JONES DAY | One Firm Worldwide®

WHITE PAPER

December 2022

Corporate Internal Investigations: Keys to an Effective Work Plan, Data and Document Management, and Budget

As described in the first White Paper in this series on internal investigations, "Conducting an Effective Internal Investigation—An Overview," corporations are under increased scrutiny by regulators across the globe, and as a result, it is more important than ever for companies to conduct an effective, defensible internal investigation when allegations of misconduct arise. An effective internal investigation allows companies to proactively examine the facts and assess any associated legal, financial, and reputational risks, whether or not a related government investigation or civil litigation is underway or anticipated.

But investigation costs can escalate quickly, especially with investigations that cover a significant period of time and/or territory, or that involve conduct that may potentially expose the entity or individuals to criminal penalties or significant civil liability. A work plan and budget are key to both ensuring a thorough investigation and managing investigation costs.

This *White Paper* summarizes considerations for creating an effective work plan for an internal investigation, successfully managing the collection and production of data and documents, and planning for the categories of expenses that typically arise in an internal investigation. We also offer guidance on how to budget for each line-item. Although each work plan and budget will necessarily vary in its components and costs, the categories described below should be considered when setting the work plan and budget in virtually every corporate internal investigation.[1] We conclude by offering a "checklist" of issues and tasks to consider in preparing an effective work plan, managing data and documents, and formulating an investigation budget.

TABLE OF CONTENTS

INVESTIGATION WORK PLANS

A detailed investigation work plan is a key initial step for conducting a thorough and efficient internal investigation. At inception, an investigation work plan should cast a sufficiently wide net, identifying all known avenues for fact development. The work plan should identify the scope and objectives of the investigation, including the issues and types of conduct to be investigated and the persons understood to be involved in the conduct. The principal components of a comprehensive work plan include: (i) objectives of the investigation; (ii) anticipated scope (i.e., allegations and issues to be investigated); (iii) identification of team members; (iv) tasks to be completed, including the data and documents to be reviewed, witnesses to be interviewed, any financial analysis to be conducted, and any required legal research; and (v) responsibility among team members for such tasks.

The work plan should include whether the investigation will be structured to be protected by attorney-client privilege or work product protections. It should address any interim or final reporting that is expected, even if the form of any final report is not certain. Additionally, the work plan should identify any required engagement with third parties, such as company auditors, the board of directors or the audit committee, government regulators, employees' counsel or representatives, contractors or vendors, and the company's insurance carriers (to the extent that any portion of the investigation, or any loss resulting from the conduct being investigated, may be covered by the company's insurance policies). A checklist of suggested items to include in a work plan can be found at the end of this section.

After a work plan is developed, it should be reevaluated on a regular basis and modified as appropriate while the investigation progresses to incorporate new information and developments in the investigation strategy. Periodic communication about the work plan is vital since the urgency of an investigation often means the various components of the work plan occur simultaneously, and adjustments to one component may require corresponding adjustments to other areas of the work plan (e.g., the addition of a witness to the interview list may require changes to the document collection and review portion of the work plan). The work plan should track the budget.

DATA AND DOCUMENT MANAGEMENT

Document preservation, collection, review, and management are key components of conducting an internal investigation. Even if a government regulator or plaintiff's counsel has not sought documents by subpoena or via document requests, reviewing documentary evidence related to the alleged conduct is crucial to gathering relevant facts and analyzing potential outcomes. Managing data and documents as part of an investigation may involve a large number of tasks, including identifying custodians and other potential sources of material (e.g., company servers, shared drives, documents stored in the cloud); conducting custodial interviews; coordinating with in-house IT teams to collect documents; arranging for document preservation; determining a method to store, host, and review data; processing data and running search terms; reviewing the documents themselves; and identifying key documents related to the conduct at issue. In addition, documents may need to be produced to regulators or summarized for internal client stakeholders. A checklist of items to keep in mind related to data and document management can be found at the end of this *White Paper*.

