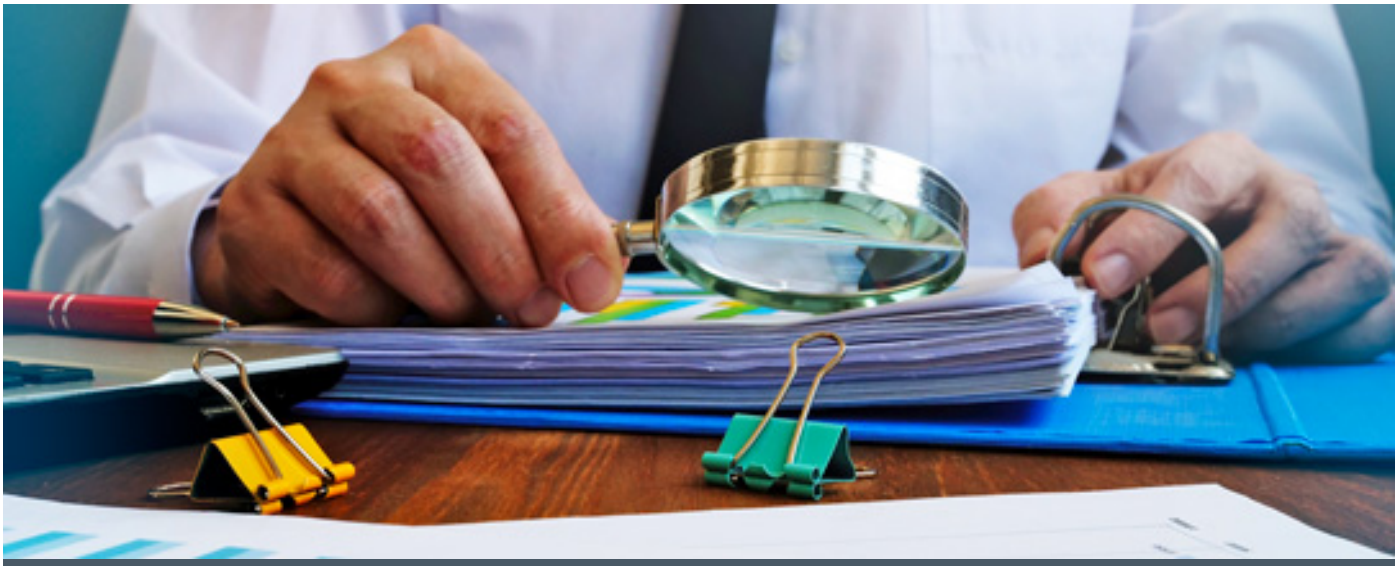
JONES DAY | One Firm Worldwide®



WHITE PAPER

November 2022

Conducting an Effective Internal Investigation — An Overview

With developments in the investigations field, including the ongoing expansion of this field internationally, companies face an unprecedented level of scrutiny from outside parties, including government agencies, and are increasingly seeing the benefits of getting to the bottom of allegations of corporate misconduct. Indeed, the stakes in both internal and government investigations are often enormously high, particularly when high-level corporate personnel or significant business operations are involved. As such, it is essential for companies and their counsel to understand how to conduct effective investigations in accordance with sound practices and governing legal principles. This *White Paper* is the first in a series of Jones Day articles that will provide "soup to nuts" coverage of corporate internal investigations. In this initial *White Paper*, we provide an overview of key investigations topics that we will discuss in more detail throughout the series.

INTRODUCTION

Now more than ever, it is important for companies and their counsel, regardless of prior investigations experience, to have at least a baseline understanding of sound investigations practices and relevant legal principles. With both internal and government investigations, the stakes are often enormously high. Companies can be sent reeling by serious allegations of misconduct from within, particularly when high-level corporate personnel or significant business operations are involved. And the external threats to a company arising out of major misconduct allegations—such as the prospect of government enforcement actions—are typically no less daunting and sometimes even threaten the company's viability. In either circumstance, companies are well-served by promptly getting to the bottom of the allegations, assessing the legal and business significance of the facts discovered, and ultimately making informed judgments on the best course of action among the available options. An internal investigation, done properly, is the means to achieve these critical objectives.

