the potentially responsive documents.

A tagging or coding system should be developed that allows for efficient organization and identification of documents.

The review team should be provided with a detailed review protocol explaining the purpose of the review, how to identify responsive documents, and how to appropriately apply tags and codes.

As the review stage proceeds, information learned may lead to an expansion of the investigation's scope, either with respect to subject matter or the individuals involved.

## 6. Protecting Privilege During the Investigation

### (a) Types of Privilege

#### (1) Attorney-client Privilege

Under U.S. law, the attorney-client privilege protects a confidential communication made between an attorney (or agent) and a client for the purpose of seeking, obtaining, or providing legal assistance to the client. Courts tend to construe the privilege narrowly because the privilege exists in derogation of the principle that the public has a right to access evidence that supports or refutes a claim pending in a public legal proceeding.[98] The attorney-client privilege applies if: (1) a person asserting the privilege is or sought to become a client; (2) a person to whom communication was made is an attorney (or certain agents of an attorney) acting in his or her legal capacity; (3) the statement was made in confidence, outside the presence of any third party, for the purpose of securing legal advice, legal services, or assistance in some legal proceeding; and (4) the privilege has been claimed and not waived by the client.[99]

#### (2) Attorney Work Product

A corollary to the attorney-client privilege, the "attorney work-product" doctrine protects from discovery materials prepared by lawyers in anticipation of litigation. The attorney work-product doctrine protects the mental processes of the attorney through which an attorney can recognize and prepare a client's case.[100] Recognizing that such preparation may require the assistance of non-lawyers, the work-product doctrine also shields any materials prepared by agents of the attorney, if prepared at the direction of counsel.[101] Thus, the attorney work-product doctrine protects interviews, statements, memoranda, correspondence, briefs, mental impressions, personal beliefs, and other tangible and intangible information gathered in anticipation of litigation.[102] Any memoranda or work prepared by the attorney or at the direction of counsel should be labeled as attorney

98. *See In re Grand Jury Proceedings,* 219 F.3d 175, 182 (2d Cir. 2000).
99. *See Wultz v. Bank of China*, 979 F. Supp. 2d 479 (S.D.N.Y. 2013) (citing *Colton v. United States*, 306 F.2d 633, 637 (2d Cir. 1962)).
100. *See United States v. Nobles*, 422 U.S. 225, 238 (1975).
101. *See id*. at 239-40.
102. *See Hickman v. Taylor*, 329 U.S. 495, 514-15 (1947) (Jackson, J., concurring).

work product. The labeling alone, however, will not be a decisive factor in determining whether the privilege applies, especially if the advice is business rather than legal in nature. The purpose of the attorney work-product doctrine, similar to that of the related attorney-client privilege, is to ensure proper functioning of the justice system.[103] It reflects a public policy that prosecution and defense of legal claims deserves the protection of privacy without interference from discovery.[104]

**(3) Common Interest/Joint Defense**

While disclosure of privileged information to a third party would typically result in a waiver of the privilege, the common interest doctrine allows for sharing of privileged information under certain circumstances. Independent entities engaged in a joint defense effort can share confidential information if the communications were made in the course of the joint defense effort, were designed to further the effort, and the privilege was not otherwise waived.

**(b) Maintaining Privilege**

**(1) Corporate Setting**

Corporations are entitled to the protections of the attorney-client privilege.[105] As a practical matter, however, a corporation can speak only through its employees. Several criteria apply to determine when a statement made by one of these employees will be entitled to the corporation's privilege protection. In general, the corporate privilege applies only if: (1) the person making the communication is an employee, (2) the communication is made at the direction of a corporate superior for the purposes of seeking legal advice, and (3) the communication is within the scope of the employee's duties.[106]

This does not mean, however, that there is a blanket privilege for communications with in-house or even external counsel, even where the communication falls within the scope of the employee's duties. Privilege law recognizes that attorneys, particularly in smaller organizations, may serve business functions. As a result, a communication will not be considered privileged simply because one of the recipients (or senders) is a lawyer. Merely copying a lawyer on a communication will not protect the communication from disclosure.

Rather, courts will carefully consider whether the communication with the corporation's in-house or outside counsel was made for the purpose of securing legal advice.[107] Where communications from in-house counsel contain both business and legal advice, courts will generally make an inquiry into the "primary purpose" of the document in order to determine if

103. *See id.* at 238.
104. *See id.*; *see also Hickman*, 329 U.S. at 514-15 (1947) (Jackson, J., concurring) ("Historically, a lawyer is an officer of the court and is bound to work for the advancement of justice while faithfully protecting the rightful interests of his clients. In performing his various duties, however, it is essential that a lawyer work with a certain degree of privacy, free from unnecessary intrusion by opposing parties and their counsel. Proper preparation of a client's case demands that he assemble information, sift what he considers to be the relevant from the irrelevant facts, prepare his legal theories and plan his strategy without undue and needless interference. That is the historical and the necessary way in which lawyers act within the framework of our system of jurisprudence to promote justice and to protect their clients' interests.")
105. *See Upjohn Co. v. United States*, 449 U.S. 383, 390 (1981) (citing *United States v. Louisville & Nashville R. Co*., 236 U.S. 318, 336 (1915)).
106. *See id*. at 394.
107. *See id.*

the privilege applies.[108] The court will deem the communication protected by the attorney-client privilege upon a finding that the "primary purpose" of the communication is legal; in other words, that the purpose of the communication is "to discern the legal ramifications of a potential course of action."[109]

**(2) Employee Interviews**

Interviews are typically conducted by an attorney, with another attorney taking written notes of the interview, including their thoughts and mental impressions. This method, rather than a "purely factual" verbatim transcript, makes the record of the meeting more likely to be protected under the attorney work product doctrine. Interviews may still be privileged if conducted by non-lawyers at the direction of an attorney.

Counsel will need to consider use of *Upjohn* warnings. Under the U.S. Supreme Court case of *Upjohn Co. v. United States*, the attorney-client privilege covers communications between company counsel and employees under certain circumstances. At the beginning of an interview, employees should be given an "*Upjohn* warning," explaining that the communications between employees and legal counsel are privileged and confidential, but that the privilege belongs to the company, which may choose to waive the privilege in the future. The *Upjohn* warning should clarify that the lawyer represents the company and not the employee. It is paramount for counsel to advise employees at the start of the interview that they represent the company and that the privilege and the right to waive it belong to the company alone. Otherwise, successful claim to the privilege by an employee can lead to suppression of information, hampering the company's efforts to cooperate with the government during an investigation.

Communications with employees will be privileged if (1) the communications were made by the employees at the direction of management for the purpose of obtaining legal advice; (2) the information sought from the employee was necessary to providing legal advice and was not otherwise available to the management "control group" (i.e., the holders of the privilege); (3) the matters communicated were within the scope of the employee's corporate duties; (4) the employee knows the communications are for the purpose of obtaining legal advice; and (5) the communications are kept confidential.[110]

Interviews of former employees may also be privileged, but the subject matter of the interview should be limited to the period of the former employee's tenure at the company. The investigation team should also consider whether the former employee can be relied upon to cooperate or maintain the confidentiality of the interview.

---

108. *See Phillips v. C.R. Bard, Inc.*, 290 F.R.D. 615, 628 (D. Nev. 2013).
109. *See id*. (quoting *Henderson Apartment Venture, LLC v. Miller,* No. 2:09-cv-01849-HDM-PAL, 2011 WL 1300143, at *9 (D. Nev. Mar. 31, 2011); *Premier Digital Access, Inc., v. Central Telephone Co*., 360 F. Supp. 2d 1168 (D. Nev. 2005)).
110. *See Upjohn*, 449 U.S. at 383.

**(3) Legal Advice**

The company should meticulously document the nature of the investigation as being for the purpose of obtaining legal advice, rather than for some business purpose.

Communications with the company should be labeled "attorney-client privilege" and the content of such communications should in fact relate to legal advice, rather than business advice.