Document Preservation

The first step in managing documents in an investigation is identifying where relevant documents are located and preserving those documents. Particularly at the outset of an investigation, it is important to consider the confidentiality of the investigation. The investigation team should work with corporate IT to identify back-end mechanisms for preserving and collecting electronically stored information ("ESI"), including disabling automatic deletions and preserving all relevant information that can be accessed by IT personnel remotely (e.g., emails or other documents stored in the cloud). The investigation team might also review organizational charts for the time period at issue, corporate document storage and retention policies, and other corporate records, such as personnel files, in order to identify relevant custodians and categories of information.

Corporate employees with potentially relevant documents should receive a litigation hold notice as early in the

investigation as advisable, typically in conjunction with, or soon after, back-end mechanisms for ESI preservation have been deployed. An effective litigation hold should be comprehensive and easily understood by employees and should instruct recipients not to delete any documents relevant to the investigation. A litigation hold notice should provide general background on the reason for document preservation and give broad, but clearly defined, categories of information to be preserved. If a subpoena, government request, or discovery request is involved, the hold notice should ensure that all categories of the subpoena or requests are fully covered by the hold notice. Companies should be mindful that issuing a hold notice may trigger insurance coverage notification obligations.

Before collecting documents, the attorneys leading the investigation should consider whether an external discovery vendor is needed to capture, host, and, if necessary, produce the collected data and documents. In deciding whether to engage an external vendor, in addition to the costs of the vendor, companies should consider in-house capacity for document hosting, review, and processing; whether vendors have the necessary expertise to handle all necessary tasks; the complexity of the investigation and the underlying collection; and whether production of documents to third parties is anticipated. In circumstances where the volume of documents is substantial, there are particular technology issues or needs, or the collection is especially complex, an external vendor can often streamline the collection, review, and production process and allow for scoping changes, if necessary, as the investigation develops. The vendor should work at the direction of outside counsel to preserve attorney-client privilege and work-product protections.

Document Collection and Custodian Interviews

Once data on company systems has been preserved, the next step is usually to preserve and collect devices and documents that cannot be collected remotely. Such collection should be done as early in the investigation as practicable but may not be executed until: (i) any related requirements under applicable labor and/or data privacy laws have been met; and (ii) the company is ready to disclose to witnesses that an investigation is ongoing.

Depending on the nature and complexity of the misconduct alleged, custodian interviews with individuals identified as potentially having relevant documents may be an important step in document collection. Many companies have a form used for custodian interviews, but it should be reviewed prior to use in particular instances to ensure it is tailored to the needs and objectives of the investigation. During the interview, custodians should be asked about their document and record-keeping practices, the types and locations of devices utilized, and where relevant data and documents are located. Consider asking the custodian about the following topics:

- Use of work or personal computers or other devices (mobile phone, tablet, etc.);
- Foldering, archiving, and deletion practices;
- Location of relevant documents used or created by the custodian (My Documents, shared drive, cloud storage, hard copy);
- Use of work or personal email addresses;
- Use of work or personal calendars; and
- Use of text messages, chats, or other instant messaging programs.

For investigations where mobile data may be relevant, it is particularly important to understand whether the custodian uses a personal mobile device or a company-owned mobile device for work purposes. Investigators should consider corporate policies concerning mobile devices (e.g., Bring Your Own Device ("BYOD") policies), as well as any data privacy laws in the relevant jurisdictions, to determine whether there are prohibitions or limitations on the collection of personal mobile data. Another White Paper in this series will address the complex issue of data privacy and cross-border transfers of data in the context of investigations.

As the investigation continues and additional information is learned, investigators should consider whether to add additional custodians or other sources of documents. Testing search terms or collecting a sample of a custodian's files can help determine the cost-effectiveness and substantive value of adding the individual as a custodian before doing so.

After relevant documents and data are collected, they will need to be processed and loaded to the agreed-upon database or review platform.

