The Directors Roundtable Institute
October 21, 2015

KEY ISSUES FACING BOARDS OF DIRECTORS: CURRENT SEC ENFORCEMENT INITIATIVES AND CORPORATE GOVERNANCE RISKS

1. FTI Thought Leadership

   2015 Law In The Boardroom Study
   SEC's New Enforcement Mandate
   Why Compliance Is Good Business
   Internal Investigations: Revealing the Core of Corruption
   Managing Cyber Risk
   Countering the Growing Threat of Cyber Blackmail

2. Updated DOJ Guidelines On Individual Liability For Corporate Wrongdoing

3. SEC Flexes Its Muscle On Accounting Fraud And Targets More Individuals

4. Accounting Fraud: Down, But Not Out

5. Effectively Managing An Independent Investigation

6. Internal Investigations: Preparing An Effective Budget

7. Court Prevents Disclosure Of Internal Investigation Materials

8. SEC Brings Hiring Practices Into FCPA Focus

9. Best Practices On Dealings With Third Parties Under The FCPA

10. Panelists

Erin Schneider
Associate Regional Director and Head of Enforcement (San Francisco), U.S. Securities and Exchange Commission

Edward Westerman
Senior Managing Director, Forensic Accounting & Advisory Services, FTI Consulting

John Tang
Partner, Securities Litigation and SEC Enforcement Practice, Jones Day

ATLASADDENDUM

FTI CONSULTING

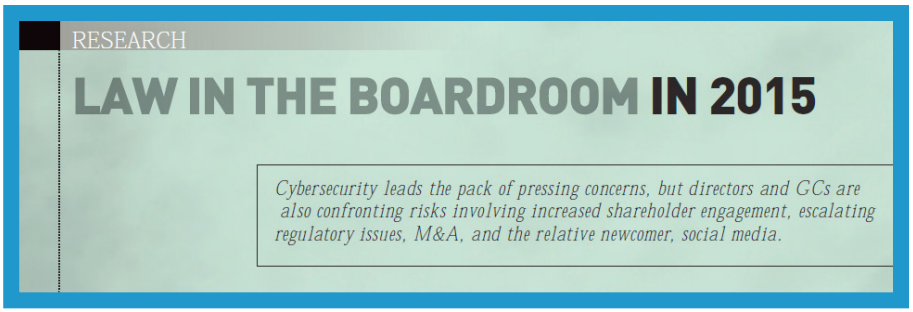
VOLUME XXIX

SPOTLIGHT

REPORT SPOTLIGHT:

2015 LAW IN THE BOARDROOM STUDY

FTI Consulting and NYSE Governance Services' 15th Annual Law in the Boardroom Study finds that IT and cybersecurity risks remain the top concern for directors and general counsel



On May 21st, FTI Consulting and NYSE Governance Services, a leading provider of corporate governance, risk, ethics and compliance services for public and privately held companies, released findings from this year's Annual Law in the Boardroom Study, which identifies key risks and legal trends for companies in 2015.

This year's study revealed that Information Technology ("IT") and cybersecurity risks remain the top concern for directors and general counsel. Other concerns cited in this year's survey are increased shareholder engagement, escalating regulatory issues, merger and acquisitions ("M&A") and social media.

According to this year's study, IT/cybersecurity is the number one worry for both directors and general counsel, with 90% of directors and 86% of general counsel indicating they are either extremely concerned or concerned about this issue. The study also found:

- 77% of both directors and general counsel believe that the cyber liability risk at their company has increased over the last two years
- 98% of directors and general counsel indicated that they do not have a high level of confidence that their companies are totally secure and impervious to hackers nor are they entirely confident that their company could quickly detect a cyber-breach
- 64% of directors and 77% of general counsel are at least somewhat confident their board knows the right questions to ask management about their company's cyber strategy
- 36% percent of directors stated that they were either extremely concerned or concerned about shareholder

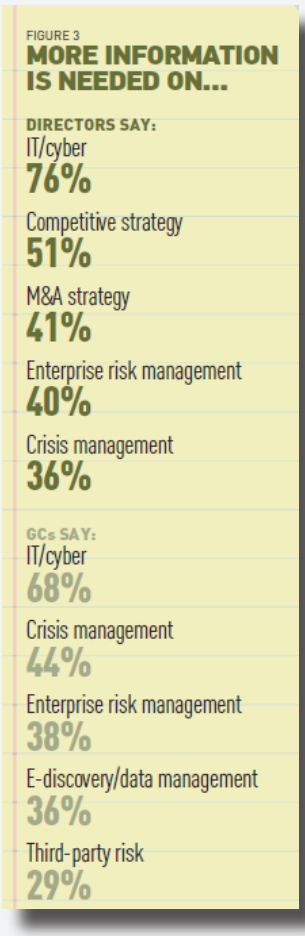
activism and litigation this year, while 43% of general counsel expressed the same levels of concern

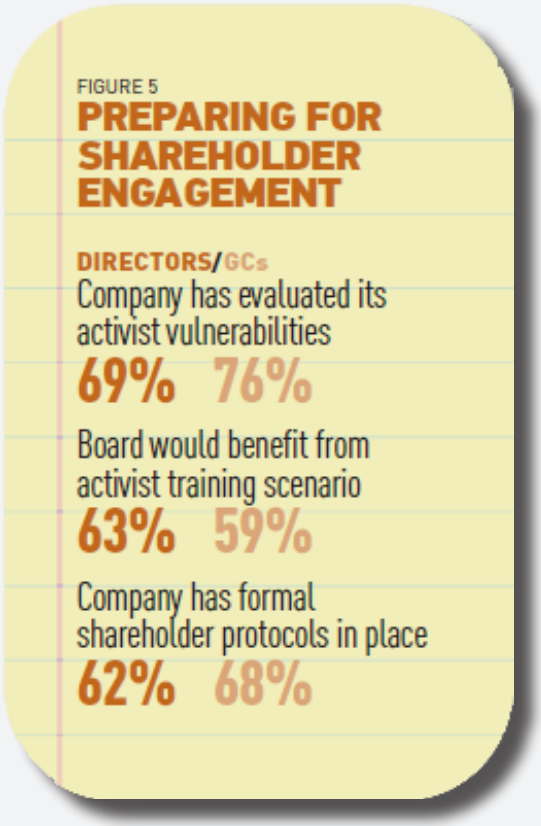
- 62% of directors and 68% of general counsel communicated that their company has formal shareholder engagement protocols in place
- When asked which key areas will likely require the most substantive time commitment in 2015, 51% of directors and 42% of general counsel chose M&A
- 30% of directors and 35% of general counsel do not feel that social media poses any risks against their company
- 91% of directors stated that their board does not have a thorough understanding of the risks related to social media for their company and 79% of general counsel stated that their legal department does not have a thorough understanding of the risks related to social media for their company

"Cyber risk poses a potentially devastating effect on a business' reputation and bottom line. Many companies don't realize the extent to which they are exposed to cyber risk until after they have suffered a cyber-attack. It is important for companies today to have a well prepared response plan in place so that they can quickly address the situation at hand." – Tom Brown, Senior Managing Director, Global Risk and Investigations Practice

"We have noticed that many companies have had to adjust to the heightened M&A risks. New levels of regulatory scrutiny around corruption in particular, involve acquiring companies to design certain anti-corruption and compliance programs as well as to develop thorough monitoring and auditing capabilities within their systems." – Michael Pace, Senior Managing Director and Global Leader of the Global Risk and Investigations Practice

To read the 15th Annual Law in the Boardroom Study, click here.





Compliance and Risk

The SEC's New Enforcement Mandate

By Martin Wilczynski

In recent speeches, Mary Jo White, the new chairman of the Securities and Exchange Commission (SEC), has outlined what investors and registrants can expect from the SEC's Division of Enforcement as her tenure begins. White, a well-respected former prosecutor, has focused on ways in which the SEC will leverage its resources and technology to be perceived as a ubiquitous agency—one that is policing the little things in addition to the headline-grabbing cases.

Referencing *The Atlantic Monthly* article titled "Broken Windows," White has channeled a 1970s New Jersey law enforcement initiative in which police were visibly detailed to neighborhoods to maintain order and remediate a range of infractions. By doing so, a signal was sent that all rules—large and small—are important. Analogizing to the SEC's Division of Enforcement program, White has theorized that like neighborhood residents who draw comfort from local police presence, investors in our capital markets will experience an enhanced level of confidence if the SEC is perceived as monitoring and maintaining order in a similar fashion.

To leverage the SEC's presence, White has cited a number of tools and initiatives. These include existing examination programs; the use of technology resources to monitor everything from trading patterns to financial statement details; cooperation initiatives with other agencies; renewed expectations for gatekeepers such as auditors, board members, and company counsel; incentives for whistleblowers; and an increased concentration on accounting and financial statements. Perhaps most significant, White has signaled that like the "Broken Windows" example, the SEC will maintain order by promptly and uniformly enforcing all infractions, including those that may be thought of as relatively minor in nature.

So what will this approach mean to corporate directors striving to improve registrant compliance and minimize risk?

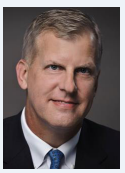
Attention to detail. First, corporate directors would be well served to appreciate—and to require management to adopt—the necessity of paying attention to compliance environment detail. Because cutting corners, ignoring weaknesses, or dismissing known errors or misconduct based on immateriality now will raise risks for registrants, management and board members, a mind-set of maintaining order should be a baseline for corporate conduct. Since the SEC will consider a focus on the little things as an essential indicator of a corporate director's interest in promoting a healthy compliance function, adoption of this perspective by all relevant parties should pay dividends in the event issues arise.

Proactive self-policing. Since the SEC will be tracking activity using sophisticated technological tools, corporate directors may benefit by encouraging management to install similar technology-driven monitoring. Various firms offer analysis of financial statement metrics by simulating computer-based programs utilized by the SEC. By pursuing these types of risk mitigation and detection tools, a proactive board would gain additional and earlier insight into potential problem areas, thus demonstrating to regulators an enhanced level of compliance activism in the boardroom.

Accounting is important again. By establishing the Financial Reporting and Audit Task Force, the SEC has reaffirmed its view of the need for increased vigilance in requiring reliable and accurate financial statement and disclosure information. Corporate directors can expect added skepticism by the SEC of maneuvers that shortcut or circumvent existing accounting rules. Potential areas of interest to the Division of Enforcement could include increased examination of "stealth restatements" or scrutiny of the accuracy of valuations applied to investment assets reported on a registrant's financial statements. Diligent and thorough accounting reviews and interaction with independent auditors will become critical undertakings for corporate boards to master.

Adopting the mind-set of a regulator, or at least appreciating his or her perspective, can be a valuable prism for a corporate director to build into one's fiduciary role. Even though a corporate director cannot be everywhere when it comes to monitoring and improving the compliance function, proactive involvement and an unwillingness to accept minor exceptions will be traits likely viewed positively by the SEC's Division of Enforcement administration.

Martin Wilczynski is a senior managing director in the FTI Consulting Forensic and Litigation Consulting segment and the leader of its Forensic Accounting & Advisory Services practice.

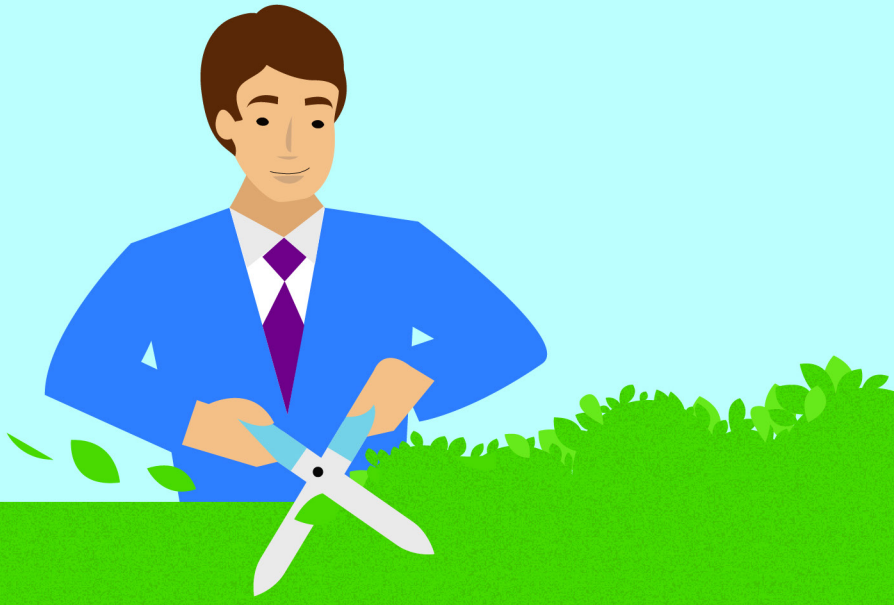


The views expressed herein are those of the author and do not necessarily represent the views of FTI Consulting or its other professionals.

FTI JOURNAL September 2015

THE NEW COSO FRAMEWORK:

Why Compliance is Good Business



FTI CONSULTING™

William Marquardt
Managing Director
Forensic & Litigation Consulting
FTI Consulting

Heather Raftery
Consultant
Forensic & Litigation Consulting
FTI Consulting

The legal and regulatory environment around the globe requires companies to ensure that they are actively working to prevent fraud and corruption, and any failure to do so may have significant legal and financial consequences. Yet, many companies do not take sufficient steps to avoid violations, making it challenging to mount an effective defense should corporate conduct be questioned.

Statutes such as the U.S. Foreign Corrupt Practices Act ("FCPA"), Brazil's Clean Company Act and the UK Bribery Act encourage companies to assess the bribery and corruption risks specific to their operations. Frequently, the results of these evaluations form the basis for assertions to investors and regulators about a company's level of compliance.

Evidence supporting these assertions — which may include procedures for procurement, processes for engaging intermediaries, widely distributed codes of conduct and compliance-related training — must be assembled and managed within an organization's compliance and governance functions. Often a company's chief compliance officer or general counsel (or both) is charged with collecting and maintaining this evidence as part of regular compliance operations. However, ultimate accountability rests with the board of directors and its Audit Committee.

Absent a robust risk assessment process and an adequate governance framework supported by internal controls and key performance indicators, the compliance team may not be able to determine whether violations of policy are occurring that might result in incidents of bribery and corruption. In many companies, the compliance function operates in a silo and standard procedures are not fully disseminated across functional or regional areas. Often legal and audit teams in one division or geography are unaware of information held or actions taken elsewhere. Thus, the compliance team may find it difficult to provide timely, accurate and comprehensive (i.e. company-wide) information to the board of directors and the executive management team.

As a result, companies often are expending more resources than necessary on day-to-day activities to monitor and enforce compliance and may not be allocating their finite compliance budgets effectively. For instance, a company may have dozens of auditors …. but it may base them in a region that is not high risk. Or it may spend a quarter of its compliance budget on staff ... but have no clear idea how the remaining money is being allocated across risk categories and geographies.

Risky Business

When companies' compliance violations are discovered by regulators, prosecutors or stakeholders, a variety of consequences may ensue, including fines, criminal prosecution and loss of value in the marketplace. Even in the best case scenarios, when management can convince regulators that a "bad apple" is responsible for a violation and this it is a one time occurrence, a company still may be fined and ordered to take remedial action.

For instance, in 2013, Ralph Lauren Corporation agreed to pay an $882,000 penalty and periodically report to the U.S. Department of Justice ("DOJ") on its compliance efforts to resolve allegations that a single employee had bribed customs officials in Argentina. **According to the DOJ**, during the time the violation occurred, the company did not have an anti-corruption program in place and had not provided anti-corruption training or oversight to its subsidiary in Argentina. The "bad apple" defense did not prevent the company from being punished because it did not have appropriate compliance/fraud prevention procedures in place.

Companies and individual executives face greater risk that they will be subject to such enforcement actions and that those actions will have severe consequences. **As *The Wall Street Journal* recently reported**, regulatory agencies increasingly are more likely to be coordinating enforcement activities and sharing information among various enforcement agencies. The investigation into corruption at FIFA, for example, involved law enforcement agencies and diplomats in 33 countries, **according to *The New York Times***. Companies are vulnerable as well to industry sweeps whenever regulators, having pursued violations at one firm, suspect that its competitors are engaged in similar practices.