In the United States, government agencies that monitor corporate conduct and demand or exact hefty fines and other penalties in connection with enforcement actions include the U.S. Department of Justice ("DOJ"), the U.S. Securities & Exchange Commission ("SEC"), the Commodity Futures Trading Commission ("CFTC"), and state attorneys general. As recently as September 2022, DOJ announced new changes to corporate criminal enforcement policies, reflecting the Biden administration's stated goal of prioritizing white-collar criminal enforcement against companies and individuals.[1] Regulators and enforcement officials in other countries are increasingly getting into the corporate enforcement game, bolstered by strengthened legal authority, local political dynamics, victories and resulting financial bounties in particular cases, and the exchange of investigative information with counterparts in other jurisdictions. Indeed, government investigations into cross-border conduct increasingly involve cooperation and even joint investigative efforts among the interested jurisdictions, or simply parallel investigations and enforcement proceedings in domestic jurisdictions. Adding yet another layer of complexity and potential risk to corporate entities is the emerging industry of whistleblower law firms that actively recruit clients and alert various authorities to alleged corporate wrongdoing in the hope of securing monetary awards under whistleblower reward programs.

The upshot is that throughout the world, corporations as well as their directors, officers, employees, and agents are being watched more closely than they have ever been by government agencies and the full range of corporate stakeholders and other interested parties (e.g., shareholders and other prospective civil litigants, the media, customers, and consumer groups, etc.). Corporations must pay increasingly close attention to conduct on the part of their employees and agents that can expose the entities to legal, financial, and reputational harm. Indeed, the rise in corporate enforcement activity is being met by a heightened awareness on the part of companies of the benefits of effective self-policing, not just as an important end in itself, but also as a means of mitigating a company's exposure in the event of a government investigation or enforcement action. While companies can be challenged in ensuring that employees and agents at all times act in accordance with the requirements of law and internal policies, what they can control is the design, implementation, and operation of their corporate ethics and compliance programs.

Central to any well-functioning corporate ethics and compliance program are well-considered and followed policies, procedures, and practices for initiating, conducting, concluding, and addressing the findings of internal investigations, and for appropriately responding to government investigations. Again, in this regard, the internal investigation is an essential tool that importantly identifies facts that may present past and current compliance risks, enables informed judgments as to any appropriate remedial action (e.g., personnel action, enhancements to relevant internal controls, and employee training), and places the company in a better position to address any government investigation or private litigation that might arise from the underlying conduct.

For any particular internal investigation to serve its purposes, it must be planned and executed with the utmost thoughtfulness and skill, and pitfalls must be avoided. There is no room for "winging it" when it comes to investigating alleged corporate misconduct; to the contrary, the field of internal investigations has undeniably matured to the point where there are certain established practices and conventions that should not be avoided without proper justification. If these conventions are not followed, this could cast doubt on the investigation's credibility and the corporate entity's good faith. And yet, internal investigations remain both science and art, and all investigations involve measures of both formal technical practice and the exercise of substantial professional judgment and discretion.

WHY CONDUCT AN INTERNAL INVESTIGATION?

Well-executed internal investigations can benefit a company in a number of respects, including by:

- **Revealing the Facts.** The principal goal of any corporate internal investigation is to identify the facts relating to the matter under investigation—typically, the who, what, where, when, and why as to something that happened (or did not happen).
- **Identifying and Analyzing Compliance Issues.** The collection of relevant facts, viewed in light of applicable laws and corporate policies, in turn, permits an informed assessment of the source(s) and reason(s) for any wrongdoing, the legal implications of the conduct, and the potential options for remediating the conduct.
- **Improving Compliance.** Internal investigations regularly result in the identification of remedial measures to address any specific wrongdoing and to improve the corporate compliance program more broadly. In addition, while much about internal investigations should typically be kept confidential and shared with corporate personnel only on a "need to know" basis, the mere existence of an investigation itself is an indication of the company's commitment to compliance and can serve as a strong deterrent to unethical conduct.
- **Managing Whistleblower Concerns.** Whistleblowers who report suspected misconduct to the companies involved (as opposed to bypassing the companies and making their allegations to government authorities in the first instance) are often genuinely interested in seeing that the companies appropriately address the allegations.[2] When warranted, launching an internal investigation is often key to responding to a whistleblower allegation and can help assure the whistleblower that the company takes the matter seriously and is committed to addressing the matter free of any government involvement.[3]
- **Mitigating Risk in Connection with Government Investigations.** Promptly and thoroughly investigating allegations of corporate misconduct can position the company to effectively respond to any ongoing or later investigative inquiry from government agencies. While regulators that become aware of such allegations may not respond with a full-scale investigation of their own, a company should, at a minimum, be prepared to explain how it responded to the allegations. When making a charging decision or reaching a resolution with companies relating to alleged corporate misconduct, DOJ, SEC, and/or other government authorities may consider whether the company conducted an effective internal investigation into the allegations and any resulting remediation.[4]

Ultimately, conducting robust internal investigations is about fostering a strong culture of compliance and reducing corporate risk. Whether the results of the investigation are shared with regulators through self-disclosure or they are otherwise aware of the allegations, if not investigating in parallel, adhering to best practices for investigating and remediating misconduct reduces improper conduct among corporate personnel and places the company in a better position vis-à-vis government agencies and potential private litigants.