Tools for Efficient Document Review

Once data is collected, the process of narrowing the universe of documents for review can begin. An important consideration in determining the scope of the document review universe is the purpose of the review (e.g., whether the review is being conducted in response to a government subpoena or a document request or as a fact-finding exercise in an internal investigation). If documents are being reviewed in response to a government subpoena, for example, investigators will generally have less discretion in determining the scope of the review. In internal investigations, outside counsel should work with company contacts to determine the most cost-efficient means of obtaining the salient facts through document review.

Some of the methods used to make a document review more efficient include use of search terms and/or date ranges, deduplication, and use of technology-assisted review ("TAR"). Search terms and date-range limitations are the most common methods for culling data before review. Both can be critical for narrowing the scope of a document review and should be developed with input from the company, including in-house counsel and, where appropriate, key employees. If government regulators are involved in the investigation, consider discussing and negotiating search terms and date ranges to be used with government attorneys. Doing so can be useful to obtaining cooperation credit and ensures that the government and company are aligned with respect to the scope of document collection and review. In some instances, the government will also ask to review the hit report to understand which terms were most productive in yielding documents. Developing and running search terms can often be an iterative process, as terms that yield a large number of irrelevant documents, or "false hits," may be removed or fine-tuned.

Another method to decrease the volume for review is deduplication, which involves cross-referencing documents that appear in multiple custodians' data sets and removing those documents that appear more than once. This process can significantly reduce the number of documents that must be reviewed and produced.

Finally, in some investigations, TAR may allow the investigation team to find and review the most significant documents early in the investigation, without conducting a front-to-back review. TAR technology uses machine-based processes and algorithms to identify potentially relevant documents. TAR is most effective in investigations involving a core set of highly relevant documents, which can then be used to "teach" the technology what to look for in potentially relevant documents.

Document Review Procedures

Prior to beginning document review, it is important to determine: (i) the protocol for reviewing the documents; (ii) who will review the documents; and (iii) the goal of the review, whether it is investigative fact-finding, preparation for witness interviews, or production to regulators.

A review protocol is a written set of procedures to provide an overview of the subject matter and clear, detailed instructions

for how to review and code documents based on their relevance, significance, and any other necessary categories. Investigators should consider adding issue tags or codes that track with themes of the investigation in order to keep documents organized and to help prepare for witness interviews, government presentations, or responding to production requests. If production to third parties is anticipated, privilege and work product tags should be utilized in order to ensure privileged material is identified and protected. Investigators should obtain a list of in-house and external counsel, as well as other company-specific privilege terms, to assist in conducting any required privilege review. Confidentiality tags may be useful for certain documents, such as sensitive financial records. A "significant" or "key" tag will also be helpful for identifying the most important documents.

Any attorneys that are participating in the review should be trained in order to ensure they have sufficient background on the investigation and can spot relevant and significant documents. The investigation team should ensure that there is a clear process for escalating questions and ensuring consistency among reviewers. Outside counsel should provide training consistent with the review protocol and to maintain privilege, and outside counsel should also lead quality control.

Many investigations call for consideration of whether to utilize contract attorneys or outside counsel associates to review the documents. Contract attorneys are generally less expensive than outside counsel, may possess foreign language capabilities that go beyond those of outside counsel associates, and are often available to mobilize quickly on a large scale, allowing for the review to proceed quickly and efficiently. Contract attorneys frequently conduct a first-level review, with outside counsel performing a second-level review of relevant and significant documents and quality-control checks. This ensures that the lowest billing rates are assigned the higher volume of document review work, increasing cost efficiencies. It also ensures that outside counsel, who will be most familiar with the underlying facts and issues, have substantial oversight.

Reviewers should be monitored on a regular basis to ensure that the review is proceeding on pace and that questions are addressed promptly.