Furthermore, regulatory agencies around the globe have indicated their intent to step up enforcement. By 2016, the UK Financial Conduct Authority expects to have in place a process for **holding individuals criminally liable** for corporate corruption. In the United

States, **the Securities and Exchange Commission** ("SEC") is increasing the number of resources allocated to enforcement activities.

The COSO Key: From Financials to Operations

Because risks transcend functional and geographic boundaries in today's highly international economy, addressing them is a critical function for boards of directors and senior executives. Firms can more readily identify financial and operational anomalies that may indicate violations of law, policy or other potential concerns about governance if they employ a well-designed set of internal controls and use key performance indicators to measure the effectiveness of these controls.

The private sector coalition known as the Committee of Sponsoring Organizations of the Treadway Commission ("COSO") provides auditors and business executives with models for evaluating and managing enterprise risks. One of these models, the COSO Framework, already is used by many companies to manage and report on their internal controls for financial reporting purposes. It offers a structure for governing compliance operations and supports the five cornerstones of strong corporate governance:

1. **Transparency:** Management standards and practices align with stated corporate values, allowing employees to feel safe in admitting mistakes or identifying weaknesses.

2. **Adaptability:** The organization is able to respond to legal or regulatory changes or address a control failure in a timely manner.

3. **Evidence:** The organization can readily provide documents, records, objects and other items relating to the existence or non-existence of alleged or disputed facts.

4. **Resources:** Based upon a continuing risk assessment process, adequate money, materials, staff and other assets are allocated to enable the organization to meet its compliance objectives.

5. **Accountability:** It is clear who has responsibility for compliance activities, who answers for their completion, who is consulted when opinions are needed and who is to be informed about progress.

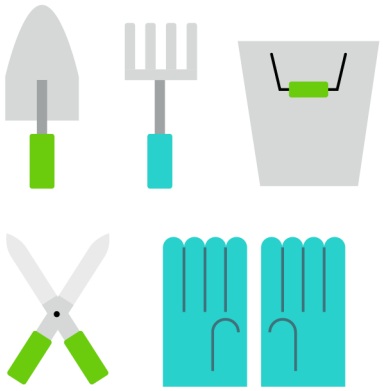
By applying these principles from the COSO framework to compliance programs, companies can not only create more effective and complaint operations, they also can more readily respond when faced with allegations of misconduct.

Losing Control: The Costs

This past May, BHP Billiton, an Australian mining, metals and petroleum company listed on the New York Stock Exchange, agreed to pay the SEC a $25 million civil penalty. The company allegedly improperly provided government officials from several countries with airfare, luxury hotel accommodations, tickets and meals at the 2008 Beijing Olympics.

Although the company knew it risked violating anti-corruption laws and developed a process for determining whether individual applications for the freebies were compliant, no one reviewed all of the applications; instead they reviewed only a small sample. Antonia Chion, SEC Associate Director of Enforcement, noted that the company's "check the box" approach to compliance in this case lacked substance and, thus, **was not sufficient to comply with the FCPA**.

Similarly, a Tampa-based engineering and construction firm, PBSJ, agreed to disgorge $2.9 million in profits and pay several hundred thousand dollars in fines to settle charges that an executive had agreed to pay bribes in exchange for inside information that helped win contracts in Qatar. Although the PBSJ legal team discovered the plan before any



payments were made, the SEC observed that **the company ignored multiple signs** that would have led officers or employees to uncover the scheme earlier.

Many companies, in fact, are unable to determine whether their programs are effective, whether they are spending the appropriate level on them, or whether or not resources have been allocated properly. In a 2014 survey of company compliance programs, fewer than half of the companies measured the impact of their programs, and only 22 percent tracked what non-compliance cost them.

No Framework, Big Problems

Management silos within a company that inhibit information sharing and coordination are at the root of these problems. Typically, employees are organized by regulatory specialty, function, market or geography, and they neither share information with each other nor pass it up and down the corporate hierarchy. Companies may have one group responsible for compliance with Sarbanes-Oxley financial reporting regulations in the United States, another group that focuses on global enterprise risk management and yet another that concentrates on anti-corruption regulations in disparate jurisdictions and they do not coordinate their efforts.

It is unusual for audit, compliance and operations executives to have insight into what their counterparts are doing in other functional or geographic units. Processes may vary by location. Data are not integrated. Operating objectives

from unit to unit are not uniform and sometimes conflict. If individual units have performance metrics, they may not be consistent across the company. This lack of integration means a company's board of directors and C-suite executives do not have a regular, consistent and accurate view of the company's compliance position.

The problems posed by organizational silos run deep. Without coordination from the top, the compliance function cannot provide consistent guidance to operations, resulting in employees following different processes and rules that lead to dissimilar outcomes in various operational units or jurisdictions. Meanwhile, the company cannot determine if compliance objectives are being met or validate management's compliance-related assertions. When a regulatory action is initiated, companies have to make heroic efforts to investigate the charges and produce accurate documentation to either confirm or counter the allegations. Consequently, companies often are not able to substantiate their public assertions that their governance programs are operating effectively and efficiently.

The failure to execute compliance operations in a consistent, integrated way has serious operational and financial consequences. Companies may have to spend millions of dollars to investigate and defend allegations of violations and pay millions if found non-compliant. (The average fine in **U.S. DOJ and SEC enforcement actions is $150 million.**) Shareholders may sue company directors and officers if, for example, they believe that by not preventing or discovering the company's conduct the officers and directors have breached their fiduciary duties to the shareholders.

Enforcement actions also take a toll on corporate value. **A recent study by George Mason University** found that companies facing bribery actions lose, on average, 7.7 percent of their market value. When companies are charged with bribery and financial fraud, reputational losses "can overwhelm direct costs" of an FCPA enforcement action to the tune of 46.3 percent of market capitalization.

Finally, routine compliance operations are inefficient and expensive when staff and information systems are duplicated across the company, and the same transactions may be reviewed for compliance multiple times. **In an ADP survey**, 78 percent of respondents said lack of integration of compliance information technology systems increases their costs.

Recently, a global mining company spent several million dollars responding to an FCPA investigation by the U.S. SEC. The investigation arose from a transaction that provided shares to individuals who did not have a direct business connection to the company. The SEC questioned the company's due diligence efforts and the transparency of the transaction but, ultimately, declined to pursue any enforcement action. The case was closed; however, the economic and reputational damage was done.

Responding to the SEC inquiry was costly in part because the company's compliance data were scattered and the company had difficulty assessing the current state of its compliance operations. The compliance program evaluation involved collecting thousands of documents from its operating units around the globe, conducting dozens of interviews in multiple locations, and analyzing numerous datasets containing records of purchasing activities, vendor due diligence and other corporate processes.

On top of that, many structural obstacles prevented the company from quickly and efficiently assembling the information it needed. These obstacles included (but were not limited to):

- **The compliance function was neither centralized nor was it provided with adequate resources, and the company's operating units lacked a set of consistent policies and procedures to follow.**
- **Operating units had no standard platform or compliance performance metrics.**
- **The company set inconsistent and sometimes conflicting operating objectives. For example, financial performance had priority over other management objectives.**
- **No third party performed risk-based due diligence processes.**
- **The company had no framework in place to establish links among corporate governance, risk management and the management control environment. Thus, it could not make connections among its internal controls, its compliance objectives and the assertions it made to regulators.**

How the COSO Framework Helps

Firms can reduce the costs and headaches of compliance with a well-designed framework of internal controls and key performance indicators to measure results. Most large companies already use the framework developed by COSO to manage their financial controls and their enterprise risk, but, in 2013, COSO expanded its guidance in order to support a greater focus on establishing and achieving operational compliance and reporting objectives that affect risk.

The expanded guidance, called the new COSO Framework, gives companies a roadmap for connecting high-level control objectives with specific policies, processes and procedures and verifiable

control points. It offers companies several benefits, including:

- A way to measure and report accurately on the effectiveness of its controls.
- The opportunity to provide an affirmative defense if the company is running its compliance operations in a widely accepted manner.
- Support for the five governance cornerstones: transparency, adaptability, evidence, resources and accountability.

Using a single governance framework across the company can help an organization ensure that all aspects of compliance are transparent, adaptable and properly monitored while effectively managing both accountability and the available, limited resources within an organization. Within this framework, companies may create a regional, integrated compliance structure with centralized oversight. Such a structure ensures that dedicated compliance professionals are engaged at the local level and that their work is monitored, measured and communicated to senior decision makers and that they are monitored on an organization-wide level.

Adopting the COSO Framework for Operations Is Good Business

Managing compliance in a global organization is complicated. As is the case with many business functions, compliance often evolves in reaction to local conditions, only receiving management attention when a new law or regulation comes into play, an allegation shines light on a narrow problem or an enforcement action forces a change in company practices.

Therefore, it is important that local legal and compliance teams do not work in a vacuum. To ensure that their company acts within the law and avoids compliance violations, compliance professionals are dependent upon other compliance offices and business functions. The compliance program should be run as a global, interconnected business function. The COSO Framework, combined with a rigorous set of key performance indicators, provides the structure for doing so.

By using the COSO Framework, companies will be able to take a proactive approach to reporting that not only saves money on compliance operations every day, but also during investigations if they arise. Most important, adopting the new COSO Framework demonstrates to all stakeholders that managing compliance risk is a high level priority within the organization. This generates confidence in the company among regulators and investors that can materially and beneficially affect the outcomes of future business activities.

William Marquardt
Managing Director
Forensic & Litigation Consulting
FTI Consulting
bill.marquardt@fticonsulting.com

Heather Raftery
Consultant
Forensic & Litigation Consulting
FTI Consulting

For more information and an online version of this article, visit ftijournal.com.

Internal Investigations

Revealing The Core Of Corruption

Greg Hallahan
Senior Director
Global Risk & Investigations Practice
Forensic & Litigation Consulting
FTI Consulting

FTI CONSULTING™

An internal investigation of fraud, bribery and other types of malfeasance often is difficult to conduct and can be disruptive to business operations. When made public, an investigation also can cause an organization great reputational harm. To mitigate these risks, companies need to take a holistic approach to an internal investigation, coordinating and synchronizing multiple actions that require investigative, legal, technical and communications skills and expertise. This article — detailing a series of FTI Consulting engagements involving one company in China — illustrates some of the challenges that arise in an internal investigation and describes how they best can be addressed.

Setting the Scene

The factory was located in a poor, little-known inland province in a dusty industrial town just like hundreds of others in China and elsewhere in Asia. Over the years, row upon row of corrugated steel facilities had been thrown up on scrubland. The sun was always dim, filtering through the unremitting smog.

This factory was very profitable for its Western owners due, in part, to the efforts of its Chinese general manager ("GM"). A diminutive man in his late 40s, the GM was energetic, smart and greatly respected by his employees. Dedicated to the business and his job, he put in long hours at the plant. His reputation within the company's Western management was spotless. He had been GM for 10 years, and the business had thrived.

One day, the company's senior Western management team heard a rumor, merely an employee's passing comment, that the hotel near the facility — the only decent place to stay in town and the one in which the company's executives reside when visiting — was owned by the GM. Contractually, the GM should have disclosed his interest in the hotel, particularly as, if true, he was deriving income from the company by owning the business. But he hadn't.

Initially, management was disinclined to pursue the matter — why rock the boat? The GM was an excellent employee; the hotel was of a decent quality (especially for the area); the rates it charged were appropriate to the market — and side businesses were par for the course in Asia. Management knew that when someone in Asia is an influential person, as was the GM, it's almost inevitable that he or she will have a little something going on the side. Family, friends and local business partners invariably approach such a person with a constant stream of business opportunities. It virtually is impossible to say no to all of those offers so, eventually, side interests start to accumulate.

However, the rumor about the GM owning the local hotel reached the company's board, which, at first, was split about whether there was cause to investigate. The board ultimately concluded that if it was true that the GM was running a business and had chosen not to disclose that information, that might be an indication of a more serious problem at the facility the GM ran. That, in the board's view, warranted an investigation.

The company's legal counsel reached out to FTI Consulting's Global Risk & Investigations Practice ("GRIP") to determine — discreetly — if the allegation that the GM owned the hotel was true. That was the beginning.

The Discreet Phase: From the Outside In

The first step GRIP took was to identify the company that owned the hotel and then to access the public State Administration for Industry & Commerce corporate records on the operation. At first, there seemed to be no connection to the GM. But when GRIP dug deeper, researching the historical records of the hotel's initial filing, it discovered that the GM had founded the business and — through another company he owned — still was the majority shareholder. The hotel's legal representative (all companies in China are required to appoint a legal representative) had been changed just the year before from the GM to a person who subsequently turned out to be the GM's driver and close friend. These findings led GRIP to send an investigator to the hotel.

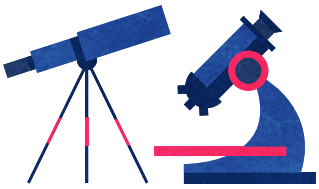
The investigator asked the hotel manager about the possibility of hosting a conference there and what it might cost. Casually chatting with the manager about arrangements, the investigator learned that the real owner and decision maker, in fact, was the company's GM.

Now that the initial allegation about the GM had been confirmed, GRIP started an extensive search of public records, social media checks and further on-site inquiries, piecing together a picture of the GM's inner circle of family and friends. The thinking was that since the GM already had demonstrated a propensity to use a friend to mask business interests, additional members of the GM's circle might be representing him in other companies and business operations. GRIP ran checks on the GM's close personal network and discovered that his mother, a retired language professor now in her 80s, was the legal representative of a recently incorporated construction company.

GRIP reported its findings to the company's Western management and was informed that the company was in the process of purchasing a large tract of land nearby upon which it intended to build a new factory. To do that, it would need to hire a construction company.

The opportunity for corruption was clear. In the natural course of business, the GM would be responsible for finding and contracting with a construction company to get the new facility built. Consequently, the company asked FTI Consulting's GRIP to continue and expand its investigation.

In China, as everywhere in Asia, the personal and the professional are deeply entwined.



The Overt Phase: From the Inside Out

The first stage of the investigation was conducted discreetly, outside the company. No employees were interviewed; no investigators entered the facility; no company records were accessed. The second stage would move inside, examining books, records and the GM's computer. Now it would be an open, overt internal investigation, and that generates a universe of risks that must be managed.

In China, as everywhere in Asia, the personal and the professional are deeply entwined. With the explosion of social media and the proliferation of smartphones throughout all of Asia, news and gossip spread with digital speed. It should be assumed that once one person inside a company becomes aware of an investigation, everyone will know within 24 hours. Therefore, the company and FTI Consulting needed to take steps to secure evidence and manage public reaction to the investigation both inside and outside the company.

To mitigate the reputational risks to the company and manage the messaging around the investigation, FTI Consulting called upon the skills of its Strategic Communications segment.

Working with the company's senior Western management team, Strategic Communications helped design the messaging about the investigation to internal employees, from factory floor workers on up, and external stakeholders.

The GM was a significant figure in the province; investigating him would attract the attention of the local press, which enthusiastically covers stories about corruption when foreign-owned companies are involved. The international media in Shanghai and Beijing, which keeps a keen eye on local counterparts, also likely would pick up the story immediately.

The company, possessing the fruits of FTI Consulting's investigation, now had to make a series of decisions.

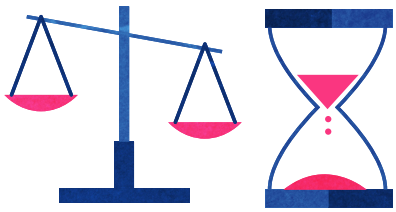
Strategic Communications needed to prepare to engage with all these outlets to make sure the company would be presented in an optimal light.

At the same time, Strategic Communications helped plan for how to handle the company's employees and managers when the story broke — to mitigate operational risk, as well as to ascertain which government agencies and officials needed to be kept informed about the investigation.