**(c) Waiving privilege**

Disclosure of privileged communications or information to a third party may constitute a waiver of the privilege. In addition to the particular communication, the disclosure may waive the privilege with respect to other communications relating to the same subject matter.[111]

For the purposes of obtaining cooperation credit, it may not be necessary to waive the attorney-client privilege, if the company can disclose all relevant facts without doing so. In fact, DOJ policy forbids prosecutors from conditioning cooperation credit on a waiver of privilege.

A disclosure of privileged information could potentially avoid being deemed a waiver of the privilege if:

1. The disclosure was inadvertent;
2. The holder of the privilege took reasonable steps to prevent disclosure; and
3. The holder promptly took reasonable steps to rectify the error.[112]

In-house counsel should be careful to involve only third parties who are essential to the communication in order to avoid the risk of being deemed to have waived the privilege. For example, in *Allied Irish Banks, P.L.C. v. Bank of America*, the court found that no privilege applied to communications where in-house counsel had included non-lawyer third parties who had no "need to know" about the content of the communications.[113] The same court also found the privilege applied to one communication where the company showed that the recipients had a reason to participate and were acting for the company.[114]

There are ways of limiting disclosure risk; in In re *Gen. Motors LLC Ignition Switch Litig.*, a case that actually distinguishes itself from *Allied Irish Banks*, the attorney-client privilege and attorney work product privileges were upheld in spite of the fact that a report of an internal investigation was widely and publicly distributed.[115] There, because the investigation and report were prepared by external counsel specifically retained to provide legal advice, the court upheld the privilege in connection with key interview materials "reflecting communications between current and former [client] employees and agents and outside counsel."[116]

111. Fed. R. Evid. 502(a).
112. Fed. R. Evid. 502(b).
113. *See Allied Ir. Banks, P.L.C. v. Bank of Am., N.A.*, 252 F.R.D. 163, 170 (S.D.N.Y. 2008).
114. *Id.*
115. *In re Gen. Motors LLC Ignition Switch Litig.*, 80 F.Supp.3d 521, 530-531 (S.D.N.Y. 2015).
116. *Id.* at 531.

*In re Kellogg Brown & Root, Inc.* is instructive on steps counsel should take to protect internal investigative efforts.[117] There, Kellogg, Brown & Root (KBR) sought mandamus twice after the district court overseeing the case found the defense contractor had waived its privilege. In the first mandamus action, KBR challenged the district court's decision that it had waived attorney-client privilege concerning certain documents; the DC Circuit "granted the writ and vacated the District Court's order to produce a key document" but allowed the district court to consider other arguments for disclosure.[118] On remand, the district court again ordered disclosure. KBR then sought mandamus a second time, and the DC Circuit again granted the writ and vacated the orders. A single writ of mandamus is unusual, but two is very rare—evidencing the importance placed on the privilege within the DC Circuit.

At issue in the case was whether an internal investigation, and its materials, would have to be disclosed. In the first mandamus action, the district court incorrectly applied the primary purpose test, requiring a "but for" analysis of the materials generated in the litigation (i.e., but for the legal advice sought, the investigation would not have been undertaken). In the second application for the writ, the district court's findings that (1) documents needed to be produced pursuant to Fed. R. Evid. 612 and (2) had been put "at issue" and therefore waived were also rejected by the Circuit. The DC Circuit reasoned: "If all it took to defeat the privilege and protection attaching to an internal investigation was to notice a deposition regarding the investigations (and the privilege and protection attaching them), we would expect to see such attempts to end-run these barriers to discovery in every lawsuit in which a prior internal investigation was conducted relating to the claims."[119]

## 7. Investigation of Individual Employees

### (a) Employee cooperation

U.S. employers may, as a matter of policy, require employees to cooperate with any internal investigation and to provide information to company counsel, and can terminate employees for failure to cooperate. U.S. courts generally uphold such policies against a wrongful termination claim, absent evidence that the policy is applied in bad faith or in a discriminatory fashion.

### (b) When to Obtain Separate Counsel for an Employee

Employees in the U.S. are free to obtain independent legal advice in the face of a potential interview with the company's counsel.

Depending on the situation, companies may provide legal representation for employees to ensure they have fully considered their legal exposure and are well-prepared for interviews.

An employee who is a current or likely subject, target, or material witness should be advised to retain separate counsel prior to the employee providing substantive information to the company's counsel.

117. *In re Kellogg Brown & Root, Inc.*, 796 F.3d 137 (D.C. Cir. 2015), *cert. denied*, 136 S.Ct. 823 (2016).
118. *Id.* at 140.
119. *Id.* at 151.

A company may be required to advance legal fees and expenses to certain of its employees depending on the laws in a company's state of incorporation and its own by-laws or internal policies.

**(c) Disciplinary Considerations**

**(1) Disciplinary Hearings**

A disciplinary procedure and any disciplinary decision must be procedurally and substantively fair. Any contractually-mandated procedure should be followed unless the parties agree to modifications.

Employees have the right to be accompanied by counsel, the right to be notified of maximum sanctions, and the right to appeal.

**(2) Reassigning, Suspending, or Terminating an Individual**

If a fair disciplinary process is followed and the employer reasonably decides that the employee is guilty of misconduct, the employer will need to apply a sanction. Sanctions may include termination, demotion, remuneration decisions, warning, and/or compliance training.

If termination does not occur, the employer should actively monitor the employee to ensure no further wrongdoing occurs and to safeguard the employer from retaliation actions.

Where employees are terminated for cause resulting from an unfair, incomplete or inaccurate investigation, they may be able to bring wrongful dismissal claims in court.

## I. Managing Stakeholders

Companies should be proactive in evaluating their crisis management infrastructure to ensure that they are prepared to move quickly at the first sign of trouble. This includes establishing reporting lines and procedures that can be implemented when a crisis arises.

### 1. Developing a Global Corporate Communications Strategy

Even before the facts are fully developed, the company may face pressure to disclose information regarding the crisis to senior management, regulators/prosecutors, the media, and/or investors. The company must develop a clear communications strategy for such internal and external communications so that it conveys a consistent message to its various constituencies. It is important that management (or anyone speaking on behalf of the company) resists the impulse to issue premature denials or apologies before the facts are fully developed and be sensitive to the risk that any inartful comments about the conduct at issue may be used by regulators in the investigative proceedings. Most large corporations have sophisticated in-house communications professionals to handle these issues.

### 2. The Role of Outside Counsel

Outside counsel is likely to be more familiar with the full array of facts developing in the various spokes of the investigation and thus to be more sensitive to risk areas. Further, outside counsel is likely to be more attuned to public comments that may provoke a negative reaction from regulators. In certain circumstances, counsel will work with regulators to preview public statements.

### 3. Managing Stakeholders Within the Company: Senior Management

Depending on the scope of potential misconduct under investigation, it may be necessary to provide periodic board updates. In such a circumstance, these periodic updates should provide sufficient detail for the board to assess the progress of the investigation and management's response to it.

Depending again on the scope of potential misconduct under investigation, it may also be necessary to involve senior management in the investigation. In such a circumstance, senior management should be informed of whatever facts are needed to run the company. Senior management will be helpful in developing strategy, marshalling resources, and ultimately deciding what the company should do with the results of the investigation. In the event the investigation involves members of senior management, counsel should revise its communications so as to preserve the integrity of the investigation.

### 4. Managing Stakeholders Within the Company: Employees

Rumors of an investigation can cause significant problems that complicate the investigation.

Facts about the investigation must be narrowly disseminated only to employees who have a need to know. Natural curiosity about an investigation can cause otherwise irrelevant witnesses to become part of the investigation and lead to examination and scrutiny from regulators. Further, counsel should be careful in conducting interviews with fact witnesses to protect the confidentiality of the investigation and to avoid contaminating witnesses. For example, in most circumstances, interviewees should not be shown communications that they were not party to or otherwise previously saw in the normal course of business.