CONSIDERATIONS FOR MOBILE DATA AND INSTANT MESSAGES

Data contained on mobile devices or in temporary mediums, such as instant messages, present unique challenges to the investigative process. However, it is increasingly common for government regulators and plaintiffs' counsel to include mobile data and instant messages in subpoenas and document requests. Further, recent DOJ guidance suggests that collection and production of all relevant, nonprivileged documents, including text messages and instant messages, will be a factor in assessing a company's cooperation.[2] Additionally, such data may be key to developing the facts in an internal investigation.

Mobile Data

A company's corporate use or BYOD policies can impact whether mobile data may be relevant or accessible in an internal investigation, as does local law. As noted above, potential document custodians should be asked about whether they use a mobile device for work purposes and, if so, whether the device is personally owned or employer-provided. Investigators should review the company's corporate use policies and local data privacy law to determine whether there are any limitations on the collection and review of mobile device data.

Additional factors to consider in determining whether to collect a particular custodian's mobile data include the custodian's role in the investigation; the custodian's use of the mobile device for work purposes, particularly with respect to text messages or messaging apps; and whether the mobile device syncs with the custodian's work email or computer, which may impact the availability of data. Investigators should balance these considerations in determining whether to collect mobile data. If a custodian utilizes text messages for work-related purposes, it may be appropriate to collect and review those. However, where a custodian utilizes a mobile device in a limited capacity, it may not be cost-effective to collect and review the data. Management or employees implicated in the allegations being investigated may be good candidates for mobile data collection.

Instant Messages

For instant messages or chats, attorneys should work with in-house IT to determine the applicable retention process and policies. If instant messages are regularly retained by the company, potentially relevant messages should be preserved, as they are frequently included in subpoenas issued by regulators. In determining whether to collect and review instant messages, consider what type of content is available in instant messages and whether that content is likely relevant to the investigation. Employees may speak more informally in instant messages than in email, and therefore instant messages may be an important source of relevant information, depending on the subject of the investigation.

INVESTIGATION BUDGETS

To control costs without compromising the fundamental objectives of the investigation, it is frequently beneficial to develop a budget at the outset of the investigation. Based on the best available information at the time, the initial budget should make appropriate assumptions about factors that will influence costs and assign reasonable and realistic cost projections to the tasks that are expected to comprise the overall work plan. As such, counsel should consider a number of issues when preparing the budget, including:

- The scope and objectives of the investigation, as outlined in the work plan;
- The complexity of the investigation, including whether there is an international component; whether government regulators are involved; whether third-parties, such as vendors, are implicated; and any novel legal issues presented;
- The number of document custodians and witness interviews (both of which may expand during the course of the investigation);
- The magnitude of the data preservation and collection effort and associated storage costs, including costs for an e-discovery vendor, if applicable;
- Document review costs, including for the document review platform, the potential use of TAR or contract reviewers, and whether foreign language reviewers or translations will be required;
- Witness interview preparation and execution costs, including whether interviews will be conducted in person or remotely and whether foreign language translators will be required;
- The time associated with preparing investigative materials and coordination among investigation team members and with the client;
- Any need for subject-matter experts (e.g., forensic accountants, computer forensic experts, local counsel, etc.);
- Any anticipated reporting obligations to the board of directors, regulators, external auditors, or other stakeholders; and
- The costs of identifying and implementing any remedial measures or resolving personnel issues.

While developing a budget necessarily involves at least some measure of estimation, and may not be appropriate for every situation, investigators and clients frequently find budgeting helpful for understanding how certain variables inherent in the investigative process, such as scope, timing, and resources, might influence the overall cost of the investigation. Budgeting also facilitates communication between counsel and client about the client's specific objectives. A checklist of proposed budget items, as well as tips for containing costs, are contained at the end of this *White Paper*.