The GM's actions raised the specter of bribery and corruption, which was a potential problem far larger in scale than the hotel business and even the possibility of bid rigging for his construction firm. To see how deep these waters ran, FTI Consulting brought in its Forensic Accounting and Technology teams to thoroughly examine the company's books and records on-site, beginning with the contracts for the new facility to evaluate whether reporting requirements for both the home and the host country were being adhered to.

Meanwhile, the Technology team secured the relevant company computers and began reviewing the GM's electronic activities. The group was responsible for controlling the data as a whole to establish a reliable, valid and defensible chain of evidence.

All this research quickly began producing a large volume of data from disparate sources, which the Technology team was able to categorize and make available to legal counsel, investigators and company executives.



Truth and Consequences: Decision Time

Through the inspection of the company's books, it became clear that the GM also had been using payments channeled through third-party consultants (predominantly travel agents) to take government officials on lavish trips to Europe — bribes for the purpose of securing contracts. This no longer was a matter of an employee making a little money on the side by steering executives to his hotel; this was a bribery and corruption case that posed a significant threat to the company, exposing it to a variety of Chinese and international anti-bribery and corruption laws.

At this stage, the GRIP team undertook a series of on-site interviews with key company employees, including the GM and his next in command, which revealed the extent to which other members of senior management were involved.

The company, possessing the fruits of FTI Consulting's investigation, now had to make a series of decisions.

The GM had deep roots within the company and the province. If he was fired, or prosecuted, what would the reaction be among the workers, many of whom he had hired? Would they disrupt operations? How would government officials react? On the one hand, several officials appeared to have personally benefited from their association with the GM. On the other hand, the last thing senior authorities wanted was for a large taxpayer and employer in their province to get on the radar of the government's Central Committee for Discipline Inspection. That wouldn't be good for the province nor for the officials responsible for running it.

And if the GM was dismissed, who would replace him? He had personally hired his subordinate, the individual next in line for the job. To what extent was that person aware of or involved in the GM's scams? (As noted above, GRIP investigated the GM's heir apparent and found him to have had knowledge of the GM's activities but not to have been an active participant in them.)

Ultimately, the company decided its best course was to dismiss the GM and a handful of his inner circle. The employees accepted the new GM — their jobs were important to them. And the reaction of both provincial and government officialdom was minimal. Consummate realists, once the GM was out of power, they shrugged their collective shoulders and waited to see how the new GM would work out.

Nor did the now former GM make heavy weather. Fluent in languages, at ease in dealing with Western businesspeople, he became a provincial ambassador. The company did not pursue civil litigation against him.

Lessons for Companies

In Asia, allegations against managers many times come via whistleblowers posting rumors on social networks or someone (often the person in question) uploading a photograph showing an example of conspicuous consumption — a manager's new super luxury Audi or an opulent addition to his or her home. Just as frequently, though, a company's suspicions can be raised, as they were in this case, by a passing comment. Because of this, Western management needs to keep its ear to the ground. It should maintain at least a semi-regular physical presence on the factory floor, as well as in the management offices, and not distance itself from operations, no matter how well things seem to be running. If fraud and corruption exist within an operation, people will know about it, and, inevitably, they will talk about it.

When global management is watching and listening, red flags can be recognized for what they are: potential signs of fraud and corruption. One common signal is the ongoing use of unapproved third-party contractors such as the travel agents the GM paid to arrange the trips he used to bribe government officials. If the company had examined those expenses more carefully, it would have seen that what was being delivered was not commensurate with normal business requirements. Indeed, all third-party providers should be monitored closely. If they are new to the company, they need to be thoroughly vetted (i.e., who owns the operation?), and it should be made clear why these particular parties are being used.

Companies must understand that once corruption begins to grow, its roots invariably will run deep. Certainly, if the corruption is major, senior people most likely will be participating. Those managers have hired the people beneath them, and, therefore, many aspects of the business — warehousing, sales, procurement, accounting and government relations, to name a few — likely will be involved.

This makes it almost impossible to run an effective on-site investigation with internal resources alone. It is natural for company executives, discovering they have been traduced, to become emotionally involved and immediately seek to confront the person under investigation, asking questions to which they do not know the answers. This will alert those associated with the fraud; potential evidence may go missing; and the company could find itself not knowing who or what to believe, with little tangible proof pointing either way. It, thus, is critical for companies to get independent counsel on board as early as possible to make sure all the bases are covered and nothing has been overlooked. Once a decision is made to initiate an internal investigation, it must proceed expeditiously and with the right combination of resources.

There is nothing new about corruption. But regulatory authorities in the United States, Europe and, more recently, China — in fact, almost everywhere — are becoming more aggressive. They are better supported, funded and more capable than ever before. Companies increasingly are being taken to task and are suffering significant, material penalties for the missteps produced by lax compliance practices and simple inattention.

An internal investigation is a crisis for most companies. Ideally, with the proper compliance policies assiduously executed and maintained, such inquiries can be avoided. But once an internal investigation becomes necessary, good, professionally conducted examinations can do much more than run down malefactors and shut down their schemes: An analysis can expose the dysfunctional processes that allowed the fraud and corruption to find a purchase and, by doing so, fix them. In that way, an internal investigation, while unpleasant and unfortunate in the short term, can provide great benefits going forward — as long as the research is conducted by professionals with the time, skills and resources to do the job correctly.

Greg Hallahan
Senior Director
Global Risk & Investigations Practice
Forensic & Litigation Consulting
FTI Consulting
greg.hallahan@fticonsulting.com

For more information and an online version of this article, visit ftijournal.com.

Managing Cyber Risk: Job #1 for Directors and General Counsel

FTI CONSULTING™

The results of the FTI Consulting 2014 Law in the Boardroom Study, conducted with NYSE Governance Services, publisher of *Corporate Board Member* magazine.

Each year, FTI Consulting and NYSE Governance Services survey public company directors and general counsel about the legal and governance issues that concern them the most.

Early this year, nearly 500 directors and general counsel participated in the 2014 Law in the Boardroom Study. Over time, this annual survey has given us the opportunity to identify the key concerns of directors and general counsel and see how these issues evolve from year to year. What directors and general counsel say provides a unique insider's view of the "currents" and practices of business, both in the United States and globally. This work also allows us to compare and contrast each group's outlook on the year's critical issues so we can gauge how well they are aligned, and it helps boards and their legal team peek over the battlements of their own enterprise and put their challenges and practices into better perspective.

In the 2014 survey, after the traditional topic of regulatory compliance — which, of course, regularly disturbs general counsel — data security topped both directors' and general counsel's lists of worries, outranking, for directors, 2013's top concern of succession and leadership transition. The risks that come along with the digitization of business (and everything else) are multiplying, as are the costs of protecting against and remediating the impact of cyberattacks and data breaches. This year, information technology (IT) cyber risk oversight was chosen by 41 percent of directors and 33 percent of general counsel as an issue upon which they will spend significant time, appreciably more than last year's 28 percent for directors and 27 percent for general counsel.

Carrying over from 2013 were the challenges presented by the seemingly unstoppable merger and acquisition (M&A) market, the (perhaps) connected demand for increased shareholder engagement, the risks presented by social media, and the traditional issues of enterprise risk management (ERM), compliance and compensation.

What follows is a closer look at these broad areas of concern.

IT/Cyber Risk and Data Security

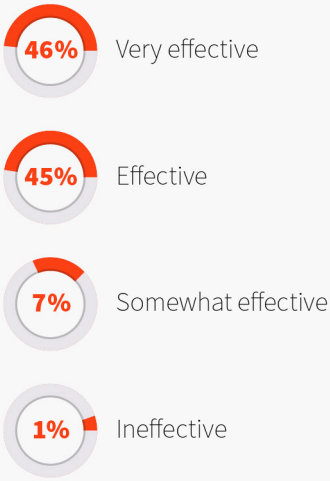
According to the Ponemon Institute's 2013 Cost of Cyber Crime Study: United States, the average annualized cost of cybercrime in 2013 was $11.6 million per company studied, with a range from $1.3 million to $58 million. The average annualized cost in 2012 was $8.9 million. This 2013 cost figure represents a 30 percent increase over 2012 — little wonder that cyber risk has risen to the top of what keeps directors up at night.

Indeed, 34 percent of general counsel and 27 percent of directors are not convinced their company is secure from hackers. What may be even more troubling is that a quarter of both directors and general counsel surveyed believed their

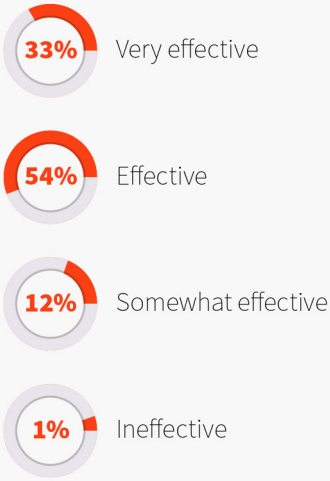
How Effective Is Your Legal Department's Oversight Of...

DIRECTORS SAY:

Ethics & Compliance Culture



Whistleblower Process



company is secure despite the fact that the Ponemon study found that the 60 U.S. companies it surveyed reported two successful attacks per company per week, an increase of nearly 20 percent over 2012's rate.

In other words, evidence indicates that the hackers are getting better at their exploits, and corporate security is not keeping up. This suggests that the confidence level expressed by general counsel in the board's ability to ask management the right questions may be ill-founded (54 percent of general counsel were either extremely confident or confident) regarding the status and risks associated with the company's IT strategy — which mirrors the confidence of directors (50 percent).

"Board-level concern often is confounded by the fact that the technology underlying cyber issues can be opaque to many executives," says Thomas Brown, Senior Managing Director in the FTI Consulting Global Risk & Investigations Practice. (Until recently, Brown led cybercrime prosecutions in the U.S. Attorney's Office in Manhattan.) FTI Consulting's role, Brown says, is to help bridge that gap, which is of utmost importance given cyber risk's ubiquity in a world in which business is increasingly conducted digitally over the Internet.

"Cyber risk's pervasive nature presents an existential threat to the operation, reputation and bottom line of virtually every company, regardless of industry," Brown says. "The priority that board members and general counsel place on cyber security and data protection not only reflects this reality but is entirely in line with our experience assisting clients to address this threat."

FTI Consulting, Brown says, has been helping more and more corporations develop incident response plans and internal controls, assess networks for vulnerabilities, secure the organization's data and evaluate cyber insurance options.

The need for this kind of bridge is underscored by the fact that this is an area in which directors and general counsel question each other's abilities: Thirty-eight percent of directors found general counsel only somewhat effective at IT/cyber risk oversight; 37 percent of general counsel said the same about their board.

M&A and Other Competitive Factors

According to Thomson Reuters, worldwide M&A totaled $710 billion in the first quarter of 2014, an increase of 54 percent compared with year-to-date 2013. U.S. M&A announced so far in 2014 comes to $361.1 billion, up 62 percent from 2013 year to date, representing the strongest period of dealmaking in the United States since 2007, the year before the global credit crisis. (U.S. M&A currently accounts for 51 percent of global activity.)

Investment banking expert Jeff Golman, on Forbes.com, wrote that he believes 2014 will be an unusually strong year for U.S. M&A, given favorable credit markets, continuing low interest rates, increased corporate cash reserves, a large inventory of private equity-owned companies with finite ownership horizons, a healthy stock market and an uptick in cross-border M&A activity.

With M&A heating up across all industries, along with other forms of corporate growth, 54 percent of directors said they'll be making a large time commitment to M&A in 2014, as did 51 percent of general counsel. That's a significant increase from 2013, when 42 percent of directors and 36 percent of general counsel identified M&A as an area to which they'd be devoting increased time. M&A strategy also made directors' top five in terms of areas where

the board needs better information and processes in order to be as effective as possible.

Shareholder Engagement

The rules of shareholder engagement have changed dramatically over the last decade. Increasingly, vocal shareholders expect dialogue not only with management but with the board itself. Accordingly, most of our director respondents reported that their board had proactively engaged in a dialogue with shareholders in the last 12 months, and 57 percent said those interactions touched on the topics of M&A and corporate growth strategies. Nearly half said they also discussed board structure and director qualifications (49 percent), and 46 percent reported their board also recently has discussed executive compensation with shareholders. And the majority of general counsel were comfortable with their board discussing these topics with shareholders.

The directors believed the way they handle shareholder communications is quite effective (81 percent), but 26 percent said they are only somewhat effective in developing strategic communications plans to build shareholder support. This suggests that directors could do a better job of monitoring shareholder sentiment to determine if and how discontent is bubbling up.

We asked general counsel if they are comfortable with this degree of openness on the part of directors and found (as we did in 2013) that approximately 80 percent said they are comfortable with directors discussing board structure and director qualifications and compensation, although general counsel were split when it comes to whether the board should engage with shareholders on matters of M&A and growth strategies (54 percent in favor), corporate social responsibility (54 percent in favor) and political contributions (51 percent in favor).

Shareholder activism is driving not only openness with shareholders, but that engagement can help board members identify and evaluate opportunities. Proactive engagement also helps build investor confidence and stands management in good stead when it comes to crises and/or proxy fights.

Social Media

Social media is looking more and more like a permanent fixture in our society. Last year, in our first foray into the topic, when we asked whether companies had developed a formal policy on the use of corporate social media, 59 percent have not done so or are unsure. Only 16 percent of directors said they have formally discussed social media issues, and 25 percent said they have no plans to do so. This year, 73 percent of general counsel and 44 percent of directors said their company has a formal policy (a significant disconnect between general counsel and directors, perhaps illustrating the still-conflicted attitude of directors toward social media), and 14 percent and 12 percent, respectively, said they are in the process of creating one — a huge change which, if fully implemented, would mean almost all companies would have social media policies next year. Still, 17 percent of directors said their company has no policy and has no plans for creating one. And 27 percent of directors were unsure of whether their company even has a social media policy.

Only 22 percent of directors thought their company has a good grasp of social media, with 45 percent saying they need more information, and 19 percent declared they have no plans to discuss the subject.

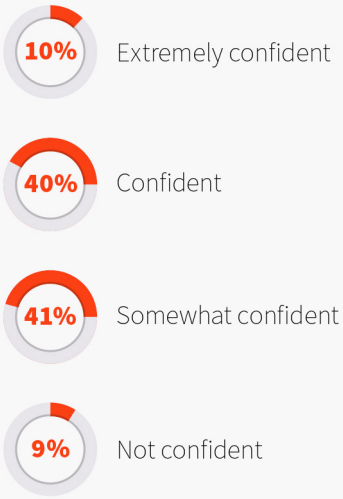
While directors and general counsel are recognizing the importance of creating a formal social media policy to mitigate risk, there still is, it seems, a worrisome lag.

ERM, Compliance, Compensation and Succession

Among the more traditional issues with which boards and general counsel deal, enterprise risk management (ERM) was chosen most often by general counsel (48 percent) as the area in which their legal department needs better information and processes in order to be as effective as possible in 2014, followed by regulatory compliance at 46 percent. Along with data security, compliance was the top issue over which general counsel said they are most likely to lose sleep. Directors did not rate those two areas as highly, although 33 percent agreed they need better information to handle ERM. Nearly 40 percent said that regulatory compliance is one of the most significant challenges to the company's ability to meet its 2014 performance goals.

Increasingly, governments and agencies are focusing on anti-corruption regulation, third-party liability, money laundering and insider trading. According to Erica Salmon Byrne, Executive Vice President, Compliance & Governance Solutions, NYSE Governance Services, compliance and ethics programs are the most effective way companies can mitigate people-created risk. "The risk that employees are out there doing the wrong thing on any given day is great." Having those programs, she says, "is the

Our Board Knows The Right Questions To Ask About IT Strategy And Risk:



most important thing the board can do to make sure the company is utilizing shareholder assets appropriately and is effectively controlling the risk."

According to Neal Hochberg, Senior Managing Director and Global Leader of FTI Consulting's Forensic & Litigation Consulting segment, "Compliance concerns are at an all-time high for publicly traded companies. With 81 percent of general counsel listing compliance as a chief concern, it is critical that companies invest in a proactive compliance program to protect their enterprise value. In this ever-changing environment with increased regulatory inquiries, companies must remain vigilant to avoid potential violations. An effective compliance program, training and continuous monitoring can play a crucial role in preventing violations that could tarnish a corporation's image."