WHEN TO INVESTIGATE

An internal investigation can be prompted by many events and sources, including:

- Written or oral whistleblower communications, or other reporting from current or former employees or other parties;
- Communications from law firms on behalf of purported whistleblowers;
- Allegations of misconduct from competitors, suppliers, or others in the industry;
- Complaints made to HR, Legal, Compliance, or other internal departments;
- Audit findings;
- Media reports containing misconduct allegations;
- Government subpoenas or other requests for documents and interviews;
- Other indicia of law enforcement activity (e.g., formal charges or "dawn raids").

Regardless of how allegations of corporate misconduct come to light, they should always receive the attention and treatment they are due in accordance with rational fact- and risk-assessment principles. Generally, full-fledged internal investigations are most advisable with respect to allegations of greater apparent seriousness and credibility. In this context, seriousness may be a function of, among other things, the person(s) implicated, the nature and extent of the alleged misconduct, and the potential legal exposure for the company. Credibility may be assessed based on the specificity and the demonstrable accuracy or inaccuracy of the information provided, and the existence or lack of any corroborating evidence.

When allegations warrant an internal investigation, it is usually advisable to involve Legal, Compliance, or investigation counsel within the company at the outset. Any personnel who themselves are or could be implicated in the conduct under investigation should not be involved. Companies routinely engage outside counsel to conduct and advise on internal investigations when, for example, such counsel have special experience or expertise; the allegations are serious in scope and severity (e.g., bribery, misrepresentations in public disclosures or financial reporting, large-scale fraud or embezzlement, misconduct by senior executives); the location or nature of the matter calls for heightened independence on the part of the lead investigators or heightened protection under an applicable privilege (e.g., attorney-client privilege); capacity constraints prevent an entirely in-house approach to the investigation; or a parallel government investigation is ongoing or expected. A robust, counsel-led investigation may be unnecessary if the allegations clearly lack credibility, can easily be disproven, or relate to workplace conditions or practices that do not rise to the level of violations of law or company policies (e.g., complaints about managers or coworkers that are appropriately managed by Human Resources).

COMPONENTS OF EFFECTIVE INTERNAL INVESTIGATIONS

In the *White Papers* that follow, we will address some of the key aspects of "effective" corporate internal investigations, while recognizing that the approach to any given investigation is highly fact- and circumstance-dependent. Broadly speaking, effective investigations conform to established sound practices, comply with applicable laws, and are designed to uncover the relevant facts. The following provides an overview of the components to an investigation that companies should typically consider in assessing the best approach to take.

THE PROPER INVESTIGATIVE TEAM

When the allegations are particularly serious—e.g., potential bribery, corruption, fraud, or a long-standing course of problematic conduct—or where there is a likelihood of a government inquiry, companies typically engage outside counsel to investigate in coordination with in-house counsel.

Among the benefits to using outside counsel, the most prominent is usually enhanced independence. Outside counsel is

typically regarded as sufficiently independent from the company so that internal stakeholders and authorities can have faith in the credibility and integrity of the investigation. In some situations, such as when the alleged misconduct implicates senior management or the company's public disclosures, independent counsel is necessary. Many white-collar lawyers also have experience and rapport with the relevant regulators, which can help streamline coordinating with a parallel government investigation.

In situations in which outside counsel is involved, it is often advisable to designate an in-house attorney to lead or jointly lead the internal investigation effort alongside outside counsel. The in-house counsel usually understands the business and its compliance program, data systems, and history of allegations. They may also have an established, trusted relationship with employee witnesses that can assist in encouraging candor in the formal interview setting.

Additionally, companies are often faced with decisions about who should oversee the investigation process. Companies may select a committee of independent directors of the board—such as an audit or special committee—to receive periodic updates of ongoing investigations and oversee larger matters with higher risk. When an internal investigation focuses on conduct that potentially implicates corporate management, it is especially important that the investigating attorneys and committee overseeing the investigation be viewed as independent.