Once developed, the budget should be reviewed and updated regularly throughout the investigation. As the investigation proceeds, the initial assumptions and corresponding budgeted

amounts for each task can be re-evaluated and modified as appropriate based on any changes to the work plan or any unforeseen developments.[3]

Witness Interviews

Witness interviews are critical to fact-finding in almost all internal investigations, and an effective budget accounts for the costs of preparing for, attending, and memorializing the interviews. Scoping interviews typically occur early and are primarily intended to discover basic facts, other sources of relevant information, and the nature and extent of the witness's own knowledge. These interviews typically require less preparation than substantive interviews, which are often completed after document review and may involve asking the witnesses about particular documents. Intensive preparation is typically required for key substantive interviews because such interviews are critical to developing a comprehensive understanding of the conduct under investigation.

The budget should reflect: (i) the anticipated number of scoping and substantive interviews; (ii) the total time expected to be devoted to preparation for, participation in, and memorialization of the interviews; and (iii) whether the interviews will take place via a web-conference platform or in-person. The use of web-conference platforms for witness interviews—which has increased substantially in the wake of COVID-19 and the corresponding increase in remote work—has the potential to save clients thousands of dollars and a significant amount of time. Nevertheless, it may be more effective to interview some witnesses—including subjects of the investigation or witnesses requiring the use of a translator—in person.

Forensic Accounting Support and Subject-Matter Experts

The budget should account for potential costs of involving other professionals and subject-matter experts in the investigation, such as forensic accountants and computer forensic experts. Forensic accountants assist in reviewing accounting or financial information, identifying potentially problematic transactions, analyzing the accounting treatment accorded thereto, and in reviewing internal controls. Forensic accountants may also assist with witness interviews, particularly where the witness is an accountant or the interview involves technical accounting issues. Forensic accountants and subject-matter experts should be asked to prepare their own budgets in consultation with other members of the investigative team, consistent with the same principles and approach used in setting the overall investigation budget.[4]

Reports and Recommendations

Preparing reports and recommendations and meeting with key stakeholders, including regulators, the board of directors, outside auditors, or other outside counsel (e.g., the company's securities disclosure counsel and counsel for individual employees), are often key elements to conducting and concluding an internal investigation. An effective budget should account for costs associated with these activities. Key budgeting considerations include: (i) the frequency and nature of the reporting; (ii) the time and resources required to prepare expected work product; and (iii) any potential follow-up items, including considerations related to self-reporting to regulatory authorities, if applicable.

Remediation and Personnel Matters

To the extent the investigative team is expected to be involved, the budget should also account for the costs of identifying, analyzing, and implementing remediation measures related to

any wrongdoing uncovered, including enhancements to the corporate ethics and compliance program, if applicable. In addition, personnel-related costs should also be included in the budget. These may consist of, for instance, time devoted by the investigative team: (i) in connection with the discipline, coaching, or retraining of employees; and (ii) to work with any counsel for or representatives of individual directors, officers, or employees.

TIPS FOR CONTAINING COSTS

Through some basic steps, those managing internal investigations can instill appropriate discipline on the investigative process, and the organization as a whole can expect reasonable certainty as to budget projections. Below are suggested tips to consider for containing investigative costs.

- Consider the potential advantages and disadvantages of engaging outside resources such as outside counsel, forensic accountants, and computer forensic experts. Depending on the circumstances, and assuming the availability of sufficiently capable internal resources, cost-savings may be achieved by foregoing some or all outside resources. However, cost-savings should not be dispositive in preparing a budget for an internal investigation. The analysis should also involve a careful assessment of the nature and scope of the issues under investigation, the benefits of independent work product from outside resources, and privilege issues.
- Have in place, and enforce, clear billing guidelines that cover, among other things, the manner in which outside professionals are to record time and expenses and the items for which billing is (and is not) permitted.
- Investigate in phases—identify priorities and key tasks at the outset of each phase, and ensure that the learning from one phase is considered when planning and budgeting for successive phases.
- Conduct scoping interviews early to understand the location of potentially relevant documents, data, and witnesses, and to protect against chasing what could be readily identified as false leads.
- Set priorities for ESI collection and review, and, if possible, stagger the review such that decisions about whether to collect and review additional ESI can be made on a rolling basis and unnecessary ESI work can be avoided.
- Similarly, leverage scoping interviews and information learned from ESI review to prioritize and carefully sequence witness interviews to avoid unnecessary or duplicative interviews.
- Use targeted search terms for ESI review and consider a database vendor that offers "predictive coding."
- Consider using contract attorneys—with appropriate training and supervision—for first-level ESI review.
- Obtain periodic budget reports (e.g., time incurred versus budget).
- Frequently (re)evaluate the scope and breadth of the investigation (e.g., performing a "sampling" approach, instead of reviewing all potentially relevant events or transactions, is often sufficient, as not all allegations of a possible violation of law or company policy necessarily merit the devotion of significant investigative time and effort).
- Consider the nature and extent of periodic substantive reporting on interviews and investigative findings or observations, balancing the need for information flow with the costs involved.
- Consider options on final substantive reporting from a cost perspective[5] (e.g., a narrative summary or slide deck, in lieu of the typically more expensive narrative report).