When asked which issues their legal department or management has specifically reviewed with the board, 77 percent of directors chose the SEC's pay ratio disclosure rules, and 65 percent said they have discussed the implication of the upcoming rules on compensation clawback policies — not surprising as compensation continues to be on the board's radar despite slipping from first to second (and to third for general counsel) in terms of the area likely to require the lion's share of the board's time.

Succession planning was second on the directors' worry list and third for requiring the greatest time commitment.

Looking Ahead

Although it's hard to predict what the next big issues will be, it's not unreasonable to imagine that the deployment of data and analytics, the worsening of the cybersecurity threat and the emerging risks associated with social media in the corporate environment will continue to consume the time and attention of directors and general counsel. Most of those we surveyed indicated that these are areas that demand a firmer grasp on the part of board members as they plan their company's strategies going forward.

Increasingly, regulators are suggesting (and expecting) that directors gain a better understanding of all IT-related corporate risks, including data security, intellectual property theft, privacy issues and social media usage to guard their company against the breaches and data disasters that could cause material financial and reputational harm. We've already seen that happen with great frequency in the first part of 2014, and there's little indication that these threats will dissipate or become less damaging.

The FTI Consulting 2014 Law in the Boardroom Study showed that directors and general counsel increasingly are aware of these concerns, which is a good first step.

This article summarizes the results of the FTI Consulting Law in the Boardroom Study, conducted with NYSE Governance Services, publisher of Corporate Board Member magazine.

Countering the Growing Threat of Cyber Blackmail

Thomas G.A. Brown
Senior Managing Director
Global Risk & Investigations Practice
Forensic & Litigation Consulting
FTI Consulting

Christopher Tarbell
Managing Director
Global Risk & Investigations Practice
Forensic & Litigation Consulting
FTI Consulting

FTI CONSULTING™

Extortion and blackmail have been around for centuries. Until recently, criminals who pursued this illegal conduct had to operate in the physical world, limiting the scope and reach of their illicit activities and materially increasing the risk that they would be identified and arrested. Today, thanks to the ubiquitous digitization of our world — especially companies' reliance on computer systems to conduct business — cyber extortionists not only have many more avenues by which to steal sensitive information or hold individuals or companies at ransom but also the means to target a broader array of victims and do so with impunity. With just the click of a mouse, criminals can launch devastating attacks that shut down corporate websites or quietly infiltrate computer networks to steal trade secrets and other valuable information. Information-age extortionists can be thousands of miles away from their victims; proximity is unnecessary in our wired world. Anonymizing technologies such as Tor and virtual currencies like Bitcoin also enable online criminals to conduct their illicit trade with anonymity and without fear of detection.

And just as the Prohibition Era saw bathtub-gin entrepreneurs create mammoth criminal organizations, cyber blackmail has quickly grown from penny-ante, one-off hits to sophisticated operations capable of extorting large sums of money from businesses.

Although much of this activity remains unreported, the risk to enterprises is growing. Computer hackers understand the low-risk/high-reward dynamic of cyber extortion and blackmail and have quietly turned their attention to these lucrative pursuits, holding hostage companies' intellectual property, reputation and even ability to function.

Cyber blackmail presents corporate leadership with the age-old dilemma: to pay or not to pay. The answer is complicated because it's not always clear what you are paying for — will I get back every digital copy of my stolen trade secret, for example, or will the extortionists be satisfied with a single payment? But there are steps companies can take to avoid being placed in this perilous position in the first place and protocols that can help guide organizations once they find themselves there.

Cyber Blackmail and Extortion: A Growing Threat

The hack of Sony Pictures Entertainment in late 2014 has drawn more attention than any previous cyber extortion plot and could cost the company millions in revenues and reputational damage. According to U.S. law enforcement, the North Korean government was behind the attack, apparently offended by one of Sony's soon-to-be-released films, "The Interview," whose plot was the planned assassination of North Korean Supreme Leader Kim Jong-un. When Sony refused to cave in to the hacker's demands to stop the film's distribution, the hackers not only released data stolen from the company's servers, including other unreleased movies, insider emails and sensitive employee data, but also used destructive malware to cripple many of the systems used by Sony's employees to conduct business.

In an attempt to appease the hackers and stop the bleeding, Sony belatedly took the unprecedented step of canceling the release of "The Interview," taking a significant hit in lost revenues and production costs. While Sony ultimately offered the movie to consumers in a small number of theaters and via video-on-demand, the entire cyber attack still could **cost the company in excess of $100 million**, including costs associated with investigating the attack, rebuilding computer networks, and lawsuits filed in the wake of the hack's public disclosure. (A more targeted attack that shut down Sony's PlayStation network for several weeks in 2011 is reported to have **cost the company $170 million**.)

Beyond quantifiable financial effects, Sony's reputation suffered as its corporate dirty laundry was paraded throughout the media and as President Obama publicly criticized the company's initial decision to cancel the release of "The Interview." Then, in late January, Sony announced that its computers — including its financial and accounting systems — were so compromised by the hack (**which reportedly included the destruction of network hardware**) that it would not be able to report its third-quarter earnings on the February 4 due date, **requesting an extension to March 31**. Sony suggested that the reporting delay would not have a material impact on its financial statements, but the move could not have instilled investor confidence. In early February, the company's co-chairman and head of its

film studio **stepped down**, a move widely reported to be a result of the attack.

The average company may think a lower public profile protects it from such a damaging cyber extortion. But while the Sony hack was unprecedented in its scope and the public interest it generated, the Assistant Director of the Federal Bureau of Investigation's ("FBI") Cyber Division — the FBI's top cyber agent — said it is likely that **90 percent of U.S. corporations — large, midsized and small — are equally vulnerable to such an attack**.

While the Sony Pictures hack has received an inordinate amount of attention, the past 12-24 months, in particular, have been busy for cyber criminals. In June 2014, **a U.S.-led international operation disrupted an Eastern European crime ring** that infected as many as a million computers around the globe with software designed to steal passwords. The gang used the scheme to steal more than $100 million, ranging from $198,000 in an unauthorized wire transfer from an unnamed Pennsylvania materials company to a $750 ransom from a police department in Massachusetts to unlock its investigative files (the files had been rendered inaccessible by **CryptoLocker**, a species of malware that can encrypt data on computers running Microsoft operating systems).

Other recent high-profile cyber crime incidents include:

- A February 2015 data breach at one of the largest health insurers in the United States, Anthem, that potentially exposed the medical information (and the Social Security numbers and home and email addresses) of 80 million customers.

- A point-of-sale hack that resulted in the theft of credit card information from the U.S. restaurant chain P.F. Chang's with **thousands of the stolen cards put up for sale on the so-called "dark web."**

- A breach of security at the Montana Department of Public Health and Human Services in May 2014 that may have **exposed the information of more than a million people.**

- A February 2014 hack of **eBay that reportedly stole the personally identifiable information of 233 million users.**

- **High-profile cyber attacks against Target and The Home Depot** that resulted in the compromise of personally identifiable data for millions of customers.

The Threatscape: Attacks, Perpetrators and Victims Vary

Would-be cyber blackmailers can initiate their criminal efforts far outside a company's network. One common approach is known as a denial of service ("DoS") attack. Here, thousands of "zombie" computers (secretly controlled by hackers without the knowledge of the computers' owners) are marshaled to launch a simultaneous assault on a target computer resource such as a website, knocking it offline. DoS attacks especially can be damaging to enterprises that rely on user access to their websites, such as e-commerce companies, to conduct business.

Apart from DoS attacks, cyber criminals may seek to break into companies' computer networks. Once inside, hackers can quickly and easily follow any number of vectors to extort money from their victims. Some of the tactics include:

- Encrypting data that exist in business systems, then holding the information hostage for payment.

- Disabling critical business systems.

- Blocking access to corporate sites.

- Redirecting part or all of a corporate website somewhere else by altering DNS (a service that controls website naming and Internet traffic direction) settings, holding the original destination hostage.

- Stealing intellectual property and threatening to sell it to competitors.

- Accessing a computer, downloading unwelcome content (e.g., child pornography) that can't be removed and threatening to call law enforcement unless payment is made.

- Posing as a "gray hat" company (hacking firms that identify weaknesses and fix them for a fee) by finding exploitable weaknesses in corporate networks and threatening to notify the press or competitors unless payment is made.

Individuals also face the risk of so-called sexploitation attacks. In such instances, cyber criminals hijack a user's webcam, microphone or file system to obtain and threaten to release embarrassing photos, videos or messages. In 2010, **the FBI published an alert** for Internet users following the arrest of an California man who hacked into the computers of 200 women, downloaded compromising photos and used them to extort more photos from the victims. Last year, **a man was charged** with threatening to distribute embarrassing pictures of women if they did not provide him with more photos. The most recent high-profile target of such a plot was **Miss Teen USA 2013**, whose webcam was hacked.

Indeed, in May 2014, federal authorities charged an international group of hackers with operating an illegal business that marketed a remote access tool, or "RAT," known as "Blackshades." The Blackshades RAT enabled thousands of hackers in over 100 countries to infect more than half a million computers. After installing Blackshades on a victim's computer, an attacker could access and view documents, photographs and other files; record keystrokes; steal passwords; activate the webcam and microphone; encrypt data; and send ransom notes to the victim.

The Blackshades RAT and similar malware easily can be adapted for corporate espionage. Criminals might commandeer a computer microphone or camera in a boardroom or executive office to film or record confidential meetings. Using that business intelligence, the hackers could blackmail a company, sell its secrets to rivals or manipulate company stock with calibrated releases of privileged information. And cyber extortionists are increasingly targeting the children of intended victims by using information gleaned from social media activities.

Perpetrators of these other forms of cyber extortion range from organized crime rings to unhappy employees. Indeed, attacks are even more insidious when launched from the inside. Law enforcement has engaged **in a number of significant investigations** in recent months involving former or disgruntled company employees. In many of these cases, employees attempted to extort money from employers by threatening to expose privileged information or activate malware. These recent incidents cost victim businesses from $5,000 to $3 million in payoffs.

But, increasingly, the perpetrators of cyber blackmail and extortion are members of organized gangs around the globe.

While breaches of large corporations like Sony Pictures and Anthem make headlines, midsized companies actually may be the most vulnerable. Many smaller organizations fail to invest in redundancies to protect themselves, fearing that even minor changes to day-to-day operations might jeopardize profitability. These companies also lack the personnel and resources required to respond effectively to cyber blackmail attempts. They do, however, have enough capital to attract a cyber extortionist.

Why Most Companies Dummy Up and Pay Up

The vast majority of cyber blackmail or extortion attempts go unreported. When it comes to insider attacks specifically, three-quarters of the time companies deal with the matter internally and do not disclose the incident to authorities, according to a 2014 **survey of cyber crime by Carnegie Mellon University**.

Many victims of cyber blackmail simply pay a ransom because the consequences of refusing to pay and going public are too damaging to contemplate. Companies don't want to risk their reputation. A major breach often causes customers or business partners to think that inadequate security invited or caused the attack. To many companies, it appears cheaper to pay the ransom than to hire a third party (or devote internal resources) to recover the information, unlock the encrypted data or bring systems back online. Many businesses can't afford to lose revenues if their site goes down anytime — but particularly over the holiday shopping season or, specifically, on Cyber Monday.

But giving in to cyber blackmail demands doesn't always work out as planned. In one high-profile case in 2007, Finnish cell phone company **Nokia not only paid the ransom — leaving millions of euros in a parking lot with the hope that authorities could trace the extortionist — but also botched the delivery**.

The criminal got away with Nokia's cash, and the case remains cold all these years later.

Alternatives to Capitulation

While it may seem like the quickest and cheapest remedy, giving in to the demands of a cyber extortionist rarely is a good idea. It can be tempting to try to buy yourself out of a problem to keep your business' systems running, retrieve critical data or preserve your reputation. However, capitulating to terrorist-like demands also carries risks. There's never a guarantee that the criminal you're paying off will stay bought, and your customers and business partners will become uneasy should they discover that paying off extortionists is your corporate policy.

In addition, paying a ransom does not address the underlying vulnerability that the criminals exploited in the first place. Only an investigation, in conjunction with law enforcement where appropriate, can reveal the weaknesses that allowed the attack to occur. Such an investigation also can provide a path to remediation that will prevent the specific attack from recurring while also potentially revealing other weaknesses that can be fixed.

There are a number of ways to recover stolen files and data, unlock hijacked systems, and save corporate and individual face without paying or otherwise dealing with manifestly untrustworthy parties.

For instance, **Domino's Pizza** allegedly was attacked in June 2014 by the hacking group Rex Mundi, which claimed it had stolen 650,000 customer records from the company's servers in France and Belgium. Rex Mundi threatened to release those records publicly if Domino's didn't pay a ransom of €30,000. Domino's refused to comply with the demand and instead advised its customers that the stolen data did not contain financial information, only contact details, delivery instructions and passwords. The company instructed customers to change their passwords and began working with authorities and appropriate experts to investigate the incident.

How to Deal With Cyber Blackmail — Before and After It Occurs

Once a company or individual becomes a victim of cyber extortion, the number of good options dwindles quickly. Rather than react after the fact, corporate leaders need to have a response plan already in place so mitigating the risk of cyber blackmail schemes can be the main focus.

Once it is clear that a company is being extorted by the threat to release stolen information, lock critical data or launch a DoS attack, leaders should:

Understand the scope of the risks:

- Who are the attackers? Are they hacktivists? Financially motived cyber criminals? State-sponsored actors? Malicious insiders? An effective response depends upon identifying the bad actors.
- How are you or your company being attacked?
- What specific part(s) of your systems are being infiltrated?

Recognize all potential consequences. Risks come in many forms, including:

- Litigation by injured parties.
- Loss of competitive advantage.
- Reputational damage.
- Cost of response and remediation.
- Regulatory investigations leading to public exposure and possible penalties.

Have a plan in place. A comprehensive plan should include:

- A list of stakeholders to be informed.
- Predetermined and defined lines of communication that will speed information sharing.
- Appropriately trained and informed leaders empowered to make decisions during an incident (avoiding confusion and a slow response).
- A process for the continuous updating of information technology systems and security policies (at least quarterly) to keep pace with changes in business and technology.

Take advantage of established relationships with law enforcement (local, state and/or federal) to reduce the chance of a slow, confused response.

Just as important, companies can take a number of steps to lessen the likelihood that they will fall victim to cyber blackmail or extortion:

Identify all potential internal and external threats by:

- Monitoring social media.
- Staying on top of public forums related to your business.
- Identifying employees who may want to harm your company.

Audit computer networks to identify and assess vulnerabilities. Questions to ask include:

- Are software patches being applied in a timely fashion?
- Does the network have segmentation so that an attack in one area won't impact others?
- Are there access controls in place for your data?
- Who determines access controls?
- Are network logs collecting sufficient detail to allow for the thorough, informed and efficient investigation of a cyber incident?
- Are network logs maintained for a long enough period of time to allow for proper historical investigation?
- Do you know where all your endpoints are? Are network topology maps up to date? This especially is important because networks are dynamic, with companies continually adding and removing servers and distributing new devices to employees.

Don't Play the Waiting Game

The cyber blackmail and extortion threatscape will only grow more varied and complex over time. Criminals are continually changing their patterns of attack. While no company can protect itself perfectly, it can make smart investments in due diligence, response plans and sensible security based on rigorous risk assessments of what they stand to lose in the event of such an attack. ■

Thomas G.A. Brown
Senior Managing Director
Global Risk & Investigations Practice
Forensic & Litigation Consulting
FTI Consulting
tom.brown@fticonsulting.com

Christopher Tarbell
Managing Director
Global Risk & Investigations Practice
Forensic & Litigation Consulting
FTI Consulting
chris.tarbell@fticonsulting.com

For more information and an online version of this article, visit ftijournal.com.