MAINTAINING PRIVILEGE

In most cases, it will be preferable for in-house or outside counsel to lead—and actively participate in—the investigation, as it will have a substantial impact on whether documents created during the investigation are protected from disclosure to adversaries by the attorney-client privilege and work product doctrine. While third parties and regulators might seek privileged documents and communications created during an investigation, taking early steps to maintain the protection creates, at minimum, an initial barrier to disclosure to enable the company to investigate the relevant conduct with limited concern that interview memoranda and other materials will be immediately discoverable.

Beyond having in-house or outside counsel function as the primary investigator, there are additional steps a company should take to strengthen confidentiality protection. They include documenting the purpose of the investigation as providing legal advice and emphasizing confidentiality to any employees aware of the investigation. In addition, counsel should retain any outside consultants or experts necessary to the investigation or should otherwise make clear in any retention agreements that their work is being completed at the direction of counsel to assist in providing the company with legal advice. When counsel takes an active role in the investigation, all relevant documents, communications, and work product should be clearly labeled as privileged and confidential throughout the investigation and should be closely maintained by the investigation working group to reduce the risk of further dissemination. When a parallel investigation is being conducted by regulators in or outside of the United States, careful consideration should be given to any disclosures and should account for the risk of potential privilege waivers. In cross-border matters, counsel should consider the privilege laws in all relevant jurisdictions.

KEY INVESTIGATIVE STEPS

Preparing a Reasonable Work Plan.

Once the company determines who will lead and oversee an investigation and how confidentiality will be maximized, it is helpful to develop a detailed work plan to guide the work of the investigation team. Typically, a work plan should, at a minimum:

- Identify the objective and scope of the review and the issues to be considered;
- Identify the anticipated data and documents to be reviewed and the witnesses to be interviewed; and

- Address the interim and possible final reporting that is expected, even if the form of any final report is not yet certain.

Ideally, a work plan will both comprehensively address the issues that require attention in the investigation and leave flexibility for any new or unexpected facts that may arise throughout the course of the review.

Developing a Reasonable Budget.

The cost of any internal investigation will largely hinge on the nature of the allegations and the effort necessary to complete investigative steps. When developing a proposed budget, counsel should consider all anticipated tasks, including:

- The number of data custodians and the number of likely witnesses to be interviewed (understanding that both often expand during the course of the investigation);
- The magnitude of the data collection effort;
- Any processing and storage fees for data vendors;
- Document review costs;
- The time associated with the preparation of investigative materials and coordination among investigation team members and client counterparts;
- Any need for subject matter experts (e.g., forensic accountants, computer forensic experts, etc.); and
- Reporting expectations to the board, regulators, or other stakeholders.

Additionally, the budget should account for the costs of identifying and implementing remedial measures related to any corporate misconduct. In cross-border investigations, companies and their counsel may also need to consider the involvement of local counsel to assist as necessary (e.g., analysis of in-country labor, data privacy, or other laws).

Preserving Potentially Relevant Evidence.

With any investigation, immediate steps should be taken to preserve any potentially relevant documents and data to protect against possible inadvertent or intentional evidence destruction. Companies should suspend regular document deletion for any individuals who may have relevant data and should take all necessary steps to maintain existing data from those individuals. Once all back-end steps are taken to ensure preservation of data and relevant employees become aware of the investigation through interviews or device collection, the company should issue legal holds to those employees. The hold should direct them to maintain all potentially relevant documents in their possession, including hard-copy documents and relevant mobile device data.

As new relevant custodians are identified during the investigation, their data should be preserved as well. Custodian documents, including hard-copy and electronic files (e.g., emails, instant messages, calendar invitations, text messages, and other electronic data), must be retained for the entire duration of the investigation. Taking a conservative approach will reduce risk. Companies should maintain all data available for as many custodians as may be involved in the conduct. As time passes and the investigation proceeds, secrecy is no longer guaranteed, and spoliation or destruction of evidence becomes a real risk.

Data Collection.

Once data on company systems has been preserved, the investigation team should determine an appropriate method for collecting relevant material for review. Many times, companies will engage outside vendors to collect relevant data, which helps preserve the chain of custody and the integrity of the imaged material. Other data collection—such as imaging business-issued devices—should be considered early but may not be executed until the company is ready to disclose to witnesses that an investigation is ongoing.