Unsupervised communications among employees can lead to a waiver of attorney-client privilege. All employees who know of the investigation should be instructed to treat it as confidential and not to discuss it with anyone other than counsel (or at counsel's direction). Thereafter, it is important to remind employees to preserve the confidentiality of regulatory investigations and to avoid gossip.

## J. Resolution Phase: Disclosure and Information-Sharing with Agency Investigators

From the beginning of the investigation, or even earlier, it is almost always desirable to maintain a continuous dialogue with officials. Proactive communication will often lead to a better working environment once the investigation reaches the resolution phase.

A good working relationship with agencies will involve clear communication. It should be made clear when a statement is being made on behalf of the company, and communications should always be made in clear, complete, and accurate language.

The company's point of contact, whether it is the investigating board committee, an in-house lawyer, or external counsel, should communicate with the government about the scope of the investigation and schedule a regular dialogue to keep the government apprised of the investigation's progress.

### 1. Managing Communications with Government Authorities

Any response to a governmental inquiry, whether voluntary or by subpoena, must be complete, accurate, and as timely as possible. Unless warranted by a deliberate strategy, counsel should foster a reasonable working relationship with their counterpart at the regulator.

The company must also be careful to take a consistent approach to communications with all of the government actors involved in the investigation. The company should generally assume that separate government entities are communicating with each other and sharing information. However, the company must be careful to share information equally among investigators or risk impairing its relationship with those left out. In so doing, however, the company must also be sensitive to any confidentiality requests from individual officials.

The company must assume that regulators and prosecutors are reviewing all of its public statements. Regulators will be particularly sensitive to any public comments from the company seeming to minimize the importance of the investigation or being unduly optimistic.

### 2. Reporting

Ultimately, the results of an internal investigation should be compiled into some form of report that can be presented to the company's leadership, and, if needed, to the authorities. Beyond the raw factual information uncovered by the investigation, there are a number of components that may be included in an investigation report, including:

1. Background information on the circumstances leading up to the investigation;
2. A description of the investigation's scope and the steps taken to collect relevant information; and
3. Conclusions and analysis based on the facts discovered.

Even though the findings of an internal investigation may reveal misconduct or other unfavorable facts, a written report is an opportunity to contextualize the conduct and present the underlying facts in a manner more favorable to the company.

## K. Resolution Phase: Outcomes

### 1. Identifying the Desired Achievable Outcome

It is important to re-evaluate the investigation's optimal achievable outcome throughout the investigation as facts develop. Moreover, in addition to assessing what an optimal achievable outcome is, companies should also evaluate the best strategies to achieve those outcomes. Factors such as credibility before the investigating body and a cooperative approach to the investigation can be significant in negotiating a favorable settlement. If multiple governmental entities are investigating a company, a settlement negotiation with all relevant parties at the table typically yields the best result, as opposed to negotiating individually with each governmental entity.

Most investigations that result in penalties are resolved through a negotiated settlement with a U.S. authority. Nevertheless, a company can adjudicate the issues being investigated where circumstances call for it.

Trial is rare, but companies can refuse to cooperate with a government investigation and instead try to contest the charges on the merits.

## 2. CFTC, SEC, and DOJ Resolution Tools

### (a) CFTC

The CFTC can administer civil penalties in settlement orders, which must be approved by the CFTC's Commission. These settlement orders will include certain findings of fact and conclusions of law, which will serve as the basis for a cease-and-desist order and a penalty.[120] Although the CFTC does not itself bring criminal charges against entities or individuals, it can refer criminal violations of the Commodity Exchange Act to the DOJ for prosecution. Civil penalties can include disgorgement of ill-gotten gains and restitution to victims. The CFTC can also require special supervision, suspend business registrations, and even bar an entity or individual from working in an industry altogether. This is an important consideration for entities registered with (or that plan to register with) the CFTC—the CEA permits the CFTC to refuse or revoke registration for entities that have committed certain violations of the Act.[121] The CFTC recently extended this statutory disqualification to exempt commodity pool operators, suggesting the Commission may expand its use of this penalty moving forward.

The CFTC may also utilize non-prosecution agreements ("NPAs") or deferred prosecution agreements ("DPAs") to resolve enforcement actions.

### (b) SEC

Like the CFTC, the SEC can administer civil penalties in settlement orders, and like the CFTC, such settlement orders must be approved by the SEC's Commission. The SEC can also refer criminal violations to the DOJ for prosecution. Typically, companies will begin settlement discussions with the SEC at or around the time that a Wells Notice is issued. Typically, an SEC settlement will include certain findings of facts and conclusions of law, which serve as the basis for a cease and desist order and a civil monetary penalty. If the matter does not settle, the SEC can bring a civil enforcement action against the company. The SEC can either bring an enforcement action in federal court or as an administrative proceeding. In federal court, the SEC may seek injunctive relief. In either an administrative or federal court proceeding, the SEC can issue cease and desist orders, suspension or revocation of broker-dealer and investment advisor registrations, censures, bars from association with the securities industry, civil monetary penalties, and disgorgement of profits.[122]

---

120. A cease-and-desist order is an order directing a company to stop engaging in conduct that violates the law.
121. *See* 7 U.S.C. § 12a(2).
122. On June 22, 2020, the U.S. Supreme Court placed significant limits on the ability of the SEC to maintain its longstanding practice of seeking disgorgement awards as part of an enforcement action in federal court for violation of the federal securities laws. Unlike the express statutory authorization for disgorgement in administrative proceedings, the SEC relies on its right to seek equitable remedies in pursuing disgorgement as a remedy in civil enforcement actions in federal court. In *Liu v. Securities and Exchange Commission*, the Supreme Court held that the SEC may continue to obtain disgorgement awards in civil enforcement actions, as long as those awards do not exceed the defendant's net profits from the violation at issue and are awarded to victims of the violation. 140 S. Ct. 1936 (2020). Prior to that decision, in 2017, the Supreme Court ruled that the disgorgement remedy constituted a "penalty" for purposes of 28 U.S.C. § 2462, and, therefore, was subject to a 5-year statute of limitations. *Kokesh v. SEC*, 137 S. Ct. 1635 (2017).

**(c) DOJ**

Most DOJ enforcement actions are settled before trial, either in NPAs or DPAs. In recent years, the DOJ has intensified its enforcement endeavors, many times requiring corporations to plead guilty before agreeing to settle their claims. Given this new, increasingly hostile environment, the level of cooperation with the government remains a key factor to the ultimate settlement outcome.

### 3. Considering Collateral Consequences

While consequences such as the loss of the ability to conduct certain business can apply in many types of inquiries, the risks are greater when facing a criminal investigation.

If a guilty plea would have significant adverse consequences for innocent third parties, the DOJ is more likely to consider an NPA or DPA than a felony guilty plea. However, the existence of potential collateral consequences will not necessarily lead the DOJ away from demanding a guilty plea for the conduct under investigation.

Regardless, an admission of wrongdoing through any settlement mechanism can have substantial negative consequences for a business's future activities. The nature of those consequences can depend on determinations made by other regulators in a given industry. In a negotiated settlement, authorities may waive such consequences or agree to reinstate the applicable memberships and authorizations.

Settlement agreements may contain admissions that can be used in follow-on civil litigation or in future criminal enforcement actions.

## L. Ethical Issues in Internal Investigations and the Attorney-Client Privilege

Multinational corporations, including those who participate in the securities and commodities markets, continue to be subjects of large-scale, high-profile, cross-border investigations. With increasing cooperation among local and international regulators, growth in real-time media coverage, and advances in technology, this trend is unlikely to abate any time soon.[123] Counsel representing corporations in these investigations must consider how cross-border considerations impact already complex ethical and tactical issues relating to the attorney-client privilege and discovery, and as discussed further below, be prepared to persistently defend the privileges at home and abroad. Evaluating and protecting the privilege, at every stage of an investigation, is now a practical reality for attorneys involved in these types of multifaceted investigations.