SEPTEMBER 2015

COMMENTARY

U.S. Department of Justice Announces Updated Guidelines on Individual Accountability for Corporate Wrongdoing

Implications for Internal and Government Investigations

On September 9, 2015, after years of criticism by Congress and commentators about the paucity of prosecutions of individuals in major white collar cases, Deputy Attorney General ("DAG") Sally Yates announced six changes to policies and practices governing investigations of corporate misconduct in a memorandum (the "Yates Memo") to prosecutors throughout the United States Department of Justice ("DOJ").[1] The next day, DAG Yates delivered a speech amplifying the new policies and practices at New York University Law School.[2] The changes, which cover virtually all criminal and civil investigations of corporate wrongdoing, result from the DOJ's internal examination of its approach to building cases against individuals at all levels in white collar cases. The six changes will be incorporated into the Department's governing policies contained in the U.S. Attorneys' Manual, and they are effective for all new investigations, as well as on existing investigations "to the extent … practicable …."

The Memo itself promises no sea change in individual prosecutions and acknowledges that there will remain "many substantial challenges unique to pursuing individuals for corporate misdeeds." Stepping back from the rhetoric associated with the rollout of the changes, what is really changing?

One thing that won't change: it will still be the case that developing proof beyond a reasonable doubt of criminal wrongdoing by senior corporate employees in corporate cases will often be difficult.

Nevertheless, as this *Commentary* describes, aspects of the Yates Memo bear particular attention.

Of primary interest to companies will be the Yates Memo's effect on internal investigations of potential misconduct by corporate personnel, company decisions to self-report (or not) potential violations of law, and resulting impacts on related government investigations. The Memo appears to alter the preexisting "disclose all relevant facts" standard for receiving cooperation credit. It explicitly requires that all relevant facts "about the individuals involved" be disclosed to the DOJ as the baseline for receiving "any" cooperation credit.[3] In practical terms, this may not

represent a substantial change for cooperating companies but may have a chilling effect on employees with knowledge of, or involvement in, misconduct.

The Six Policy Changes

The Yates Memo sets forth the six policy changes as follows:

1 In order to qualify for any cooperation credit, corporations must provide to the Department all relevant facts relating to the individuals responsible for the misconduct;
2 Criminal and civil corporate investigations should focus on individuals from the inception of the investigation;
3 Criminal and civil attorneys handling corporate investigations should be in routine communication with one another;
4 Absent extraordinary circumstances or approved departmental policy, the Department will not release culpable individuals from civil or criminal liability when resolving a matter with a corporation;
5 Department attorneys should not resolve matters with a corporation without a clear plan to resolve related individual cases and should memorialize any declinations as to individuals in such cases; and
6 Civil attorneys should consistently focus on individuals as well as the company and evaluate whether to bring suit against an individual based on considerations beyond that individual's ability to pay.[4]

Three of these—(1), (2), and (5)—are most likely to have consequences for every case involving corporate misconduct and merit further explanation.

Qualifying for Credit. In detailing this change, the DOJ explained: "[c]ompanies cannot pick and choose what facts to disclose. That is, to be eligible for any credit for cooperation, the company must identify all individuals involved or responsible for the misconduct at issue, regardless of their position, status, or seniority, and provide … all facts relating to that misconduct." The Yates Memo goes on to highlight that this obligation is "subject to the bounds of the law and legal privileges" and that the Department will proactively test the evidence provided by the company and seek out evidence through other sources.[5]

Focusing on Individuals from the Outset. The Yates Memo directs prosecutors to "focus on individual wrongdoing from the very beginning of any investigation …." In the Department's view, doing so is the efficient and effective way to conduct investigations, will cause lower-level employees to cooperate and provide information against more senior employees, and will maximize the chance of successful individual prosecutions.[6]

Requiring Plans to Resolve Individual Cases Before Resolving Corporate Cases. Prosecutors will be required to present "clear plans" for concluding individual cases as part of seeking authorization to resolve cases against corporations. Even when civil claims or criminal charges are not being sought against individuals, prosecutors will be required to document and obtain approval from their superiors before resolving the corporate case.[7]

In our experience, two changes in the Yates Memo—items (3) and (4) above—are less likely to materially alter current practice. Defense counsel should already have been assuming that civil and criminal prosecutors are in "routine communication" with each other within the bounds of Federal Rule of Criminal Procedure 6(e) governing grand jury secrecy. In cases where the company has decided to cooperate, often civil and criminal prosecutors participate jointly in meetings and communications with company counsel and otherwise engage in joint information-collection and case-resolution activities. We also regularly encounter substantial reluctance or outright refusals to condition corporate resolutions on individual releases, other than where Department policy is explicitly contrary.

The Likely Practical Changes Resulting from the Yates Memo

Is It Appreciably Harder for Companies to Receive Cooperation Credit? This is perhaps the most important and puzzling question for corporate subjects of investigation.

Viewed one way, there is nothing new here. Since at least 1999, DOJ policy has required that cooperating companies disclose all relevant, nonprivileged facts.[8] Indeed, once a company decides to cooperate, it is foolhardy to do otherwise. There is little to be gained and much to be lost by seeking to withhold incriminating facts about employees at

any level. After the company opens the floodgates through partial cooperation, the government's ability to develop independent evidence through subpoenas to third-party sources, or informal interviews of employees, as well as the prospect of whistleblowers or other cooperators acting for their own interests, create substantial risks that selective disclosure of facts to benefit employees or senior management will backfire. These same dynamics have always required thorough corporate internal investigations, without pulling punches as to sensitive issues or favored corporate constituencies. As a result, most companies that cooperate already try to do so to the same extent as the "new" Department policy will require.

If there is something new here, it may be an implication that in order to qualify for cooperation credit, a corporation *must* serve up a prosecutable case against individuals:

> The rules have just changed. Effective today, if a company wants any consideration for its cooperation, it must give up the individuals, no matter where they sit within the company. And we're not going to let corporations plead ignorance. If they don't know who is responsible, they will need to find out. If they want any cooperation credit, they will need to investigate and identify the responsible parties, then provide all non-privileged evidence implicating those individuals.[9]

But that implication itself overlooks the fact, acknowledged by DAG Yates herself, citing former Attorney General Eric Holder, that many cases of *corporate* misconduct do not present evidence of *individual*, *criminal* responsibility:

> In modern corporations, where responsibility is often diffuse, it can be extremely difficult to identify the single person or group of people who possessed the knowledge or criminal intent necessary to establish proof beyond a reasonable doubt. This is particularly true of high-level executives, who are often insulated from the day-to-day activity in which the misconduct occurs.[10]

This is not always because evidence of *individual*, *criminal* responsibility is hidden from investigators, or because prosecutors fail to discover it, but equally often because it simply does not exist. The DOJ has properly cited this phenomenon in defense of the "imbalance," if it be viewed as such, between corporate and individual convictions. It remains to be seen whether the DOJ will now require from corporations, as a condition of cooperation credit, results that are often not supported by the facts.

Does the Yates Memo Change Whether Companies Should Self-Report? Since the early 2000s and the Enron/WorldCom era, the DOJ and other governmental agencies broadly and frequently have encouraged companies to self-report suspected wrongdoing in order to receive cooperation credit.[11] Vigorous exercise of Section 10A of the Securities Exchange Act of 1934,[12] as well as the reforms of the Sarbanes-Oxley Act,[13] created structural changes that reinforced that message. The advent of the post Dodd-Frank whistleblower economic incentives[14] add substantial risk that unreported corporate misconduct would nonetheless come to the attention of the government. Increased enforcement and financial penalties at all levels of government on corporate America has made the benefits of self-reporting seemingly less clear. As a result, making a corporate decision to self-report is often already complicated and challenging for senior managers and corporate boards. The individual prosecution priority may make corporate decision-makers more reluctant to self-report, particularly where personal financial consequences[15] and relationships may be implicated. In the end, consistent with their corporate duties and responsibilities, decision-makers will need to set aside those concerns and strive to act in the best long-term interests of the company and shareholders, and nothing in the new policies will make that easier.

How Will the New Policies Affect the Conduct of Internal Investigations? The DOJ's ongoing vocal prioritization of individual prosecutions is likely to further heighten tensions in internal investigations. Most importantly, concerns about their own exposure not just to personnel action, but also to criminal charges, as a consequence of providing information to internal investigators, brought into sharper focus with the Yates Memo, may very well result in fewer employees choosing to cooperate with internal investigations. And presumably any such trend will be more evident with respect to corporate personnel who have the most potential exposure to indictment (i.e., the most knowledge of and involvement in the offense(s) at issue).[16]

Corporate employees, of course, are frequently required to cooperate with duly authorized internal probes and may be

subject to termination or discipline for refusing to so cooperate. The rock-and-a-hard place predicament that criminally culpable corporate employees can find themselves in with internal investigations (i.e., not cooperating and facing discipline versus cooperating and potentially facing prosecution) is more clearly defined with the Yates Memo. If there was previously any ambiguity as to whether a company could hold back material information relating to individuals from the DOJ and still get cooperation credit, the Memo, on its face, eliminates that ambiguity.

One of the first questions that many employees ask during internal investigations is whether they need their own lawyers. The wide publicity concerning the Yates Memo can only increase and accelerate the rush to separate counsel. Employees, especially those represented by counsel well versed in this area of criminal practice, will now think longer and harder about submitting to an interview with internal investigators or otherwise cooperating with the internal investigation. At the barest minimum, the new policies highlight for employees the risk of prosecution when they do cooperate.

The Yates Memo requires that prosecutors consider evidence of individual liability from the outset. This is not a new policy. Such evidence in companies generally comes from electronically stored communications and records, as well as witness statements. Companies understand the financial and technological resource costs of retaining, retrieving, and reviewing voluminous electronic records during investigations. In her September 10 speech, DAG Yates stated that the new policies should not be interpreted to require additional investigation in terms of cost, breadth, depth, or duration.[17] Seasoned investigators may be skeptical of this claim. Companies seeking to cooperate will need to carefully assess the extent to which they review electronic records at an early stage of the investigation at the least, and they may well need to expend more resources earlier to satisfy the new policy requirements to obtain cooperation credit. If nothing else, the Yates Memo policies provide additional leverage for prosecutors to pressure companies to act quickly to remediate wrongdoing, including terminating culpable employees.

Will the New Policies Lead to Quicker Resolutions of Government Investigations? Probably the opposite. The need to develop evidence addressing individual liability during the investigation will add some burden, despite DAG Yates's expressed contrary view. Further, the requirement that prosecutors resolve or include a "clear plan" for completing investigation of individual conduct before resolving the corporate case cannot shorten the time to resolution of the company case, whether that resolution means bringing charges or claims, settling, or closing the company case.

How Do the New Policies Apply to Non-U.S. Companies? The new policies apply to all DOJ investigations, civil and criminal. By definition, that includes investigations related to U.S. laws that apply both within and outside the United States. Foreign companies and individuals otherwise already subject to U.S. jurisdiction and U.S. laws that have extraterritorial application, such as economic sanctions, the Foreign Corrupt Practices Act, antitrust, and conspiracies to violate U.S. laws, therefore will be subject to the new policies.

During her speech, DAG Yates also noted that multinational investigations encounter "restrictive foreign data privacy laws and a limited ability to compel the testimony of witnesses abroad [which] make it even more challenging to obtain the necessary evidence to bring individuals to justice." It remains unclear how the DOJ will view cooperation by multinational companies that seek to cooperate fully with criminal investigations, while also seeking to comply with local laws that restrict companies' ability to produce such evidence to the DOJ.

Conclusion

The new policies contained in the Yates Memo are designed at least in part to address criticism of the DOJ's efforts to criminally punish executives following the financial crisis of the last decade.

Whether these new policies will ultimately make it easier for the DOJ to overcome the hurdles to individual prosecutions, or merely shift to cooperating corporations the adverse consequences, is far from clear. But at least some of the new policies will further complicate the already very difficult process of conducting internal investigations and of dealing with the government in moving corporate cases to resolution.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

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

Henry W. Asbill
Washington
+1.202.879.5414
hasbill@jonesday.com

José Bonilla
Madrid
+34.91.520.3907
jbonilla@jonesday.com

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

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

Samidh Guha
New York
+1.212.326.3721
sguha@jonesday.com

Marcello Hallake
São Paulo / New York
+55.11.3018.3933 / +1.212.901.7058
mhallake@jonesday.com

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

Jerry C. Ling
Shanghai
+86.21.2201.8002
jling@jonesday.com

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

Stephen J. Obie
New York
+1.212.326.3773
sobie@jonesday.com

Matthew D. Orwig
Dallas
+1.214.969.5267
morwig@jonesday.com

Glyn S. Powell
London
+44.20.7039.5212
gpowell@jonesday.com

Daniel E. Reidy
Chicago
+1.312.269.4140
dereidy@jonesday.com

Peter J. Romatowski
Washington
+1.202.879.7625
pjromatowski@jonesday.com

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

Aldo Verbruggen
Amsterdam
+31.20.305.4246
averbruggen@jonesday.com

Hank B. Walther
Washington
+1.202.879.3432
hwalther@jonesday.com

Peter J. Wang
Shanghai / Beijing
+86.21.2201.8040 / +86.10.5866.1111
pjwang@jonesday.com

David Woodcock
Dallas
+1.214.969.3681
dwoodcock@jonesday.com

Mingda Hang, an associate in the New York Office, provided assistance with the preparation of this Commentary.

Endnotes

1 Sally Q. Yates, "Individual Accountability for Corporate Wrongdoing" (Sept. 9, 2015).

2 "Deputy Attorney General Sally Quillian Yates Delivers Remarks at New York University School of Law Announcing New Policy on Individual Liability in Matters of Corporate Wrongdoing" (Sept. 10, 2015).

3 Yates, *supra* note 1, at 3.

4 *Id*. at 3-7.

5 *Id*. at 4.

6 *Id*.

7 *Id*. at 6.

8 *See* Eric H. Holder, "Bringing Charges Against Corporations" (June 16, 1999) (the "Holder Memorandum").

9 *Supra* note 2, ¶ 14.

10 *Id*. at ¶ 7; *see also* "Attorney General Holder Remarks on Financial Fraud Prosecutions at NYU School of Law" (Sept. 17, 2014).

11 *See* Larry D. Thompson, "Principles of Federal Prosecution of Business Organizations" (the "Thompson Memorandum") (Jan. 20, 2003), and Paul J. McNulty, "Principles of Federal Prosecution of Business Organizations" (the "McNulty Memorandum") (Dec. 12, 2006), and Mark Filip, "Principles of Federal Prosecution of Business Organizations" (the "Filip Memo") (Aug. 28, 2008); *see also* Exchange Act Release No. 44969, "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" (Oct. 23, 2001) (the "Seaboard Report").

12 15 U.S.C. § 78j-1(b) (requiring auditors to report illegal acts and management failure to take remedial action to public company boards, and in some instances resign and notify the SEC).

13 E.g., Sections 302 and 404, 15 U.S.C. §§ 7241, 7262.

14 *See* Securities Whistleblower Incentives and Protections, 17 C.F.R. § 240.21F (2011).

15 *See* Forfeiture of certain bonuses and profits, 15 U.S.C. § 7243(a) (2002); *see also* Recovery of erroneously awarded compensation policy, 15 U.S.C. §78j-4(b) (2010).

16 As such, in the world of federal corporate criminal law, where resource-strapped enforcement agencies are, and will continue to be, heavily dependent upon internal corporate investigations for fact-gathering, the Yates Memo may undermine, rather than facilitate, the DOJ's efforts to ferret out and prosecute corporate misconduct and culpable individuals, at least in certain instances.

17 *Supra* note 2, ¶ 20 ("The purpose of this policy is to better identify responsible individuals, not to burden corporations with longer or more expensive internal investigations than necessary.")

JONES DAY

SEPTEMBER 2015

COMMENTARY

SEC Flexes Its Muscle on Accounting Fraud and Targets More Individuals

The Securities and Exchange Commission recently announced the settlement or filing of a number of significant accounting fraud cases. Coupled with recent statements by the SEC and the Department of Justice, it is clear that accounting fraud is a priority and that individuals are in the cross hairs.

This focus on accounting reflects a return to bread-and-butter issues that have been the agency's traditional focus, now that the financial crisis cases are largely behind it. The agency has signaled this trend for some time, through speeches by staff and commissioners.[1] The data support this shift: The number of accounting matters has increased by more than 40 percent from 2013 to 2014, and 2015 appears to be at least on par with the prior year. Indeed, the early part of September saw the SEC bring several financial reporting and accounting fraud actions over the span of a few days, demonstrating its commitment to this area. Below is a sampling of the most recent cases brought by the SEC.