Another *White Paper* in this series will address the complex issue of data privacy and cross-border transfers of data, which can be an increasingly difficult issue to navigate at the outset of an investigation. The collection and review of

company-issued devices and personally owned devices used to conduct business can pose serious challenges under data privacy laws enacted in many countries following the European General Data Protection Regulation, or GDPR, model. Further, highly protective local labor laws in some countries may invalidate employee waivers to data privacy and require notification to labor councils of any investigation into conduct of a company's employees. In many cases, these hurdles are not insurmountable, but they often require a nuanced approach and careful planning, especially in light of DOJ's expectations regarding personal device policies.[5] In the case of a parallel or follow-on government investigation, U.S. regulators will often expect the company to do all within its power to secure relevant data during the course of an investigation despite competing foreign restrictions.

Review of Documents and Evidence.

If at all possible, the investigative team should review potentially relevant documents before conducting witness interviews. This can enable the company to begin to get a sense for whether the underlying allegations have merit and the investigators to better prepare for the interviews. Indeed, showing documents to a witness during an interview often substantially assists the fact-finding process. A truthful witness who might—based solely on memory—inadvertently misstate factual information contained in documentary evidence can have his or her recollection refreshed by that evidence and thus avoid any such misstatement. Similarly, a witness who might be inclined to provide incorrect or misleading information in response to questions unaccompanied by contrary documentary evidence is likely to shed (or at least rethink) that inclination when confronted with those contrary documents.

In some cases—where an investigation is particularly urgent, for example—it may be advisable to take steps to preserve data quickly, conduct initial scoping interviews, and later conduct more in-depth, follow-up interviews after the completion of document review. Scoping interviews, which typically involve gathering basic information from witnesses about corporate personnel, functions, and practices relevant to the allegations under review, can allow the investigation team to make initial assessments about locations and identities of key records and witnesses, and to streamline the document collection and review and the planning of interviews, accordingly.

Document reviews require highly organized and strategic, case-by-case planning. In most investigations involving a substantial volume of electronic communications and other electronic data, it is helpful to apply a set of carefully crafted search terms and a date filter to try to limit the universe of documents to review, while reducing, if not entirely eliminating, the risk of missing key documents. In other instances, it may be more helpful to run a set of very narrow, targeted searches across the data set initially to attempt to identify the most important documents as quickly as possible, and then to utilize technology-assisted review to locate other key documents in the data set. In all cases, it will be helpful to establish a process for categorizing and tracking significant documents and events as the review proceeds. A well-thought-out document coding strategy can assist in this process, as can fact chronologies or significant document charts.

Witness Interviews.

Witness interviews are a centerpiece of an effective internal investigation, and thus, another *White Paper* in this series will be dedicated to addressing interview best practices. Like other phases of an investigation, interviews require careful planning, both with respect to the structure and substance of each interview, and with respect to the overall interview plan and sequencing of interviews. Advance thought should be given to the timing, location, and participants for each interview. It is often helpful to have outside counsel conduct the interviews, but participation by in-house counsel may help with witness comfort and candor in some instances. It is critical that at least one participant take detailed notes of the interview.

At the outset of a witness interview in a corporation internal investigation, the interviewer must make clear whom he or she

represents with a proper *Upjohn* warning and must ensure the witness understands that the privilege covering the interview belongs to the company and that the company may decide to waive the privilege and share information with third parties. The interviewer should be prepared to answer questions from witnesses that may arise, including whether a witness needs his or her own lawyer and how the information shared with the interviewer will be used by the company in the future.

In most cases, the interviewer or notetaker should reduce the notes of the interview into a privileged summary shortly after the interview is complete. Cost and time considerations will often drive the type of summary prepared by the interview team. In many cases, it will be helpful and important to prepare a formal interview memorandum summarizing the discussion, but a simpler bullet-point summary may be appropriate sometimes. The summary should provide details as to who attended the interview, the instructions given to the witness, the witness's responses to targeted questions about the issues at play in the investigation, and any documents shown to the witness during the interview.

Reports and Closing the Investigation.

As the conclusion of an investigation approaches, the investigative team should continue to consult with the company about the format of any final report. Findings can be set forth in a written narrative report, a slide deck, some other summary document, or an oral presentation. The nature of the investigation and the potential for follow-on investigations or litigation may drive the company's decision-making on the format and structure of final reporting. Whatever form it takes, the report should typically address the issues and allegations involved, the company's investigative process, key findings, and any recommended remedial action. If the company intends to preserve privilege, distribution of any written report should be limited so as to avoid privilege-waiver risk. If necessary, the company also should carefully consider the potential pros and cons of disclosing the mere existence of any final report. Such disclosure is likely to increase pressure and litigation around disclosing the final report itself.