CONCLUSION

A thorough work plan, which includes all of the anticipated tasks and deliverables, is an essential tool for conducting an effective investigation. Preserving, collecting, and reviewing data and documents can be one of the most time-consuming and expensive aspects of an investigation; however, investigators and companies can more efficiently manage even large volumes of documents and data with early planning and thoughtful consideration of the issues discussed in this White Paper. Finally, preparation of a detailed budget, which includes line items for all of the tasks and deliverables identified in the work plan, allows investigators and companies to more accurately project and manage costs as the investigation progresses.

CHECKLISTS

Items to Include in a Work Plan

- Goal(s) of the investigation
- Anticipated scope of the investigation
- Team members involved and roles
  - Outside counsel
  - In-house counsel and staff
  - Third parties (if/as necessary), including e-discovery vendor, forensic accountants, and contract attorneys
- Communication protocols
  - Means and frequency of communication between outside counsel and client points of contact
- Division of responsibilities and determination of whether the investigation will be structured to be protected by attorney-client privilege or work product protections
- Key categories of investigation tasks
  - Document preservation and collection
  - Document review and production
  - Legal research
  - Fact development
  - Witness interviews
  - Meetings and communications regulators and investigators
  - Expert analysis
  - Third-party work, including forensic accountant review and analysis, document collection and production
  - Reporting to client and other stakeholders
  - Insurance coverage, claims, and recovery
  - Remediation
- Deliverables
  - Investigation presentation and client report on findings
  - Witness interview materials, including outlines and documents
  - Witness interview memoranda and/or summaries
  - White papers or presentations to regulators
  - Document productions
- Potential outcomes
  - Internal remedial measures related to employees or vendors, such as termination (of employment or of the vendor's contract); disciplinary measures; additional compliance training or retraining of employees, etc.
  - Enhancements to the company's ethics and compliance program
  - Internal or external audits
  - Self-reporting to regulators
  - Further investigation by regulators
  - Settlement with regulators, including payment of fine or ongoing monitoring

Data and Document Management Checklist

- Document preservation
  - Coordinate with corporate IT personnel to preserve documents and suspend deletion practices
  - Review organizational charts and corporate policies related to mobile device usage and retention
  - Conduct scoping interviews to determine potential custodians and record sources
  - Decide on engaging external discovery vendor
  - Distribute litigation hold
- Document collection
  - Conduct custodian interviews
  - Capture and process data from identified custodians and document sources (e.g., ESI, hard drives, mobile devices, hard-copy files)
- Document review and production
  - Assess methods for narrowing data set
    - Search terms and date ranges (in coordination with client and regulators)
    - De-duplication
    - Technology-assisted review

- Determine who will review documents
  - In-house attorneys
  - Contract attorneys
  - Outside counsel
- Draft review protocol
- Train first-level document reviewers and establish processes to answer questions promptly and quality control checks
- Conduct first- and second-level review and quality control checks
- Identify and track key documents
- Identify privileged documents and log on privilege log
- Produce documents to regulators in connection with a request or subpoena, if applicable
- Summarize documents for client or for presentation to stakeholders, if applicable