- The SEC sued a former U.S. Attorney for allegedly making materially misleading statements and omissions to investors and auditors during his term as chairman of a publicly traded staffing services company.[2] The SEC also announced a settlement with the company's auditors relating to their allegedly deficient audits.[3] The entire matter centered on $2.3 million (half of the company's assets and most of its cash) that went missing and then reappeared under "suspect circumstances." The SEC alleged the former U.S. Attorney not only knew where the $2.3 million initially went and how it eventually came back to the company, but that he also was acting as the agent for a convicted felon, the alleged orchestrator of the entire scheme.

- The SEC announced that it had settled, for $15 million, accounting fraud charges against a company that operates an internet-based consumer banking and personal finance network.[4] The SEC alleged the company's former CFO, director of accounting, and vice president of finance had directed certain of the company's divisions to record unsupported revenue and had reduced or failed to book certain expenses, all in an attempt artificially to inflate its financial results to meet analyst earnings targets. The executives also allegedly provided misleading and generic explanations to auditors to justify the fabricated numbers. The former president of finance settled with the SEC, agreeing to pay a civil penalty, disgorge all ill-gotten gains, and accept five-year officer, director, and public-accounting bars.[5]

- The SEC reached an agreement with a sports nutrition company and four individuals, including the company's former audit committee chair, to settle a series of accounting and disclosure violations.[6] The SEC alleged the company's disclosures understated the perquisites paid to executives by almost $500,000. These included the use of a private jet, vehicles, meals, apparel, private golf club memberships, and medical costs for the birth of a child. The company also allegedly committed a number of other violations, including failing to disclose related party transactions, overstating revenue, and failing to implement internal accounting controls. The company agreed to pay a $700,000 penalty, and the executives who received the unreported perks agreed to pay $180,000 in penalties.

- The SEC filed civil charges against the former CEO and CFO of a bankrupt online video management company.[7] The SEC alleged the executives engaged in a number of schemes to falsify the company's financial statements so that it appeared more profitable. The executives allegedly caused the company falsely to recognize revenue from sales that were never consummated and diverted money from the company to create a slush fund that was then used to create phony reductions in receivables. The SEC also alleged the executives hid a $2 million loss of cash and, as a result of their various frauds, caused the company to file false and misleading forms with the SEC.

What This Means

These cases, as well as the recent guidance from the DOJ and the SEC staff and commissioners, provide several important lessons or reminders to public companies and their officers and directors:

The SEC is intensely focused on accounting fraud and looking to bring cases. This is clear from the guidance from senior SEC leadership, the creation of the Financial Reporting and Audit Group,[8] the increasing number of filed matters, and the increasing number of financial reporting-related whistleblower complaints that the SEC is pursuing. And while many of the recent matters look like simple fraud cases, management and audit committees should avoid complacency when it comes to financial reporting. The SEC is looking more closely at internal controls failures, multiple revisions that do not individually amount to a material error, accounting errors that might result from misjudgments about estimates or reserves, disclosures relating to executive compensation and related party transactions, and other areas that are beyond simple fraud.

The SEC and DOJ are focused on naming individuals, not just companies, in these cases. In all the recent accounting cases, the SEC has named individuals, including a former audit committee chair, partners, CEOs, CFOs, and accounting directors. In the most egregious cases, the government has also brought criminal charges against individuals. The recent DOJ guidance emphasizing the prosecution of individuals highlights the new risks that face both individuals and companies.[9]

Companies and boards must continue to focus on internal controls. This directive has been repeated over and over in SEC speeches, but it also comes through in the cases the agency has filed. Good controls can prevent fraud and accounting errors, or at least allow companies to detect such errors earlier. Companies and management must be diligent in not only putting appropriate and realistic internal controls in place, but also in adhering to them.

We are seeing the fruits of the SEC's whistleblower program: After being in place for more than three years, it is resulting in more whistleblower complaints, many of which relate to financial reporting and accounting and contain information the agency could not have obtained otherwise. This heightens the need for (i) strong procedures for promptly escalating and addressing whistleblower complaints internally and (ii) good controls for preventing retaliation against whistleblowers.

The risk of clawbacks against executives is also only increasing. Under Sarbanes-Oxley section 304 (and in the future under Dodd-Frank section 954),[10] executives face a fatal trap any time there is accounting or financial reporting misconduct. The best way to avoid the possibility of a clawback is to limit the opportunity and incentives for wrongdoing within the company.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

David Woodcock
Dallas
+1.214.969.3681
dwoodcock@jonesday.com

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

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

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

Peter J. Romatowski
Washington
+1.202.879.7625
pjromatowski@jonesday.com

Joseph Van Asten and Tyson Lies, associates in the Dallas Office, assisted in the preparation of this Commentary.

Endnotes

1 *See* Andrew Ceresney, Director, SEC Division of Enforcement, Address at the American Law Institute Continuing Legal Education (Sept. 19, 2013); Oversight of the SEC's Division of Enforcement before the S. Comm. on Financial Services, 114th Cong. 1 (2015) (statement of Andrew Ceresney, Director, SEC Division of Enforcement); Oversight of the SEC's Agenda, Operations, and FY 2015 Budget Request before the H. Comm. on Financial Services, 114th Cong. 1 (2015) (statement of Mary Jo White, Chair, SEC); Daniel M. Gallagher, Commissioner, SEC, Remarks at the 21st Annual Stanford Directors' College (June 23, 2015); Kara M. Stein, Commissioner, SEC, Address at the Institute of Chartered Accountants in England and Wales (Sept. 9, 2015).

2 Complaint, No. 1:15-CV-7077 (S.D.N.Y. Sept. 9, 2015).

3 *See id.*; Exchange Act Release No. 75,862, Accounting and Auditing Enforcement Release No. 3692 (Sept. 9, 2015); Exchange Act Release No. 75,859, Accounting and Auditing Enforcement Release No. 3689 (Sept. 9, 2015).

4 *See* Securities Act Release No. 9901, Exchange Act Release No. 75,849, Accounting and Auditing Enforcement Release No. 3683 (Sept. 8, 2015).

5 Litigation against the former CFO and director of accounting is ongoing.

6 *See* Securities Act Release No. 9903, Exchange Act Release No. 75,851 (Sept. 8, 2015); Securities Act Release No. 9904, Exchange Act Release No. 75,852 (Sept. 8, 2015); Securities Act Release No. 9905, Exchange Act Release No. 75,853, Accounting and Auditing Enforcement Release No. 3685 (Sept. 8, 2015); Securities Act Release No. 9906, Exchange Act Release No. 75,854, Accounting and Auditing Enforcement Release No. 3686 (Sept. 8, 2015); Exchange Act Release No. 75,855, Accounting and Auditing Enforcement Release No. 3687 (Sept. 8, 2015).

7 *See* Press Release, SEC, "SEC Charges Video Management Company Executives With Accounting Fraud" (Sept. 8, 2015). In a parallel action, the U.S. Attorney's Office has announced criminal charges against the executives.

8 *See* Stephanie Russell-Kraft, "SEC's 'RoboCop' Drags Agency Into 21st Century," Law360 (Aug. 21, 2015).

9 Jones Day *Commentary*, "U.S. Department of Justice Announces Updated Guidelines on Individual Accountability for Corporate Wrongdoing" (Sept. 2015).

10 Jones Day *Commentary*, "SEC Proposes Dodd-Frank Act Clawback Rules" (July 2015).

Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Accounting Fraud: Down, But Not Out

David Woodcock

Law360, New York (September 11, 2015, 10:38 AM ET) -- Accounting fraud is one of the most costly types of fraud, not just in dollars lost by investors or companies, but also in the way it erodes confidence in the capital markets. The last major accounting fraud scandal played out in the early 2000s. In the interim, we've had two historic pieces of legislation enacted, in part, to decrease the likelihood of another widespread accounting fraud scandal. And we've seen a sharp decline in the number of financial restatements, private securities class actions and accounting-related U.S. Securities and Exchange Commission enforcement actions.

Have the legislative fixes worked? Is there really less accounting fraud today? This article will take a brief look at why we might have seen a diminished amount of accounting fraud and then consider why celebrating its decline might be premature.

Why We Might See Less Accounting Fraud Today

1. Sarbanes-Oxley Worked

There is good evidence that Sarbanes-Oxley Act of 2002 has improved financial reporting quality by improving the audit profession, audit committees, internal controls and corporate and individual accountability.[1] There are also a smaller number of potentially high-risk companies because post-SOX, many went private or "dark."[2] Audit quality has improved, in part because of the Public Company Accounting Oversight Board. There have been far fewer restatements post-SOX, and they arise more often from unintentional errors, more likely come from noncore accounts, more likely have no impact on earnings, and elicit a lower average negative market reaction.[3]

In addition, audit committees are far more engaged. They are more attentive to potential whistleblowers, internal controls and the auditor relationship. SOX's requirement that CEOs and chief financial officers provide certifications regarding their company's financial statements and internal controls, along with the clawback risk in the event of a restatement, also may incentivize management. The recently proposed Dodd Frank clawback provision, which expands the scope of clawbacks, could further increase those incentives.[4]

2. Internal Controls Have Improved

Whether due to SOX, market pressure or regulatory scrutiny, there is evidence that internal controls at public companies have improved. Internal controls are one of the fundamental drivers of earnings quality.[5] Numerous studies show that firms with internal control weaknesses have accruals that are less consistent with cash flows, more auditor resignations, more restatements and SEC enforcement actions, less precise management forecasts, and CFOs with weaker qualifications.[6]

Better empowered and engaged audit committees, CEO/CFO certifications and improved auditing quality have helped improve internal controls. In addition, there is "significant evidence" that Section 404 reports — in which a company reports on the scope, adequacy and effectiveness of its internal control structure — "prompt companies to make managerial and governance improvements."[7] Researchers have documented a negative market reaction for material weakness disclosures, suggesting that investors value those disclosures.[8] Audit Analytics, an audit and accounting intelligence service and researcher, recently concluded that the relatively low number of restatements "is the positive effect of Sarbanes-Oxley section 404 and internal controls ... Everything

gets better after [Section] 404."[9] Finally, a recent survey of corporate leaders suggests that Section 404 has causally improved accounting quality and internal controls.[10]

3. Many Eyes Are On the Lookout for Fraud

The quest to find companies engaging in earnings management is far more sophisticated than it was even a few years ago, and this should make it more difficult to conceal accounting fraud.

Academics: There are now thousands of academic research papers on earnings management and accounting fraud, on the motivations, financial impacts and detection methods, among other things. They apply methods or concepts like Benford's Law, quadrophobia, Beneish M-Scores, F-Scores, and cash flow variances, and they draw correlations between CEO/CFO driving records and propensity for ostentatious lifestyles. Their work is being used by regulators and analysts to detect accounting fraud earlier.

Analysts and Short Sellers: In addition to the institutional and private fund analysts, there are now several intelligence firms focused on detecting accounting fraud and earnings management. Whether they're using quantitative analytics, fundamental analysis, or some combination, their work is contributing to the earlier detection of accounting fraud. And although short sellers are frequently wrong and regulators and others should subject their work to close scrutiny before acting on it, some believe they "help keep the market honest,"[11] thereby exposing fraud earlier.

Regulators: Most of the SEC's enforcement effort to combat accounting fraud is begun in response to restatements, self-reports, press accounts, etc. But in recent years, the agency has ramped up efforts to be more proactive in detecting accounting fraud. The SEC created the Fraud Task Force over two years ago, and the Division of Economic and Risk Analysis and the agency as a whole have increased their focus on accounting fraud.[12] The task force has now evolved into the "Financial Reporting and Audit Group," signifying a long-term interest by the agency's leadership.[13]

There is some evidence these beefed-up regulatory efforts, and more particularly, greater divisionwide focus on this area, may be having an effect. In 2014, for example, the SEC brought 46 percent more financial reporting fraud cases than it did the year before. From 2013 to 2014, there was a 47 percent increase in class actions alleging accounting violations, and more than one in four of those cases referred to an SEC inquiry or action (the highest level since this correlation began to be tracked in 2010).[14]

4. Whistleblowers Make Potential Violators Think Twice

It's fair to say the Dodd-Frank-created whistleblower program has been a success for the SEC. The volume and quality of tips the commission receives has gone up every year in the four years of the program. In 2014, the SEC received over 3,600 tips,[15] and the largest number of self-categorized tips alleged violations relating to corporate disclosures and financial statements: 630 or around 17 percent of all whistleblower complaints. For whistleblowers, the financial incentives are significant. The SEC has paid over $50 million in whistleblower bounties in the few years the program has been in operation.[16]

Not all whistleblower tips are useful, but there are instances where whistleblowers provide information the SEC is unlikely to obtain any other way. Whistleblower tips often include detailed analysis, key documents, and an insider's view of the fraud that proves integral to building a case. This means that corporate insiders are incentivized to nip a problem in the bud rather than allowing it to grow into a larger problem that might be reported to the SEC.

5. Other Possible Reasons

It is possible that the tone at the top and compliance culture improvements so often called for by companies, regulators, auditors, consumer groups and corporate attorneys have actually taken hold.[17] Moreover, the increase in corporate penalties could be deterring management from taking the risk of large-scale accounting fraud. Some recent prosecutions in this area may have the effect of reinforcing the message that the costs outweigh the benefits.[18]

Why Accounting Fraud Hasn't Gone Away

Despite these improvements in controls, detection and incentives, it is unlikely accounting fraud is on the brink of eradication.

1. People are Imperfect

Human nature has not changed in the last 20 years. The "fraud triangle," developed over 50 years ago, posits that when people are faced with certain pressures, have opportunities and can form rationalizations for misconduct, you have the necessary ingredients for accounting fraud.[19]

The pressures that might lead someone to commit accounting fraud include: desires to increase personal wealth or obtain promotions; efforts to maintain or elevate social status; attempts to escape from the penalties of poor performance; the desire to obtain a higher stock price or to meet the expectations of investors; or desires to postpone dealing with financial difficulties.[20] The rationalizations often used to excuse misconduct may include the notion that the conduct was within the bounds of an accounting gray area or was only going to be continued for a short time. The perpetrator might also rationalize that the fraud was necessary for deserved, but withheld, personal bonuses, was a short-term fix needed to protect jobs or the company, or was nothing different from what many other companies were already doing.[21]

The opportunities for accounting fraud are always present at the highest levels of the company, where many accounting frauds originate. This is largely because management almost always has the ability to override even effective internal controls.[22] The opportunities for accounting fraud are only enhanced by the persistent difficulty of its detection, despite the advances described above. In a recent survey of several hundred CFOs, many cautioned that earnings management is difficult to unravel from the outside.[23] One CFO stated that "the chances an analyst would spot an occasional instance of earnings management are low, and only persistent abusers have a high chance of being detected."[24] These revealing comments are supported by other studies,[25] one of which concluded: "there may be a persistent residual level of inappropriate conduct that cannot be eradicated."[26] If these surveys and studies are believed, there may be a lot of at least minor accounting fraud in our economy today.

2. Short-Termism Hasn't Gone Away

Related to the discussion of human nature is the problem of "short-termism," or the excessive focus on short-term results over long-term value.[27] Think of the focus on quarterly earnings. Former SEC Chairman Arthur Levitt decried the "runaway problem" of short-termism and earnings management back in 1998. Since then, we've had two massive financial crises (both caused in part by short-termism),[28] two historic regulatory responses, and an endless amount of ink spilled on the need to move away from the temptations of short-term thinking.