TO DISCLOSE OR NOT TO DISCLOSE

Once an internal investigation is complete, the company may be in the position of needing to determine whether to disclose the investigative results to any number of stakeholders. Assuming disclosure is not required under U.S. or other applicable laws, the decision whether to notify the government, other third parties, or the public at large of investigative results will require a highly nuanced analysis.

In the case of potentially criminal conduct, additional disclosure guidance may be forthcoming from DOJ. While some DOJ components have existing policies that provide significant incentives for companies that voluntarily self-disclose criminal conduct, Deputy Attorney General Lisa Monaco recently issued a Memorandum directing each DOJ component that prosecutes corporate crime to adopt and publicly share a policy that incentivizes voluntary disclosures. Monaco's Memorandum states, among other things, that these policies should require that, absent aggravating factors, DOJ components will not seek a guilty plea from a company where the company has voluntarily self-disclosed, fully cooperated, and timely and appropriately remediated the misconduct.

Another *White Paper* in this series will cover in greater detail various considerations in the self-disclosure analysis. If a company decides to self-disclose, it should do so as part of a comprehensive strategy for dealing with the relevant governmental authorities that would include cooperating with the authorities' future requests, and also for other consequences that could flow from the self-disclosure (e.g., potential administrative penalties and civil litigation).

PRIVILEGE AND DISCLOSURE/COOPERATION CONSIDERATIONS

Under some circumstances, disclosing information about an internal investigation may result in waiver of the privilege over the subject matter at issue. There may be reason to waive

privilege at the conclusion of an investigation—for example, when a company is indisputably the victim of criminal conduct or when a company is in settlement negotiations with a government agency and wishes to better position itself for cooperation credit through the disclosure of factual information that might otherwise be privileged. Companies should keep in mind, however, that a privilege waiver in response to a government investigation may be interpreted as a waiver regarding the same subject matter in other legal proceedings—whether an investigation by another government agency, civil enforcement action, or litigation by a private plaintiff.

Historically, DOJ and SEC considered a company's willingness to waive privilege over investigation materials as one factor of cooperation credit to be considered in charging and penalty decisions.[6] But under current DOJ guidance, prosecutors are prohibited from explicitly requesting the waiver of "core" attorney-client or attorney work product materials, or from crediting corporations that do waive privilege with respect to that type of information.[7] The SEC Enforcement Manual similarly discourages any explicit requests for a privilege waiver.[8]

As with disclosure more generally, companies and their counsel should undertake a fact-specific evaluation as to the risks and benefits of disclosing privileged attorney-client communications and work product created throughout the course of an investigation.

CONCLUSION

While the precise steps and scope of an internal corporate investigation will depend on the specific facts and circumstances presented, it will almost always be necessary to respond quickly to allegations of misconduct, craft a thorough and precise work plan, identify and address legal issues specific to any relevant non-U.S. jurisdictions, take steps to maintain privilege by involving counsel from the outset, and quickly preserve documents for potential collection. These steps, in combination with effective witness interviews, any appropriate remediation, and a documentary record that sufficiently memorializes the corporate response to the allegations, will best position the company with respect to any future legal action and reinforce the company's commitment to ethical and lawful conduct.

LAWYER CONTACTS

Theodore T. Chung
Chicago
+1.312.269.4234
ttchung@jonesday.com

Henry Klehm III
New York
+1.212.326.3706
hklehm@jonesday.com

Kendra L. Marvel
Los Angeles
+1.213.243.2366
kmarvel@jonesday.com

Leigh A. Krahenbuhl
Chicago
+1.312.269.1524
lkrahenbuhl@jonesday.com

Karen P. Hewitt
San Diego
+1.858.314.1119
kphewitt@jonesday.com

Hank Bond Walther
Washington
+1.202.879.3432
hwalther@joneday.com

Sion Richards
London
+44.20.7039.5139
srichards@jonesday.com

Sheila L. Shadmand
Dubai
+971.4.709.8408
slshadmand@jonesday.com

Bénédicte Graulle
Paris
+33.1.56.59.46.75
bgraulle@jonesday.com

Cristina Pérez Soto
Miami/New York
+1.305.714.9733/+1.212.326.3939
cperezsoto@jonesday.com