The attorney-client privilege and the related attorney work-product doctrine are long-standing hallmarks of the U.S. legal system. Maintaining and protecting legal privilege in cross-border investigations, however, can be particularly challenging, in part because many jurisdictions offer far less privilege protection than in the United States or do not recognize privilege at all. The privilege also may be jeopardized during the course of a government or internal investigation, especially in the context of voluntary disclosures. Voluntary disclosures to the government, incentivized by the offer of

123. *See e.g., Press Release,* Dec. 21, 2016, **https://www.justice.gov/opa/pr/odebrecht-and-braskem-plead-guilty-and-agree-pay-least-35-billion-global-penalties-resolve**. The U.S., Brazil, and Switzerland jointly settled an investigation into two Brazilian companies, which involved "a massive and unparalleled bribery and bid rigging scheme," for $3.5 billion in penalties, illustrating the increasingly global nature of many internal investigations and potential ramifications of the same.

cooperation credit for disclosure of misconduct, directly implicate the issues of privilege and waiver.

An additional consideration relevant to defendants in the age of social media is the extent to which information shared with public relations firms or specialists is protected by the privilege. Increasingly, courts appear unwilling to extend the privilege to such individuals or entities, finding that "a media campaign is not a litigation strategy."[124] In the limited circumstances where the privilege is upheld in connection with public relations efforts, it is construed narrowly. To be protected, the communications must be "(1) confidential communications (2) between lawyers and public relations consultants (3) hired by the lawyers to assist them in dealing with the media… (4) that are made for the purpose of giving or receiving advice (5) directed at handling the client's legal problems . . ."[125] Accordingly, before retaining and communicating with public relations personnel, clients should consult with their legal counsel to determine what information to share and how to utilize the consultants within the scope of the privilege.

Another exception to the general rule on waiver of privilege is the inadvertent production doctrine that applies where reasonable precautions were taken to protect the privilege, but information was nonetheless produced. Finally, as discussed below, the privilege may be preserved as to other parties where disclosures are made to government regulators pursuant to a negotiated confidentiality agreement.

### 1. Privilege in the Corporate Setting

Ethical issues arise where counsel represents the company but engages, as counsel must, with company employees in the course of the investigation. As a general proposition, the privilege belongs to the corporation, not the individual employee communicating with the attorney. This means that the company holds the right to decide whether or not to waive the privilege and, relatedly, to disclose information received from that employee to regulators. The company ultimately may decide to share that information with the government, leading to criminal prosecution or civil penalties for the employee—a risk that may not be clear to the interviewee who does not appreciate that counsel's role is not to protect the employee's interests.

As a result, company counsel must provide employees with so-called "*Upjohn* warnings" when conducting investigatory interviews. As explained above, these warnings are derived from the seminal Supreme Court opinion in *Upjohn Co. v. United States*, which held that communications between corporate counsel and corporate employees are protected by the attorney-client privilege[126] *Upjohn* warnings notify employee witnesses that the company holds the attorney-client privilege and maintains the option to claim it or waive it, at its discretion, in case of disclosure to regulators. As part of these warnings, company counsel must make it clear to the employee that the company may, in fact, disclose the information obtained to regulators. Relatedly, counsel should also explain to the employee that the employee may be subject to obstruction of justice charges if he or she makes misleading statements in the interview that are relayed to the government.

124. *See Chevron Corp. v. Donziger*, No. 11 Civ. 0691, 2013 WL 3805140 (S.D.N.Y. Jul. 19, 2013), *quoting Haugh v. Schroeder Inv. Mgmt. N. Am. Inc.*, No. 02 Civ. 7955, 2003 WL 21998674, at * 3 (S.D.N.Y. Aug. 25, 2003); *see also Waters v. Drake*, No. 2:14-cv-1704, 2015 WL 8281858 (S.D. Ohio Dec. 8, 2015) (In employment discrimination matter involving the discharge of the Ohio State University's marching band director, the court found that the privilege did not attach to documents shared with a public relations firm. The documents were ultimately not produced, however, because they were found not relevant.).

125. *In re Grand Jury Subpoenas Dated March 24, 2003 Directed to (A) Grand Jury Witness Firm and (B) Grand Jury Witness*, 265 F.Supp.2d 321, 331 (S.D.N.Y. 2003) (public relations consultant and firm employed by target of the grand jury to influence prosecutors' perceptions sought to shield communications from disclosure based upon the privilege).

126. 449 U.S. 383 (1981).

Failure to adequately explain these points to employees may jeopardize the company's ability to disclose this information down the road, and may also disqualify counsel. In some instances, courts have recognized a personal privilege with respect to conversations between employees and corporate counsel, despite the fact that the privilege belongs to the company.[127] Although the employee bears a high burden in showing that an attorney-client relationship existed between the employee and counsel and that it concerned "personal matters,"[128] companies should still be aware that employees may prevail on such claims.

Courts have suppressed information where they recognize such a dual privilege. For example, in *United States v. Nicholas*, the court suppressed statements made by the company's chief financial officer (CFO) to outside counsel because counsel had failed to make it clear that he did not represent the CFO personally.[129] The CFO was jointly represented by company counsel in an unrelated civil matter and the CFO claimed that he had a continuing attorney-client relationship with counsel. The notes taken at the time the statements at issue were made also did not reflect that the *Upjohn* warnings were given and the CFO did not recall hearing them. The court found that if any warnings were given, those warnings were inadequate and that outside counsel had a "clear conflict" because of the joint representation of the CFO and the company in another matter. The court ordered suppression of any disclosed information, holding that the CFO held the privilege and the disclosure by company counsel violated the duty owed to him.[130] The court also referred the counsel to the State Bar for appropriate discipline.[131]

U.S. counsel should also be aware that foreign counsel may be unfamiliar with *Upjohn* warnings. Therefore, it is important to ensure that *Upjohn* warnings are given, even if the employee interviews are not conducted in the United States. Counsel must also avoid any inclination to soften or water down the warning because of concerns that such warnings will have a chilling effect on interviewees. Note that issuing *Upjohn* warnings and memorializing them in interview notes may not be sufficient to preserve privilege in cross-border investigations. In order to preserve U.S. privilege, it may therefore be necessary for the company to demonstrate the efforts it has taken to protect privilege. In any event, in addition to giving *Upjohn* warnings, companies should engage local counsel in the foreign jurisdiction to advise and ensure that proper protocols are followed to protect privilege.

*Upjohn* warnings protect the company in the event that employees may become targets of the investigation. Company counsel must be sensitive to the fact that an employee's status as a witness or a target may shift as the facts are developed in the course of the investigation, giving rise to a conflict between counsel's corporate client and the individual. This presents a potential conflict of interest as employees who are targets or subjects of an investigation likely have interests that are adverse to that of the company. *Upjohn* warnings are intended to address a

127. *See United States v. Int'l Brotherhood of Teamsters*, 119 F.3d 210, 215 (2d. Cir. 1997).
128. *See id.* at 214-216.
129. 606 F. Supp. 2d 1109 (C.D. Cal. 2009).
130. *See id.* at 1120.
131. *Id.* at 1121. The suppression of evidence in *Nicholas* was reversed on appeal. The Ninth Circuit held that the lower court applied the state law standard for determining whether there was a privileged relationship between the company counsel and the CFO where it should have applied federal common law. Under federal common law, the CFO failed to meet the burden of showing an attorney-client relationship existed. However, the Ninth Circuit did not reverse the lower court's ruling that the counsel violated state ethical rules by jointly representing the CFO and the company without obtaining a waiver. *See United States v. Ruehle*, 583 F.3d 600, 613 (9th Cir. 2009). Thus, where there is a potential conflict of interest with interviewed employees, company counsel should advise the employee to retain separate counsel, or, at a minimum, obtain a written conflict waiver.

potential conflict between the company and the employee, namely, that company counsel represents the company and not the individual employee. Such warnings are essential to maintaining the separation of representation between the company and employees; they also help prevent employees from trying to usurp the company's privilege by putting employees on notice that it is the company, and not the employee, that holds the privilege.