Surveys of financial executives demonstrate that the threat of short-termism is alive and well. One survey of several hundred financial executives, for instance, confirmed that many would take an action that is "value-decreasing for their firms to beat earnings expectations."[29] Furthermore, "[o]ver 80% of financial executives said they would decrease discretionary spending, such as advertising expenses, maintenance expenses, and research and development expenses, to meet earnings targets."[30] And "[o]ver 50% of financial executives said that they would 'delay starting a new project even if this entailed a small sacrifice in value to meet earnings expectations or to smooth earnings.'"[31] In another survey of business leaders, researchers found that only 49 percent of respondents at larger companies, and 35 percent of smaller companies, would be willing to miss earnings of up to 5 percent in the current period in order to pursue an investment that would boost profits by 10 percent over the next three years.[32]

Interestingly, not only does the market seem to fail to penalize short-termism,[33] the trading practices and decisions of so-called "transient" institutional traders — those with a short-term time horizon reflected by high-portfolio turnover and high-momentum trading — probably even lead to earnings management.[34] As SEC Commissioner Dan Gallagher recently suggested: "if individual and institutional investors are focused on the short term, it's no surprise that companies are in turn managing themselves for the short term.[35]

3. SOX May Have Helped, But It Isn't Perfect

SOX was focused on improving audit committees, auditing and internal control disclosures, not

directly on preventing fraud. Improvement in the three areas will at best minimize the opportunities for committing fraud, but the possibility of management override and collusion are inherent limitations of internal controls.[36]

SOX also may get credit for reducing the number of restatements, but it is unclear whether the reduced number of restatements is entirely positive. As noted in a recent article, managers are increasingly using earnings revisions, rather than Item 4.04 restatements, in order to handle errors quietly and therefore avoid clawbacks on executive bonuses and shareholder lawsuits.[37] In theory, frequent revisions could raise questions about the internal controls surrounding the accounts revised.

The increase in revisions coincides with companies' seeming hesitation to disclose material weaknesses in internal controls, perhaps to avoid negative market reactions that might follow. The SEC has expressed concern for several years that it is "surprisingly rare to see management identify a material weakness in the absence of a material misstatement."[38] The PCAOB has also noted this issue in the audit context.[39] This raises the concern that companies and their auditors are not adequately assessing and testing internal controls.[40] And on overall audit quality, the PCAOB continues to find deficiencies in the auditing of accounting estimates in areas such as revenue, allowances for loan losses, inventory reserves and fair-value measurements.[41]

Another possible reason to question the effectiveness of SOX is the 2008 financial crisis. Although designed to address accounting and auditing scandals, SOX does apply to internal controls across all industries, and the failure of internal controls played an undeniable role in the crisis.[42]

4. The Current Environment May Not Be Right for Large-Scale Accounting Fraud to Thrive, But That Doesn't Mean It Won't Return

The pressures to commit accounting fraud may not be as strong today. A manager's decision "to commit accounting fraud is related to macroeconomic conditions."[43] More specifically, "managers start committing accounting fraud during periods of strong macroeconomic performance, as measured by gross domestic product, and in the two years leading up to an economic peak."[44] And fewer managers tend to begin "committing accounting fraud in the two years following an economic trough."[45] A related pressure that drives earnings management is the desire to keep up with your competitors in the earnings race ("keeping up with the Joneses").[46] But if everyone in the market is facing tough economic conditions, then that pressure is less powerful.

Without getting into a detailed analysis of recent economic growth or the stock market's performance, it is clear that the years since the 18-month long recession that kicked off in December 2008 would likely not be considered "strong macroeconomic performance," and thus, we should not expect as much accounting fraud as we've seen in periods where there is strong performance.

However, these effects may not last forever. As the Ethics Resource Center put it in their 2009 National Business Ethics Survey, we "see an important connection between workplace ethics and the larger economic and business cycle: when times are tough, ethics improve. When business thrives and regulatory intervention remains at status quo, ethics erode."[47] Although this pattern may have been broken in the 2011 survey,[48] the ERC opined that the "soft recovery" post-recession "may have taken a toll on workers' confidence and tempered risktaking on the job."[49] The key question is what will happen when robust economic growth returns and executives and companies face greater pressures to perform or keep up with peers.

What Can We Say With Some Confidence About the Future of Accounting Fraud

The only thing that can be stated with certainty is that accounting fraud is unlikely ever to disappear completely. While conditions may not be prime right now, there is no guarantee that improved economic conditions or decreased regulatory focus could not pave the way for more widespread accounting fraud. And we can be pretty sure the next crisis won't look exactly like the last. Regardless of the overall trends, however, we know that companies with strong ethical and compliance cultures experience less fraud and discover it more quickly. So the best approach for those who want to avoid problems is to build and nurture an ethical and compliance culture that minimizes the pressures and opportunities that might tempt otherwise good people to engage in misconduct.

—By David Woodcock, Jones Day

David Woodcock is a partner in Jones Day's securities litigation and enforcement group in Dallas. He is a former chairman of the SEC Enforcement Division's Financial Reporting and Auditing Task Force and director of the SEC's Fort Worth, Texas, regional office.

The author would like to thank Peter Romatowski and Joan McKown, partners in Jones Day's Washington, D.C., office, and Tyson Lies and Katie Wall, associates in the firm's Dallas office, for their assistance on this article.

[1] Suraj Srinivasan, and John C. Coates IV, SOX After Ten Years: A Multidisciplinary Review 31 (Sept. 2014), http://dash.harvard.edu/bitstream/handle/1/12175242/Srinivasan_Suraj_J2_SOX%20After%20Ten%20Years%20-%20A%20Multidisciplinary%20Review.pdf? sequence=1; Adam Hartung, Benefits Of SOX And Dodd- Frank, Forbes Online (Aug. 16, 2015), available at http://www.forbes.com/sites/adamhartung/2015/08/16/ regulations-work-benefits-of-sox-and-dodd-frank/.

[2] Srinivasan & Coates, supra, at 16-20.

[3] Srinivasan & Coates, supra, at 33 (citing numerous studies).

[4] SEC Proposes Dodd-Frank Act Clawback Rules, Jones Day (July 2015), available at http://www.jonesday.com/sec-proposes-dodd-frank-act-clawback-rules-07-09-2015/.

[5] See, e.g., Jeffrey Doyle, Weili Ge, & Sarah McVay, Determinants of Weaknesses in Internal Control over Financial Reporting and the Implications for Earnings Quality, 44 J. Acct. & Econ. 193 (2007); Dain C. Donelson, Matthew Ege, and John M. Mcinnis, Internal Control Weaknesses and Financial Reporting Fraud 7 (May 2014), http://ssrn.com/abstract=2449287 or http://dx.doi.org/10.2139/ssrn.2449287.

[6] Srinivasan & Coates, supra, at 34.

[7] Id. at 60.

[8] Id. at 13.

[9] Maxwell Murphy, The Big Number, The Wall Street Journal CFO Journal Blog (Apr. 20, 2015), http://www.wsj.com/articles/the-big-number-1429577020.

[10] Cindy R. Alexandera, Scott W. Bauguess, Gennaro Bernile, Yoon-Ho, Alex Lee, & Jennifer Marietta-Westberg, Economic Effects of SOX Section 404 Compliance: A Corporate Insider Perspective, at 56 J. Acct. & Econ. 267, 268 (Aug. 2013); Srinivasan & Coates, supra, at at 34.

[11] James Surowiecki, In Praise of Shortsellers, The New Yorker (Mar. 23, 2015), available at http://www.newyorker.com/magazine/2015/03/23/in-praise-of-short-sellers; see Cory A. Cassell, Michael S. Drake &, Stephanie J. Rasmussen, Short Interest as a Signal of Audit Risk, 28 Contemp. Acct. Res. 1278 (Apr. 2011).

[12] Peter J. Henning, The S.E.C. Is 'Bringin' Sexy Back' to Accounting Investigations, New York Times Dealbook (June 3, 2013); Andrew Ceresney, Co-Director, Div. of Enforcement, Financial Reporting and Accounting Fraud, American Law Institute Continuing Legal Education (Sept. 19, 2013).

[13] Stephanie Russell-Kraft, SEC's '"RoboCop"' Drags Agency Into 21st Century, Law360 (Aug. 21, 2015), http://www.law360.com/articles/693679/sec-s-robocop-drags-agency-into-21st-century.

[14] Cornerstone Research, Accounting Class Action Filings and Settlements: 2014 Review and Analysis 1 (2015).

[15] Mary Jo White, Chair, Sec. & Exch. Comm'n, The SEC as the Whistleblower's Advocate (Apr. 30, 2015).

[16] Id.

[17] Ethics Resource Center, 2013 National Business Ethics Survey 14-17 (2013), available at http://www.ethics.org/downloads/2013NBESFinalWeb.pdf.

[18] Press Release, Dep't of Justice, Former Arthrocare Executives Sentenced for Orchestrating $750 Million Securities Fraud Scheme, U.S. Department of Justice (Aug. 29, 2014), http://www.justice.gov/opa/pr/former-arthrocare-executives-sentenced-orchestrating-750-million-securities-fraud-scheme.

[19] Joseph T. Wells, Principles of Fraud Examination 20 (2d Ed. 2008).

[20] Id. at 300-01.

[21] Id.

[22] Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934, 72 Fed. Reg. 35,324 (June 27, 2007) (codified at 17 C.F.R. pt. 241).

[23] Ilia Dichev, John Graham, and Shiva Rajgopal, Earnings Quality: Evidence from the Field 40-41 (Oct. 10, 2012).

[24] Id. at 40.

[25] Ernst & Young, 13th Global Fraud Survey, Overcoming Compliance Fatigue: Reinforcing the Commitment to Ethical Growth, 13th Global Fraud Survey 7 (2015); I.J. Alexander Dyck, Adair Morse, & Luigi Zingales, How Pervasive is Corporate Fraud? 4 (Rotman School of Mgmt., Working Paper No. 2222608, 2013) (finding that the probability of a company engaging in a fraud in any given year is 14.5%).

[26] Ernst & Young, supra, at 1.

[27] Lynne L. Dallas, Short-Termism, the Financial Crisis, and Corporate Governance, 37 J. Corp. Law 265 (2012).

[28] Id. at 268 n.7 (noting that it is generally accepted that short-termism contributed to both the most recent financial crisis well as the accounting scandals of the early 2000s).

[29] Id. at 280.

[30] Id.

[31] Id.

[32] Jonathan Bailey & Jonathan Saul Godsall, Focusing Capital on the Long-Term, Short Termism: Insights from Business Leaders 6 (Dec. 26, 2013).

[33] Dallas, supra, at 280-81.

[34] Id. at 302-06, 362.

[35] Daniel M. Gallagher, Commissioner, Sec. & Exch. Comm'n, Activism, Short-Termism, and the SEC: Remarks at the 21st Annual Stanford Directors' College n.50 (June 23, 2015).

[36] Donelson at 7.

[37] Christine E. L. Tan and Susan M. Young, An Analysis of "Little r" Restatements, 29 Acct. Horizons

668 (Sept. 2015).

[38] Brian T. Croteau, Dep. Chief Accountant, Office of the Chief Accountant, Remarks Before the 2013 AICPA National Conference on Current SEC and PCAOB Developments — Audit Policy and Current Auditing and Internal Control Matters (Dec. 9, 2013).

[39] PCAOB, Audit Committee Dialogue (May 2015), http://pcaobus.org/sites/digitalpublications/audit-committee-dialogue (noting that 83% of the restatements announced during 2013 and 2014 by companies required to report on ICFR had no material weakness reported in the ICFR opinion preceding the announcement); see Srinivasan & Coates, supra, at 14.

[40] Croteau, supra.

[41] PCAOB, Audit Committee Dialogue, supra.

[42] See, e.g., Press Release, Sec. & Exch. Comm'n, JPMorgan Chase Agrees to Pay $200 Million and Admits Wrongdoing to Settle SEC Charges (Sept. 19, 2013), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539819965 (citing firm's failure to establish and maintain internal controls); Press Release, Sec. & Exch. Comm'n, SEC Charges Bank of America With Securities Laws Violations in Connection With Regulatory Capital Overstatements (Sept. 29, 2014), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370543065483 (same).

[43] Robert H. Davidson, Accounting Fraud: Booms, Busts, and Incentives to Perform 4-5 (Jan. 26, 2011).

[44] Id. at 5.

[45] Id.

[46] Wells, supra, at 300-01.

[47] Ethics Resource Center, 2009 National Business Ethics Survey 2 (2009), http://ethics.org/files/u5/nbes-final.pdf.

[48] Id. at 11.

[49] Id. at 15-16.

INVESTIGATIONS QUARTERLY

RICK OSTILLER, rostiller@navigant.com
JOHN C. TANG, ESQ., jctang@jonesday.com

All Eyes on the Independent Investigation

Effectively managing an independent investigation

Illustration by Josh Leipciger

- The credibility of the investigation is of paramount importance.
- Accuracy, efficiency, proportionality, sound processes and judgment, active committee and Board involvement, and responsiveness to the company's various constituencies are all characteristics of a well-run investigation.
- The minimum investigation necessary to satisfy the business judgment rule in a court of law may not be enough to satisfy the court of public opinion or other interested third-party constituents such as the Securities and Exchange Commission (SEC), US Department of Justice (DOJ), and the company's outside auditors.

The financial crisis that started in late 2008 has led to a heightened focus on corporate governance and financial transparency, including the passage of the Dodd-Frank Act in 2010 and the implementation by the SEC of its whistleblower award program in 2011, not to mention corresponding litigation and criminal prosecution activity. These and other related developments have underscored the need for companies to have a plan in place to investigate and resolve issues promptly and effectively should problems arise.

When circumstances dictate that a company conduct a probe independently of management, the Board of Directors or a Board committee typically takes responsibility for managing the investigation with the assistance of outside advisors. Since an investigation can have far-reaching implications for an organization, the company's directors have an obligation to manage the project effectively, balancing often-competing considerations in the best interests of the company's stakeholders.

This article discusses several topics related to investigations, namely: 1) the factors a company should consider when determining whether to perform an independent investigation; 2) the initial steps a Board of Directors should take when an issue arises that merits an independent investigation; 3) keys to a well-run investigation; 4) common investigative challenges; and 5) reporting considerations.

Factors To Consider When Determining Whether To Perform an Independent Investigation

Depending upon the circumstances, management may advocate conducting an "internal" investigation by itself, rather than having the Board's independent directors and outside advisors perform an "independent" investigation. Understandable concerns about cost containment often influence management's desire to conduct an internal investigation. However, while an independent investigation may involve more time and expense, it undoubtedly carries significantly greater weight in the eyes of courts, regulators, auditors, and other interested third parties, such as the press, who may later judge the investigation with the benefit of hindsight. Consistent with the value placed on independent investigations, the Sarbanes Oxley Act of 2002 contains provisions permitting (although not requiring) companies to empower the audit committee and other independent Board committees to retain independent counsel and other advisors.

Who conducts the investigation can make a significant difference to regulators or other interested third parties. For example, in exercising their charging discretion, both the SEC and the DOJ give strong consideration to the company's investigation. A reliable and properly conducted investigation that is shared with the government can lead not only to reduced charges but even to no charges being filed at all.[1] However, the government can be a skeptical consumer. If it perceives an investigation is insufficiently independent because the person(s) conducting it is(are) deemed too familiar or too aligned with the potential subjects of the investigation, the investigators' work may not receive the full benefits that would otherwise accrue to an independent investigation. Similarly, while an investigation may provide the basis for a motion to dismiss a shareholder derivative lawsuit in its preliminary stages, the independence of the investigators is a key factor in the court's consider-

1. S.E.C. Enforcement Manual § 6.1.2; U.S. Attorney's Manual § 9-28.720.

ation of whether to defer to the findings of the company's investigation.[2]

The company's outside auditors, who generally work in parallel with the company's investigators, may also take a dim view of an investigation that isn't sufficiently independent. Maintaining the confidence of the outside auditors is obviously a critical objective. Often, the audit firm will have its own forensic accountants conduct a "shadow" investigation that is intended to monitor the work of the company's investigators. The primary goal of the shadow investigation is to ensure that the scope and process of the independent investigation is adequate and sufficiently robust to allow the auditors to rely on the findings.

In summary, the credibility of the investigation is of paramount importance. While an independent investigation can be more costly than a management-led process, it has greater impact, and if handled appropriately can be managed to keep costs under control.