Dr. Thomas Preute
Düsseldorf
+49.211.5406.5569
tpreute@jonesday.com

Peter J. Wang
Hong Kong/Shanghai
+852.3189.7211
pjwang@jonesday.com

ADDITIONAL CONTACTS

United States

Bethany K. Biesenthal
Chicago
+1.312.269.4303
bbiesenthal@jonesday.com

Scott W. Brady
Pittsburgh
+1.412.394.7233
sbrady@jonesday.com

Yvonne W. Chan
Boston
+1.617.449.6914
ychan@jonesday.com

Toni-Ann Citera
New York
+1.212.326.3454
tcitera@jonesday.com

Roman E. Darmer
Irvine
+1.949553.7581
rdarmer@jonesday.com

Richard H. Deane Jr.
Atlanta
+1.404.581.8502
rhdeane@jonesday.com

David J. DiMeglio
Los Angeles
+1.213.243.2551
djdimeglio@jonesday.com

Anders Folk
Minneapolis
+1.612.271.8923
afolk@jonesday.com

Louis P. Gabel
Detroit
+1.313.230.7955
lpgabel@jonesday.com

Rasha Gerges Shields
Los Angeles
+1.213.243.2719
rgergesshields@jonesday.com

Harold K. Gordon
New York
+1.212.326.3740
hkgordon@jonesday.com

Fahad A. Habib
San Francisco
+1.415.875.5761
fahabib@jonesday.com

Justin E. Herdman
Cleveland
+1.216.596.7113
jherdman@jonesday.com

Brian Hershman
Los Angeles
+1.213.243.2445
bhershman@jonesday.com

Adam Hollingsworth
Cleveland
+1.216.586.7235
ahollingsworth@jonesday.com

Samir Kaushik
Dallas
+1.214.969.5092
skaushik@jonesday.com

Kathy Keneally
New York
+1.212.326.3402
kkeneally@jonesday.com

James T. Kitchen
Pittsburgh
+1.412.394.7272
jkitchen@jonesday.com

Andrew E. Lelling
Boston
+1.617.449.6856
alelling@jonesday.com

James P. Loonam
New York
+1.212.326.3808
jloonam@jonesday.com

Barbara Mack Harding
Washington
+1.202.879.4681
bharding@jonesday.com

Rebecca C. Martin
New York
+1.212.326.3410
rcmartin@jonesday.com

Jordan M. Matthews
Chicago
+1.312.269.4169
jmatthews@jonesday.com

Shireen Matthews
San Diego
+1.858.314.1184
shireenmatthews@jonesday.com

Yvette McGee Brown
Columbus/ Cleveland
+1.614.281.3867/+1.216.586.7055
ymcgeebrown@jonesday.com

Joan E. McKown
Washington
+1.202.879.3647
jemckown@jonesday.com

Colleen Noonan Ryan
New York
+1.212.326.3444
cnryan@jonesday.com

Cheryl L. O'Connor
Irvine
+1.949.553.7505
coconnor@jonesday.com

Brian C. Rabbitt
Washington
+1.202.879.3866
brabbitt@jonesday.com

Jeff Rabkin
San Francisco/Silicon Valley
+1.415.875.5850/+1.650.729.3954
jrabkin@jonesday.com