In *United States v. Wells Fargo Bank, N.A.*, a former vice president of Wells Fargo sought to assert an advice of counsel defense in connection with a civil action that alleged "Wells Fargo [and the defendant]…engaged in misconduct with respect to residential mortgage loans insured by the Government."[132] The advice on which the defendant sought to rely, however, was that of Wells Fargo's counsel. At issue was whether the attorney client privilege, held by Wells Fargo, could be relied upon by the employee-defendant and effectively waived by him in the course of his defense. Ultimately, the court ruled that "[h]olding that [the employee—who, indisputably, lacks authority to waive the privilege on behalf of Wells Fargo—can force disclosure of the Bank's privileged information, even if only for the purpose of using it to defend against the Government's claims, would essentially transform a corporate entity's attorney-client privilege into a qualified privilege."

In short, it is paramount for counsel to advise employees at the start of the interview that they represent the company and that the privilege and the right to waive it belong to the company alone. Otherwise, successful claim to the privilege by an employee can lead to suppression of information, hampering the company's efforts to cooperate with the government during an investigation.

### 2. Protecting the Privilege During and After Internal Investigations[133]

Companies develop and deploy internal investigations to strengthen both business operations and legal compliance efforts. Yet, despite the tremendous value-add offered by such investigations, the collection of sensitive data, interviews, and analyses presents its own unique set of challenges. Often the material assessed and incorporated in investigations is at the core of contentious litigation (or expected litigation), delicate public relations, or other highly sensitive company considerations. Accordingly, legal departments and executives alike frequently (and correctly) fear the dissemination of investigative reports and their underlying materials. The disclosure of internal investigation materials is increasingly being litigated, and as recent precedent demonstrates, efforts to preserve the privilege should begin as soon as a company is put on notice of circumstances warranting further inquiry.

For better or worse, the intersection of privilege jurisprudence and internal investigations has already begun to alter the way in which investigations are conducted. This evolution was the subject of litigation in *United States v. Baroni*, a case involving the so-called "Bridgegate Scandal" that occurred when parts of the "George Washington Bridge were closed without public warning," seemingly as an act of political retribution.[134] A law firm conducted an intense review of the matter, ultimately conducting "70 interviews and review[ing] more than 250,000 documents" in only two months. After its investigation, the law firm issued a public

132. *United States v. Wells Fargo*, 132 F. Supp. 3d 558, 559 (S.D.N.Y. 2015).
133. For further discussion of privilege and waiver considerations, see Part G(6)(c).
134. *United v. Baroni*, No. 2:15-cr-00193, 2015 WL 9049528 (D.N.J. 2015).

report detailing its findings. *Baroni* arose when two individuals indicted in the misconduct sought access to the "handwritten notes" and related materials underlying the publicly-released documents. The law firm, however, had intentionally deviated from its usual recordkeeping practices (contemporaneous notes and follow-up memoranda) and instead prepared memoranda in the same documents in which they had taken contemporaneous notes—which had already been produced. Though finding the change of practice distasteful and frustrating, the court had no choice but to quash the subpoenas:

> Although [the law firm] did not delete or shred documents, the process of overwriting their interview notes and drafts of the summaries had the same effect. This was a clever tactic, but when public investigations are involved, straightforward lawyering is superior to calculated strategy. The taxpayers of the State of New Jersey paid [the law firm] millions of dollars to conduct a transparent and thorough investigation. What they got instead was opacity and gamesmanship. They deserve better.[135]

Yet despite "deserving better," no notes were produced.

In sum, strategies for protecting and preserving the privilege in internal investigations need to be rigorously considered and implemented before the first interview, document dump, or report is issued. As the cases illustrate, courts are increasingly forcing litigants to turn over investigative materials where only ad hoc or retrospective approaches to privilege are deployed.

### 3. Strategic Reasons to Waive the Attorney-Client Privilege

#### (a) Traditional View

In some jurisdictions, regulators or prosecutors may require legal privilege to be waived before crediting cooperation. Generally, the privilege will not apply if the communication is made in the presence of a third party. The privilege also is waived if shared with other third parties.

In DOJ investigations, until recently, cooperation credit was dependent on waiver of privilege. That is no longer the case. The DOJ has recognized that the attorney-client privilege and attorney work-product doctrine are "essential and long-recognized components of the American legal system."[136] As a result, DOJ policy does not allow prosecutors to condition cooperation credit on a waiver of privilege.[137] Similarly, the CFTC and the SEC prohibit their enforcement staff from asking a party to waive privilege unless authorized by the Director or a Deputy Director of their respective Divisions of Enforcement.[138] Company counsel should be mindful, therefore, that waiver is voluntary in almost all situations.

##### (1) Voluntary Waiver

There are many reasons a company might consider a voluntary waiver of its attorney client or attorney work product privileges. Among the reasons is that companies in the U.S. are eligible for "cooperation credit" from the

135. *Id.* at *4.
136. Justice Manual, *supra* note 47 at § 9-28.710.
137. *See* Justice Manual, *supra* note 47 at § 9-28.700.
138. *See* CFTC Enforcement Manual 9.3; SEC Enforcement Manual 4.3.

government where they are willing to disclose information about their potential misconduct.[139] Cooperation can lead to lower financial and regulatory penalties, faster resolution of the government's investigation, and even non-prosecution or deferred prosecution agreements.

If and when a company chooses to waive the privilege voluntarily to the government, the company should seek a confidentiality agreement with the regulator to protect the privilege. Note that courts may not find that a confidentiality agreement provides adequate protections against third parties seeking access to privileged materials that have been disclosed to the government. Under the doctrine of selective waiver, in certain limited circumstances, a voluntary disclosure of privileged documents to the government will not waive privilege as to all other parties and proceedings.[140] However, U.S. appellate courts have largely ***rejected*** the doctrine of selective waiver.[141]

The Second Circuit, however, has refused to adopt "a per se rule that all voluntary disclosures to the government waive work-product protection."[142] In *In re Steinhardt Partners L.P.*, the Second Circuit found that Steinhardt Partners had waived privilege over a memorandum prepared by its attorneys and submitted to the SEC. However, it instructed trial courts to examine the applicability of the selective waiver doctrine on a case-by-case basis, explaining that the doctrine may apply when "the disclosing party and the government may share a common interest in developing legal theories and analyzing information, or situations in which the SEC and the disclosing party have entered into an explicit agreement that the SEC will maintain the confidentiality of the disclosed materials."[143] Steinhardt had no such common interest with the SEC nor did it have a confidentiality agreement with the SEC. Following Steinhardt, district courts in the Second Circuit have found selective waiver only in limited circumstances.[144] By contrast, most courts have rejected parties' invocations of selective waiver. For example, in *Gruss v. Zwirn*, the court did not allow a hedge fund to invoke the selective waiver doctrine in a defamation action brought by its former CFO.[145] Instead, the court found that witness interviews made during the course of an internal investigation and subsequently disclosed to the SEC were discoverable, reasoning that a company cannot produce privileged material to its adversary, but maintain its privilege as to others.[146]

The shifting landscape in U.S. courts as to whether a party effectively may assert selective waiver principles and take comfort in the enforceability of