Budget Checklist

- Scoping and planning
  - Initial fact gathering (including scoping interviews)
  - Legal research
  - Developing work plan
- Data preservation and collection
  - Litigation hold notice
  - ESI, hard drives, mobile devices, and servers
  - Hard-copy documents
- Document review
  - First- and second-level reviews, as well as any necessary quality control reviews
  - Training and monitoring
  - Review platform
  - Technology-assisted review
  - Foreign language reviewers
  - Translations
- Witness interviews
  - Preparation (outline, exhibits, etc.)
  - Foreign language translators
  - Web-conference vs. in-person
  - Travel expenses
  - Memorandum or summary memorializing interview
- Subject-matter experts
  - Forensic accountants
  - Computer forensic experts
  - Industry experts
- Reporting to the client and other stakeholders
  - Analysis and reporting to client and other stakeholders, including outside auditors
  - Potential government disclosure analysis
- Insurance
  - Coverage analysis
  - Claims and recovery
- Remediation
  - Compliance program and training
  - Personnel changes
- Personnel matters
  - Individual or pool counsel for personnel
  - Potential employee severance negotiations and parallel litigation

ENDNOTES

1 Alternative fee arrangements (e.g., flat fees or "success" fees) should be evaluated with great care in the context of corporate internal investigations and should generally be avoided if they may be reasonably viewed as inducing corner-cutting in the fact-gathering process or otherwise creating incentives inconsistent with the basic, truth-seeking objective of the investigation.

2 For more about the DOJ's recent guidance on mobile data and instant messages, see Jones Day *Commentary*, "DOJ Announces Major Changes to Corporate Criminal Enforcement Policies" (Sep. 2022).

3 To ensure protection under the attorney-client privilege and work-product doctrine, the investigation budget and supporting materials should clearly state that they have been prepared in anticipation of potential litigation and that the purpose of the investigation is to provide legal services and advice.

4 In attorney-client privileged investigations, external experts should be retained by counsel so as to maintain the privilege.

5 Note that other considerations may also influence the format of final substantive reporting (e.g., privilege concerns and concerns over maintaining confidentiality generally).

LAWYER CONTACTS

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

Erin Sindberg Porter
Minneapolis
+1.612.217.8926
esindbergporter@jonesday.com

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

Terri L. Chase
Miami / New York
+1.305.714.9722 / +1.212.326.8386
tlchase@jonesday.com

Sidney Smith McClung
Dallas
+1.214.969.5219
smcclung@jonesday.com

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

Elizabeth B. McRee
Chicago
+1.312.269.4374
emcree@jonesday.com

Sion Richards
London
+44.20.7039.5139
srichards@jonesday.com

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

Thomas Preute
Düsseldorf
+49.211.5406.5569
tpreute@jonesday.com

Bénédicte Graulle
Paris
+33.1.56.59.46.75
bgraulle@jonesday.com

Hank Bond Walther
Washington
+1.202.879.3432
hwalther@joneday.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

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

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

Roman E. Darmer
Irvine
+1.949.553.7581
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

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

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

Barbara Mack Harding
Washington
+1.202.879.4681
bharding@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

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

Leigh A. Krahenbuhl
Chicago
+1.312.269.1524
lkrahenbuhl@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

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

Kendra L. Marvel
Los Angeles
+1.213.243.2366
kmarvel@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

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

Mary Ellen Powers
Washington
+1.202.879.3870
mepowers@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

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

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

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

Evan P. Singer
Dallas
+1.214.969.5021
epsinger@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
+49.211.5406.5569
tpreute@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

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

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

Annie Leeks
Brisbane
+61.7.3085.7023
aleeks@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

Holly Sara
Sydney
+61.2.8272.0549
hsara@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

Rebecca E. Kline, associate in the Minneapolis Office, and Scott B. Scheinberg, associate in the Pittsburgh Office, contributed to this White Paper.