Ronald W. Sharpe
Washington
+1.202.879.3618
rsharpe@jonesday.com

Erin Sindberg Porter
Minneapolis
+1.612.217.8926
esindbergporter@jonesday.com

Mary Ellen Powers
Washington
+1.202.879.3870
mepowers@jonesday.com

Evan P. Singer
Dallas
+1.214.969.5021
epsinger@jonesday.com

Sidney Smith McClung
Dallas
+1.214.969.5219
smcclung@jonesday.com

Stephen G. Sozio
Cleveland
+1.216.586.7201
sgsozio@jonesday.com

Neal J. Stephens
Silicon Valley
+1.650.687.4135
nstephens@jonesday.com

Edward Patrick Swan Jr.
San Diego
+1.858.703.3132
pswan@jonesday.com

Jason S. Varnado
Houston
+1.832.239.3694
jvarnado@jonesday.com

Alexander J. Wilson
New York
+1.212.326.8390
alexanderwilson@jonesday.com

Kristin K. Zinsmaster
Minneapolis
+1.612.217.8861
kzinsmaster@jonesday.com

Europe

José Bonilla
Madrid
+34.91.520.3907
jbonilla@jonesday.com

Adam R. Brown
London
+44.20.7039.5292
abrown@jonesday.com

Glyn Powell
London
+44.20.7039.5212
gpowell@jonesday.com

Ansgar Rempp
Germany
+49.211.5406.5500
arempp@jonesday.com

Paloma Valor
Madrid
+34.91.520.3903
pvalor@jonesday.com

Rick van 't Hullenaar
Amsterdam
+31.20.305.4223
rvanthullenaar@jonesday.com

Middle East and Africa

Heather Martin
Dubai
+971.4.709.8484
hmartin@jonesday.com

Asia and Australia

Stephen J. DeCosse
Tokyo
+81.3.6800.1819
sdecosse@jonesday.com

Steven W. Fleming
Sydney
+61.2.8272.0538
sfleming@jonesday.com

Lillian He
Shanghai
+86.21.2201.8034
lhe@jonesday.com

Jerry C. Ling
San Francisco/Shanghai
+1.415.875.5890
jling@jonesday.com

Hiromitsu Miyakawa
Tokyo
+81.3.6800.31828
hmiyakawa@jonesday.com

Daniel Moloney
Melbourne
+61.3.9101.6828
dmoloney@jonesday.com

Zachary Sharpe
Singapore
+65.6233.5506
zsharpe@jonesday.com

Simon M. Yu
Taipei
+886.2.7712.3230
siyu@jonesday.com

Latin America

Luis Riesgo
São Paulo
+55.11.3018.3939
lriesgo@jonesday.com

Guillermo E. Larrea
Mexico City
+52.55.3000.4064
glarrea@jonesday.com

Fernando F. Pastore
São Paulo
+55.11.3018.3941
fpastore@jonesday.com

Brittany N. Wilhelm, an associate in the Cleveland Office, contributed to this White Paper.

ENDNOTES

1 https://www.jonesday.com/en/insights/2022/09/doj-announces-major-changes-to-corporate-criminal-enforcement-policies.

2 An initial step in the investigation of a whistleblower complaint is ordinarily to seek to engage with, and obtain additional information from, the whistleblower (e.g., any relevant documents in the whistleblower's possession and/or information the whistleblower would share in an interview).

3 It should be noted that, in recent years, as whistleblower rewards have become larger and more prominent (and an industry of private law firms representing anonymous whistleblowers emerged), a flood of corporate misconduct allegations have been sent directly to regulators, at times bypassing internal corporate reporting mechanisms altogether. For example, since 2020, the SEC has reported a significant increase in whistleblower tips compared to prior years. In its 2021 Annual Report to Congress regarding the SEC whistleblower program, the SEC disclosed that it received more than 12,200 whistleblower tips in fiscal year 2021—the largest number of tips received by the agency in any given year. This also represents a 76% increase from the number of tips that the SEC received in 2020. Whistleblower tips specifically related to the Foreign Corrupt Practices Act ("FCPA") also increased in 2021 with 258 FCPA-related tips in fiscal year 2021, a 24% increase compared to 2020 and the highest number of tips that the SEC has received in *any* given year. 2021 Annual Report to Congress, Whistleblower Program, SEC (2021), https://www.sec.gov/files/owb-2021-annual-report.pdf. The SEC reports on significant rewards, issuing millions to individual whistleblowers from settlements. See, e.g. *SEC Press Release, SEC Issues More than $17 Million Award to a Whistleblower* (July 19, 2022), https://www.sec.gov/news/press-release/2022-125.

4 In June 2020, for example, DOJ published an update to its guidance addressing the "Evaluation of Corporate Compliance Programs," which includes a number of considerations for prosecutors making charging decisions; such as, what steps the company took to ensure that the investigation was independent, objective, appropriately conducted, and properly documented. This guidance has been under further review since 2021 as the new administration seeks to streamline and clarify the "metrics" for evaluating the effectiveness of corporate compliance programs. *See* Monaco Memorandum (Sept. 15, 2022, https://www.justice.gov/opa/speech/file/1535301/download.

5 *See* Monaco Memorandum, September 15, 2022, p. 11, available at https://www.justice.gov/opa/speech/file/1535301/download.

6 *See, e.g. Memorandum from Eric H. Holder, Deputy Att'y Gen., U.S.Dept. of Justice, to All Component Heads and United States Attorneys,* (June 16, 1999) (DOJ would consider a company's "willingness to cooperate in the investigation of its agents, including, if necessary, the waiver of the corporate attorney-client and work product privileges."); *Securities and Exchange Commission, 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*, Release No. 44969 (Oct. 23, 2001); *Memorandum from Paul J. McNulty, Deputy Att'y Gen., U.S. Dept. of Justice, to Heads of Department Components, United States Attorneys* (Dec. 12, 2006) (DOJ attorneys could request a waiver only when there was a legitimate need for the privileged information).

7 *Memorandum from Deputy Att'y Gen., U.S. Dept. of Justice, to Heads of Department Components, United States Attorneys* (Aug. 28, 2008).

8 SEC Enforcement Manual, http://sec.gov/divisions/enforce/enforcementmanual.pdf.