139. *See e.g.*, Mark Filip, U.S. Dep't of Justice, *Principles of Federal Prosecution of Business Organizations* (Aug. 28, 2008), **https://www.justice.gov/sites/default/files/dag/legacy/2008/11/03/dag-memo-08282008.pdf**; Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation of Agency Enforcement Decisions, released as Securities Exchange Act of 1934 Release No. 44969, Accounting and Auditing Enforcement Release No. 1470 (Oct. 23, 2001).
140. *See Diversified Indus. v. Meredith*, 572 F.2d 596 (8th Cir. 1977).
141. *See*, *e.g., In re Qwest Commc'ns Int'l*, 450 F.3d 1179, 1197 (10th Cir. 2006); *Burden-Meeks v. Welch*, 319 F.3d 897, 899 (7th Cir. 2003); I*n re Columbia/HCA Healthcare Corp. Billing Practices Litig.*, 293 F.3d 289, 295 (6th Cir. 2002); *United States v. Mass. Inst. of Tech.*, 129 F.3d 681, 686 (1st Cir. 1997); *Genentech, Inc. v. U.S. Int'l Trade Comm'n*, 122 F.3d 1409, 1416-18 (Fed. Cir. 1997); *Westinghouse Elec. Corp. v. Rep. of Philippines*, 951 F.2d 1414, 1425 (3d Cir. 1991); *In re Martin Marietta Corp.*, 656 F.2d 619, 623-24 (4th Cir. 1988); Permian Corp. v. United States, 665 F.2d 1214, 1221 (D.C. Cir. 1981); *In re Pacific Pictures Corp*., 679 F.3d 1121 (9th Cir. 2012).
142. *In re Steinhardt*, 9 F.3d 230 (2d Cir. 1993).
143. *Id.* at 236.
144. *See, e.g., Police and Fire Retirement System of City of Detroit v. Safenet, Inc.*, 2010 WL 935317 (S.D.N.Y. Mar. 12, 2010) (finding privilege to still apply to materials provided tot he government pursuant to a confidentiality agreement); *In re Natural Gas Commodities Litig.*, 232 F.R.D. 208 (S.D.N.Y. 2005) (same).
145. *Gruss v. Zwirn*, 276 F.R.D. 115, 122 (S.D.N.Y. 2011); *see also In re Weatherford Int'l Sec. Litig.*, No. 11 Civ. 1646, 2014 WL 6628964 (S.D.N.Y. Dec. 16, 2013) (finding the privilege did not apply to interview materials that are "explicitly identified, cited, or quoted in information disclosed to the SEC").
146. *Id.*

confidentiality agreements with the government counsels on careful consideration of the degree to which and the manner in which parties choose to disclose privileged material to the government in a cooperation setting. For example, oral presentations to the government highlighting key findings rather than wholesale disclosure of full investigative reports complete with citations to interview memoranda and other attorney work product will more likely protect privileged materials from third party access in subsequent proceedings.

In certain instances, communications with third parties will not necessarily result in waiver of privilege. For example, communications made in the presence of a non-client who is necessary to facilitate attorney client communication (e.g. an accounting expert) to help the attorney give legal advice will not waive the attorney-client privilege. The privilege also will not be waived during inadvertent document production in litigation if reasonable precautions were taken.[147] However, absent such special circumstances, the general rule in most U.S. jurisdictions remains that if there is a waiver as to one person, the privilege is waived as to everyone.

**(2) Specific Federal Cooperation Programs**

The cooperation credit described above, including the relevant sections of Justice Manual and the Yates Memo, applies to all criminal matters for which the U.S. Sentencing Guidelines may be at issue.[148] A number of specific government programs also exist, however, which further incentivize voluntary self-disclosure. Among the most prominent of these are the (i) Foreign Corrupt Practices Act ("FCPA") Pilot Program, and (ii) DOJ Antitrust Leniency Program.[149] Both the CFTC and SEC also have a cooperation program.[150]

Under the FCPA Pilot Program,[151] parties that self-disclose misconduct, cooperate fully with the government's investigation, and remediate appropriately, may be entitled to "a 50% reduction off the bottom of the Sentencing Guideline fine range" and avoid the imposition of a corporate monitor. Additionally, voluntary self-disclosure under the FCPA Pilot Program may also help a party avoid prosecution altogether—as of September 2016, the DOJ has issued five declinations to participants in the program.[152]

Similar to the FCPA Pilot Program, the DOJ's Antitrust Division offers a Leniency Program to parties that report misconduct.[153] As explained by the Antitrust Division, "the first corporate or individual conspirator to confess participation in an antitrust crime, fully cooperate with the Division, and meet all other conditions that the Corporate Leniency Policy or the

147. *See Reckley v. City of Springfield*, No. 3:05-cv-249, 2008 WL 5234356 (S.D. Ohio Dec. 12, 2008) ("attorney client privileged" label and prompt action after learning of production indicated necessary precaution).
148. Additional information on the U.S. Sentencing Guidelines is accessible at: **http://www.ussc.gov/guidelines/2016-guidelines-manual**.
149. Many other DOJ divisions and government agencies accept voluntary self-disclosures, including the Office of Foreign Asset Controls and the DOJ's National Security Division ("NSD") regarding export control and sanctions-related violation. For additional information on the NSD's policy, *see* **https://www.justice.gov/nsd/file/902491**.
150. For more information about the CFTC's and SEC's cooperation programs, see the discussion at pages 21-27 above.
151. U.S. Dep't of Justice, Criminal Division, Fraud Section, *Foreign Corrupt Practices Act Enforcement Plan and Guidance* (April 5, 2016), **https://www.justice.gov/criminal-fraud/file/838416**.
152. For specific declinations, please *see*: **https://www.justice.gov/criminal-fraud/pilot-program/declinations**.
153. *See* U.S. Dep't of Justice, *Frequently Asked Questions about the Antitrust Division's Leniency Program and Model Leniency Letters*, (Jan. 26, 2017), **https://www.justice.gov/atr/page/file/926521**.

Leniency Policy for Individuals specifies receives leniency for the reported antitrust crime." In short, the first party to report misconduct and complete the program's requirements avoids criminal prosecution, financial penalties, and imprisonment. The program provides tremendous incentives for a party that is "first in" to disclose the contents of its internal investigations into possible misconduct, potentially implicating privilege issues, in order to avail itself of the benefits of leniency. For more information on the DOJ's Leniency Program, see the discussion at pages 19-21 above.

In short, with the development and success of these programs, the DOJ and other agencies are likely to implement similar self-disclosure programs in other areas of the law—both criminal and civil. Such programs will further implicate privilege-waiver issues, and therefore practitioners should consider whether possible voluntary self-disclosure might be necessary at the start of every investigation.

**(b) Other Considerations**

Treatment of waiver may differ in other jurisdictions. The UK, for example, may recognize selective waiver under certain circumstances.[154]

Overall, there is some uncertainty as to the effectiveness of confidentiality agreements, but it nevertheless is still prudent to have one in place. Companies considering whether to waive privilege will need to weigh the likelihood that a U.S. court will refuse to recognize a selective waiver of privilege against the need to disclose such information.

## 4. Impact of Foreign Law on Privilege Protections

Another consideration in cross-border investigations is that the attorney-client privilege and attorney work-product doctrine may not have a U.S. equivalent in other jurisdictions. It is important for companies to be aware of these differences, where they do exist. The consequences may be dire: in jurisdictions where privilege is not recognized, authorities have been known to conduct searches or dawn raids of external counsel's offices. Other jurisdictions do not consider communications with the company's in-house counsel to be privileged.[155] This can pose problems in the United States, where courts may refuse to recognize privilege in communications involving a company's foreign in-house counsel where the local law does not recognize it.[156] In such instances, a company should mitigate this risk by conducting the investigation through external counsel.

Southern District of New York Magistrate Judge Gabriel Gorenstein's January 2015 decision in *Wultz v. Bank of China Limited* illustrates the risk foreign companies face when seeking to assert attorney-client privilege and attorney work-product privilege over communications with foreign in-house legal counsel.[157]

154. *See* Financial Conduct Authority, *The Enforcement Guide*, Section 3.28, ("[F]irms may seek to restrict the use to which a report can be put, or assert that any legal privilege is waived only on a limited basis and that the firm retains its right to assert legal privilege as the basis for non-disclosure in civil proceedings against a private litigant."); *see also Berezovsky v. Hine*, (2011) EWCA Civ 1089 (C.A. Civ) (recognizing limited waiver); *Property Alliance Group Limited v. The Royal Bank of Scotland plc*, (2015) EWHC 1557 (Ch) (recognizing limited waiver and the validity of non-waiver agreements, even where they include carve-outs permitting onward disclosure, and citing Irish and Hong Kong decisions to similar effect).
155. Certain jurisdictions do not recognize the attorney-client privilege congruent to U.S. privilege, particularly with respect to in-house counsel. See, e.g., Case C-550/07, *Akzo Nobel Chem. Ltd. v. Comm'n*, 2010 E.C.R. I-08301 (finding that legal professional privilege requires an exchange emanating from independent lawyers, which excludes lawyers bound to the client by a relationship of employment).
156. *See, e.g., Wultz v. Bank of China Ltd.*, 979 F.Supp.2d 479, 495 (S.D.N.Y. Oct. 25, 2013) (quotations omitted) (holding that the attorney-client privilege did not apply to communications with in-house counsel in China because it does not apply to "communications from, to and among members of legal or other departments who are not licensed attorneys" and ordering the production of such documents).
157. *See Wultz v. Bank of China Ltd.*, 304 F.R.D. 384 (S.D.N.Y. 2015) (hereinafter the "Bank of China Opinion and Order").

In *Wultz*, the family of a victim of a terrorist attack issued a demand letter to the Bank of China. In the demand letter, the family alleged that the bank was liable for its role in holding and transferring the funds the senior terrorist operative used in perpetrating the attack. The demand letter also indicated that the family intended to file suit against the bank in federal court. Subsequently, the bank initiated an internal investigation using mainly Chinese employees in the bank's compliance and legal departments,[158] consistent with the bank's anti-money laundering policies. The bank did not use any U.S.-qualified attorneys in its internal investigation. After filing suit in the Southern District of New York, the family sought discovery of the documents the bank created during its internal investigation.[159] The Bank of China argued that the documents prepared in connection with the internal investigation were protected under the attorney-client privilege because the documents were prepared to submit to U.S. counsel for review.[160] Judge Gorenstein disagreed, finding that the attorney-client privilege does not attach to documents foreign employees prepare for U.S. counsel to review.[161]

Practitioners must also be aware of how foreign courts will treat materials prepared at the behest of U.S. counsel when that material is taken or prepared outside of the U.S. In a recent landmark English case, *The RBS Rights Issue Litigation*,[162] an English court found that the privilege did not shield interview notes, prepared in response to a SEC subpoena, from discovery in subsequent English civil litigation. In short, the court held that materials compiled for fact gathering purposes, such as employee interview notes, are not covered by the English law legal advice privilege. Thus, although it is likely that attorney-prepared interview notes containing some legal analysis or assessment would be covered by both the attorney-client and work product privileges in the U.S., because the notes were subject to production in England, the English court applied English privilege rules and required production of the notes. When planning interviews or preparing to take other investigative steps, it is crucial that counsel consider the privilege rules of not only their own jurisdiction, but also the jurisdiction where the interview will take place.

In cross-border matters, the fact that a company is compelled to disclose privileged material in a foreign jurisdiction may not necessarily result in a waiver in subsequent U.S. proceedings. Some U.S. courts have held that involuntary or compelled disclosure of privileged documents does not automatically result in a waiver of attorney-client privilege.[163] Likewise, under the work-product doctrine, the result is the same.[164] However, even when the disclosure of protected documents is involuntary, the disclosure may still result in a waiver if the party

158. In a prior discovery ruling in the same litigation, U.S. District Judge Shira Scheindlin found that in-house counsel in China as a general rule do not need to be admitted to the practice of law, and therefore, held that the employees in the Bank of China's compliance department could not invoke the attorney-client privilege despite the Bank of China's argument that the compliance employees were "the functional equivalent" of attorneys. *See Wultz v. Bank of China Ltd.*, 979 F. Supp.2d at 493-95.
159. *See* Bank of China Opinion and Order, at 304 F.R.D. at 386-390.
160. *See id.* at 391-392.
161. *See id.* The court also found that the attorney work-product doctrine did not apply to the documents prepared in connection with the internal investigation. Although Rule 26(b)(3) of the Federal Rules of Civil Procedure states that an attorney does not need to be the author of the document for the work-product doctrine to apply, the Bank of China failed to meets its burden of demonstrating that the documents produced in response to demand letter would not have been produced if the threat of litigation did not exist. *See id.* at 393-397.
162. [2016] EWHC 3161 (Ch).
163. *See, e.g., In re Parmalat Sec. Litig.*, No. 04-MD-1653, 2006 WL 3592936, at *4 (S.D.N.Y. Dec. 1, 2006) (seizure of privileged documents by Italian *authorities* did not on its own constitute a waiver of privilege over those documents in subsequent U.S. class action litigation because the disclosure to Italian authorities was involuntary); *see also Pension Comm. of U. of Montreal Pension Plan v. Banc of Am. Secs. LLC*, No. 05-37 9016, 2009 WL 2921302, at *1 (S.D.N.Y. Sept. 8, 2009) (disclosure of communications with counsel did not amount to a waiver of privilege because disclosures were made pursuant to a court order).
164. *Shields v. Sturm, Ruger & Co.*, 864 F.2d 379, 382 (5th Cir. 1989) ("When a party is compelled to disclose privileged work product and does so only after objecting and taking other reasonable steps to protect the privilege, one court's disregard of the privileged character of the material does not waive the privilege before another court.").

asserting privilege cannot establish that it took steps "reasonably designed to protect and preserve the privilege."[165] Therefore, making every effort to preserve U.S. privilege every step of the way (and keeping records of those efforts) is crucial to preventing disclosure.

**(a) Considerations for U.S. Discovery in Foreign Jurisdictions**

In cross-border investigations, the information gathering process is further complicated because the relevant documents, witnesses, and information may be located at the company's foreign offices. Counsel representing multi-national corporations in these investigations, including those entities located outside of the U.S. whose trading occurs in or affects U.S. securities and commodities markets, thus need to be sensitive to important differences in information gathering expectations and laws overseas.

Preliminarily, counsel should be sensitive to the fact that management and employees in these foreign offices may not be as familiar with the breadth and scope of U.S.-style discovery. Counsel must take care to ensure that these officers preserve potentially relevant documents and information. This means putting a document hold into effect via a notice to employees likely to have relevant documents and suspending any routine document destruction policies.

Counsel must also consider any laws, bar rules, and privilege customs related to data privacy and bank secrecy of the local jurisdiction in which the investigation is being conducted that may affect data collection and preservation efforts. Data privacy and bank secrecy regimes present significant challenges to disclosure of cross-border information by companies to U.S. regulators and their counterparts in other jurisdictions. Non-U.S. organizations are often subject to additional duties of confidence and professional secrecy owed to their clients and may be placed in a difficult position when faced with a request for information from the U.S. authorities.

**(1) Data Privacy**

In countries with strict data privacy rules, companies should be aware that the laws may apply differently for data stored in the U.S. and data stored locally. Local laws may limit access to documents and the ability to move them from one jurisdiction to another. This is particularly true in the U.K. and Europe, where data privacy laws place restrictions on how data can be collected and transmitted. In some instances, a company may need to enter agreements with the concerned individual. Certain jurisdictions also differentiate between data in emails and data in financial documents.

Personal data has a high standard of protection under the laws of EU countries. The latest applicable data privacy and security law in the EU, the General Data Protection Regulation "GDPR", went into effect in 2018 and is one of the toughest privacy and security laws in the world. It imposes obligations on organizations anywhere, so long as they offer goods or services to or monitor the behavior of data subjects in the EU.[166]

165. *In re Parmalat*, 2006 WL 3592936, at *4 (internal quotation omitted).
166. *See* Art. 3, 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

The GDPR is drafted broadly to cover a wide range of processing activity and data. The GDPR defines data "processing" to include any action performed on data, whether automated or manual. As for what data is covered, the statute defines "personal data" to include any information that relates to an individual who can be directly or indirectly identified. This includes obvious data elements such as names and contact information as well as other data such as location information, ethnicity, gender, biometric data, religious beliefs, web browsing history, and political opinions. Pseudonymous data can also fall under the definition if it is relatively easy to identify a data subject associated with the data.[167]

The GDPR also places restrictions on cross-border transfers of personal data. Specifically, the statute requires companies seeking to transfer data to countries outside the European Economic Area to ensure that data subjects retain protections and rights relating to their data at a level analogous to that under the GDPR.[168] For some countries such as Japan and Switzerland, the European Commission has determined that these jurisdictions' local data protection regime are sufficient to protect personal data, meaning no specific additional protections need to be put into place. For countries without such "adequacy decisions," companies must put into place certain protections, including contractual obligations for receiving parties.[169]

**2) Bank Secrecy**

Financial institutions are subject to bank privacy laws of foreign jurisdictions in which they operate. The English common law, which is followed in the U.K. offshore islands, the Cayman Islands, and many other jurisdictions, recognizes a duty of confidentiality that banks owe to their customers. Such a duty can extend to instances where banks may be prevented from disclosing confidential customer information, including to domestic and foreign regulatory authorities, except in limited circumstances. Generally, data may not be shared without consent, necessity to protect a bank's interest, by virtue of a domestic court order (not foreign), and in rare instances where there is a duty to disclose to the public. Other jurisdictions such as Germany treat any bank-customer relationship as an implied contract and prohibit disclosure of customer-related information without consent. An exception is often made for domestic court orders, but not foreign. Violation of these duties by disclosure may lead to sanctions of civil penalties as well as injunctions against disclosure.

Finally, companies should be aware of statutory bank secrecy obligations, such as those in Luxembourg and Switzerland, which may prohibit disclosure of confidential information even in instances of consent.

167. *See id.*, Art. 4.
168. *See id.*, Art. 44.
169. Guidance from EU data protection regulators regarding what protections must be put into place is still developing following the Schrems II decision issued on July 16, 2020. *See generally Schrems II (Data Protection Commissioner v. Facebook Ireland Ltd.)*, 2020 C-311/18 (July 16, 2020).

**(3) Blocking Statutes**

In addition to data privacy and data protection regimes in non-U.S. jurisdictions, certain jurisdictions also have so-called "blocking statutes" that may directly place limitations on discovery in the United States. Such statutes may prohibit transfer of documents sought for the purpose of constituting evidence for a potential foreign judicial or administrative proceeding or in connection with it. However, notable exceptions in such statutes are made for discovery of documents through "treaties or international agreements." Where such statutes do exist, companies should be aware that the evidence may still be within the reach of U.S. authorities.

**(b) Cooperation Agreements**

U.S. regulatory authorities may be able to overcome restrictions on data transfer by operation of cooperation agreements known as "mutual legal assistance." Many countries, including the U.S., are party to treatises, conventions, protocols, and Framework Decisions, designed to facilitate cooperation in transnational sharing of information among legal authorities. The Mutual Legal Assistance Treaties ("MLAT"), for example, can assist U.S. regulators to request information from non-U.S. companies through the assistance of local authorities. The use of MLATs in criminal and civil proceedings, thus, overcomes the restrictions that non-U.S. companies may face under domestic law to sharing the information directly with U.S. regulators. MLAT requests do impose a number of requirements, however, such as establishing "dual criminality" under both countries' laws.

# CONTACTS

**David Yeres**
**Senior Counsel**
T: +1 212 878 8075
E: david.yeres@cliffordchance.com

**Robert Houck**
**Partner**
T: +1 212 878 3224
E: robert.houck@cliffordchance.com

**Celeste Koeleveld**
**Partner**
T: +1 212 878 3051
E: celeste.koeleveld@cliffordchance.com

**John Friel**
**Partner**
T: +1 212 878 3386
E: john.friel@cliffordchance.com

**Robert Rice**
**Counsel**
T: +1 212 878 8529
E: robert.rice@cliffordchance.com

**Benjamin Berringer**
**Associate**
T: +1 212 878 3372
E: benjamin.berringer@cliffordchance.com

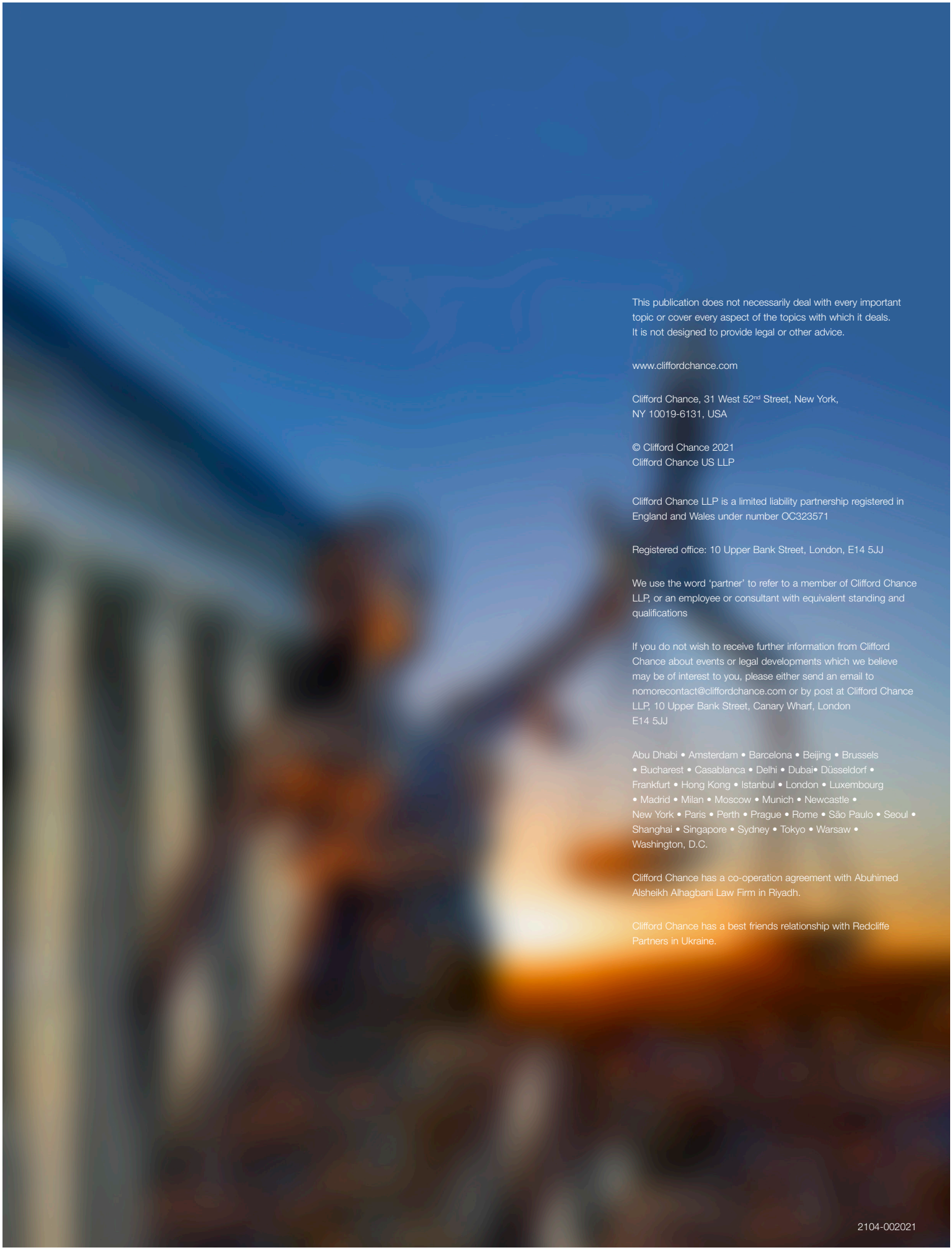
**E. Carlisle Overbey**
**Associate**
T: +1 212 878 8504
E: carlisle.overbey@cliffordchance.com

**Benjamin Peacock**
**Associate**
T: +1 212 878 8051
E: benjamin.peacock@cliffordchance.com

**Brendan Stuart**
**Associate**
T: +1 212 878 8133
E: brendan.stuart@cliffordchance.com

**Brian Yin**
**Associate**
T: +1 212 878 4980
E: brian.yin@cliffordchance.com

# Notes





www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA



2104-002021