Initial Steps a Board Should Take

If the Board decides to undertake an independent investigation, it often will form a special committee of independent (i.e., non-employee) directors to manage and oversee the investigation. For the reasons discussed above, it is essential that the members of the committee be disinterested and independent of any of the people, companies, and issues that could be the subject of the investigation. Although some types of connections between members of the committee and the subject(s) of the investigation (for example, common membership in a trade organization or social club) may not be legally disabling, the Board should identify and objectively consider *all* connections, however modest, at the time the special committee is formed.

Indeed, it is not unusual for a Board to appoint additional directors with no prior connection to the company, primarily for the purpose of constituting the special committee charged with conducting the independent investigation. Alternatively, the company's audit committee may lead the investigation (provided its members are not associated with the people, companies, and issues that prompted the investigation).

If the Board decides to form a special committee, the Board should establish a charter or resolutions that clearly delineate the committee's charge and authority. Among the matters that the charter or resolutions should specifically address are the committee's authority to retain outside advisors, incur costs, gain access to company information and personnel, and whether the committee is empowered with the full decision-making authority of the Board, or rather is empowered to recommend a course of action to the Board based upon the investigation's findings and conclusions.

The committee should promptly check that the appropriate persons have been directed to preserve relevant documents and information, and the committee should also evaluate the need to engage outside advisors to assist with the investigation. In addition, the committee should communicate with the company's outside auditors and work with the appropriate resources within the company (for example, the investor relations department) to plan for external communications regarding the investigation and the matters that prompted it. The recipients of such external communications will depend upon the circumstances, but often will include various regulators (SEC, DOJ, Financial Industry Regulatory Authority (FINRA), listing agencies, etc.), investors (individuals and institutional holders), market analysts, the press, and other interested third parties.

Keys to a Well-Run Investigation

Accuracy, efficiency, proportionality, sound processes and judgment, active committee and Board involvement, and responsiveness to the company's various constituencies are all characteristics of a well-run investigation. In addition to their fact-finding mission, the committee and its advisors must also consider the company's business, legal, reputational, and other interests surrounding the matters under investigation.

To the extent that the Board does delegate the investigation process to a committee or rely on the work of internal or external personnel, it is important to remember that in the end it is the Board's investigation, and the Board is the ultimate fact finder and decisionmaker (bearing in mind that, as circumstances warrant, a Board may decide to empower a committee with the Board's decisionmaking authority).

It is certainly appropriate for the directors to utilize and rely upon the help of others (such as outside advisors) in the investigation process. It is not expected or legally required that individual directors or committee members personally conduct the investigation without assistance. But, by the same token, the directors cannot discharge their fiduciary duties by "over-delegating" their responsibilities to the point of abdicating them. It is important to strike the right balance.

The Board, through its committee, should stay informed and remain actively involved throughout the investigation, by monitoring, overseeing, and directing the course of the work. Examples of oversight and direction include: meeting regularly with and obtaining regular reports from the outside advisors; providing feedback on the investigation; challenging the committee's advisors by raising questions and participating in decisionmaking; in certain circumstances, reviewing key documents and interview summaries prepared by the investigators; and formally making final findings of fact and decisions about any disciplinary actions, reporting, process remediation, or other measures arising from the investigation.

At a minimum, the investigation must be sufficiently thorough to satisfy the directors' fiduciary duty to ensure that the Board adequately investigates problematic issues that come to the Board's attention, and to make any remedial or process and control adjustments based upon the results of the investigation.[3] In this regard, the typical evaluation standard for the committee's investigation,

2. *Zapata Corp. v. Maldonado*, 430 A.2d 779 (Del. 1981).
3. *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).

whether carried out using internal resources or independent outside personnel, is the business judgment standard, which gives significant deference to a Board's considered judgment regarding the cost and scope of the investigation, as long as that decision is made in good faith and on an informed and disinterested basis. It is important to bear in mind, however, that the minimum investigation necessary to satisfy the business judgment rule in a court of law, may not be enough to satisfy the court of public opinion, or other interested third-party constituents such as the SEC, DOJ, and the company's outside auditors.

The investigative team should establish a work plan and be prepared to adjust it as the facts emerge and circumstances change. It is important for the committee and its advisors to be disciplined and thorough in identifying areas of inquiry and designing and carrying out the appropriate investigative steps. In addition, the team should remain flexible and willing to follow the investigation into additional areas as it learns information. At the same time, the committee should maintain its focus on the core investigation issues, and avoid unnecessary and expensive "scope creep." Therefore, the investigative team should carefully consider significant scope changes, and obtain Board or committee approval (as the case may be) before implementing them. If unrelated allegations arise during the investigation, the committee may responsibly determine to refer those matters to other constituencies within the company (including management and the legal department) for appropriate consideration.

In addition to interviews of relevant personnel, the team should preserve, collect, and review relevant documents (including electronic data) and perform financial or accounting analyses as needed. It is also very important to meet regularly with the company's outside auditors, who (as noted above) will ultimately need to concur with the scope and process of the investigation, particularly if it relates to internal controls over financial reporting or results in a financial restatement.

Common Investigative Challenges

Numerous challenges are bound to arise during the course of every investigation, no matter how well managed. One common investigative challenge is balancing the company's attorney-client privilege against responding to appropriate information requests from important third parties (such as regulators, auditors, and courts) about the investigation. Government regulators are generally prohibited from asking for privileged material and basing their charging decisions on whether the company will waive work product and the attorney-client privilege as part of its cooperation, although they will expect the company to provide "factual information."[4] This balance is often achieved by providing high-level status reports that convey the progress or results of the investigation without disclosing privileged details.

Another common challenge is for the committee to conduct its investigation while the company preserves its position with respect to threatened or pending litigation stemming from the matters under investigation. In addition to allocating limited resources and managing the company's ongoing responsibilities to its personnel, customers, and shareholders, the Board needs to remain attentive to coordinating the (at times conflicting) demands and strategies on both the litigation and non-litigation fronts. When and what steps are taken – or not taken – in one arena can have an unintended collateral impact on the other.

Yet another common challenge lies in the fact that the Board committee and its advisors conducting the investigation lack subpoena power. This circumstance can significantly hinder the investigators' ability to obtain cooperation and information from important third parties. An additional challenge for investigations that involve obtaining information from third parties outside the United States is the need to navigate the applicable laws and practices in the local jurisdiction. For example, state secrecy laws (such as those in China) or prohibitions on "US-style" discovery may pose a significant obstacle to gaining access (let alone timely access) to necessary information. A number of jurisdictions outside the United States also have expansive privacy statutes and data security laws that may limit the ability of a company's investigators to take documents and other information (including, for example, information obtained during interviews) out of that country – sometimes upon pain of criminal penalties. Therefore, it is essential to understand in advance and plan for the requirements and restrictions of non-US jurisdictions.

Reporting Considerations

With respect to reporting on the investigation, certainly the company must provide sufficient information about the investigation to meet applicable public reporting obligations. Beyond that, the company should consider the implications of disclosure about the investigation on potential shareholder or derivative litigation and regulatory action. Two of the most important reporting considerations are the report's format (oral vs. written, detailed vs. summary, exhibits vs. no exhibits, etc.) and the intended audience. Regulator and external auditor expectations, as well as the scope and nature of the findings (among other considerations), will all affect those decisions. The range of potential outcomes from an investigation will vary depending on the circumstances, but typical potential outcomes include:

- financial reporting restatements;
- corporate governance changes and internal controls enhancements;
- remedial actions, including termination/reassignment of and pursuing financial reimbursement from wrongdoers;
- regulator attention and monitoring; and
- shareholder litigation.

After the investigation, directors should follow up to ensure that recommended actions are implemented.

4. S.E.C. Enforcement Manual § 4.3; U.S. Attorney's Manual, § 9.28.720.

JONES DAY

APRIL 2014

COMMENTARY

Internal Investigations: Keys to Preparing an Effective Budget

Government prosecution of white collar crime has been on the rise in recent years. The uptick in enforcement activity is being felt across many industries and continues with, for instance, investigations into alleged violations of statutes carrying potentially devastating penalties, including the Foreign Corrupt Practices Act and the False Claims Act. The same trend can be seen on a global basis, with many international regulators focusing not only on local businesses but also on U.S. organizations with international operations. At the same time, organizations are increasingly relying on internal investigations to find the facts themselves and to assess any associated legal, financial, and reputational risks when evidence or an allegation of potential wrongdoing surfaces, whether or not a related government investigation is underway or anticipated. But investigation costs can escalate quickly, especially with investigations that cover much time and territory and that involve conduct that may expose the entity and individuals to serious criminal penalties and significant civil liability.

This Commentary summarizes the types of expenses that typically arise in an internal criminal investigation and offers guidance on how to budget for particular investigative activities. Although each budget will necessarily vary in its components and values, the hallmarks described below are relevant to setting the budget in virtually every internal investigation.[1] We conclude by offering a "checklist" of issues and tasks to consider in preparing an effective and efficient investigation budget.

Overview

To control costs without compromising the fundamental objectives of the investigation, corporations and their counsel may consider developing a budget at the outset of the investigation that—based on the best available information—makes appropriate assumptions about cost-influencing factors and assigns reasonable and realistic cost projections to the particular tasks that are expected to comprise the overall work plan. While developing a budget involves at least some measure of estimation, and may not be appropriate for every situation, companies frequently find budgeting helpful for understanding certain variables inherent in the investigative process, such as scope, timing, and resources, that can at times make the process seem unpredictable or even unsettling. Budgeting also facilitates communication between counsel and client about the client's specific goals.

Once developed, the budget should be reviewed regularly throughout the investigation. In this way, the initial assumptions and the task-based budgeted amounts (and therefore the aggregate budget) can be re-evaluated and modified as appropriate based on the actual conduct of the investigation and any unforeseen developments.[2]

Scoping and Planning

An effective internal investigation budget accounts for the costs of assessing the scope and goals of the investigation and developing a work plan to meet those goals. Time spent up-front gathering background information, identifying legal issues to be researched, and memorializing the scope and goals is critical to rightsizing the investigation—and budget—from the start. Like the budget, the work plan should be periodically evaluated and modified, if needed, as the investigation develops.

Data Preservation and Collection

In this age of emails, text messages, and other forms of electronic communication, the costs of identifying, preserving, and prioritizing relevant data are often major pieces of an internal investigation budget. In particular, the budget should account for the costs of issuing and monitoring a document hold, if applicable, and initial and ongoing collection, hosting, and storage costs. In many cases, it may be advisable to retain an external vendor to perform data collection and preservation tasks. Keep in mind that analyzing and navigating international privacy and state secret laws in foreign markets may drive up related costs—in some cases significantly.

Document Review

Depending on the nature of the investigation, the costs of reviewing and analyzing the data and hard-copy documents collected may constitute a large portion of the budget. Considerations here include (i) whether to use in-house resources, outside counsel, or contract attorneys to perform the various levels of the review, and (ii) whether the review presents foreign language challenges, such that foreign language reviewers or translators are required. In many cases, costs can be minimized by using contract attorneys to conduct the first-level review and by narrowing the universe of data by careful selection of custodians and the appropriate use of targeted terms, date ranges, and predictive coding.

Witness Interviews

Witness interviews are critical to extracting the facts in almost all 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 sources and locations of relevant information, in addition to the nature and extent of the witnesses’ own knowledge. These interviews typically entail less preparation than “substantive” interviews. While substantive interviews involve more intensive preparation, they are often critical to developing a comprehensive understanding of the conduct under investigation. The budget should reflect (i) the anticipated number of scoping and substantive interviews, and (ii) the total time expected to be devoted to preparation, participation, and memorialization. This information, coupled with individualized rate and fee information and any travel expenses, will enable a good-faith projection of interview-related costs.

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 identifying potentially problematic transactions, and the accounting treatment accorded thereto, and in reviewing related internal controls. Computer forensic experts are especially helpful when collecting and preserving large amounts of data and conducting analyses of computer data and systems. 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.[3]

Reporting and Recommendations

Preparing reports and recommendations and meeting with key stakeholders, including outside auditors and other outside counsel (e.g., the company’s securities disclosure

counsel and counsel for individual employees), are often key elements to conducting an internal investigation, and an effective budget accounts for associated costs. In this regard, considerations include the frequency and nature of the reporting, time and resources to prepare expected work product, and potential post-reporting follow-up items, including possible consideration and execution of self-disclosure.

Remediation and Personnel Matters

To the extent the investigative team is expected to be so involved, the budget should 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. 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 of or litigation with sanctioned employees, and (ii) to work with any counsel for individual directors, officers, and employees.

Cross-Border Considerations

Wherever an internal investigation extends into multiple jurisdictions, the budget should allow for specific costs that are needed to ensure that the investigation is conducted effectively, in compliance with local laws, and in such a way that any evidence collected can be properly relied on by the organization. Another key consideration is whether evidence collected can be protected from disclosure to the maximum extent permitted by local law.

Budgeting in these circumstances normally includes consideration of (i) the involvement of outside legal counsel, (ii) whether local laws require engagement with employee representatives (such as unions or works councils) as part of an investigation process, (iii) limitations on the processing and transfer of data from the local jurisdictions to the U.S. or elsewhere, and (iv) specific local laws that may affect the investigation process in certain jurisdictions. For example, compliance with state secret laws in certain jurisdictions (e.g., China) and the trend in Europe to tighten up data privacy regulations may be relevant factors in preparing an effective budget for cross-border investigations.

Tips for Containing Costs

If managed carefully from start to finish, an internal investigation—even a sizable, protracted one—does not have to devolve into a money pit. To the contrary, through some basic steps, internal personnel directly managing the investigation can instill appropriate discipline on the investigative process, and the organization as a whole can expect reasonable certainty as to budget projections.

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 forgoing some or all outside resources. However, cost savings should not be dispositive in preparing a budget for a criminal 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.[4]

- 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 electronically stored information ("ESI") collection and review and witness interviews, 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.
- 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 of the investigation and when to stop investigating (e.g., performing a "sampling" approach, instead of a review of all potentially relevant events or transactions, is often sufficient, as not all allegations that may hint at a possible violation of law or conduct standards necessarily merit the devotion of 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).

Budget Checklist

In sum, it is important for organizations to ensure not just that they get to the bottom of compliance concerns but also that this process is undertaken in a responsible, cost-effective way. In conjunction with the tips set forth above, a budget that touches on the items below can help achieve these ends.

Scoping and Planning
- Initial fact gathering (including scoping interviews)
- Legal research
- Developing work plan

Data Preservation and Collection
- Document hold
- Capturing ESI, hard drives, mobile devices, and servers
- Copying hard-copy documents
- Data archiving

Document Review
- First- and second-level reviews
- Training and monitoring
- Review platform
- Foreign language reviewers
- Translations

Witness Interviews
- Preparation and follow-up
- Foreign language translators
- Travel expenses

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

Remediation
- Compliance program and training
- Personnel changes

Personnel Matters
- Individual or pool counsel for personnel
- Potential employee severance negotiations and parallel litigation

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

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

Charles M. Carberry
New York / Washington
+1.212.326.3920 / +1.202.879.5453
carberry@jonesday.com

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

Randy S. Grossman
San Diego
+1.858.314.1157
rsgrossman@jonesday.com

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

Jonathan Leiken
Cleveland / New York
+1.216.586.7744 / +1.212.326.3771
jleiken@jonesday.com

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

Brian A. Sun
Los Angeles
+1.213.243.2858
basun@jonesday.com

Harriet Territt
London
+44.20.7039.5709
hterritt@jonesday.com

Hank B. Walther
Washington
+1.202.879.3432
hwalther@jonesday.com

Brooke Schultz, an associate in the San Diego Office, assisted in the preparation of this Commentary.

Endnotes

1 Alternative fee arrangements (e.g., flat fees or "success" fees) should be evaluated with great care in the context of internal investigations and should generally be avoided if they reasonably may be 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 To ensure protection under the attorney-client privilege and work-product doctrine, the investigation should be undertaken by the corporation's legal team or outside counsel, and 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. Budgets that are prepared for investigations undertaken by a non-lawyer or undertaken in the ordinary course of business, regardless of whether legal advice is sought, may not be protected under the attorney-client privilege and work-product doctrine.

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

4 A full discussion of issues and circumstances that may be relevant to a determination of whether to engage outside counsel and other third-party vendors in a particular matter is beyond the scope of this Commentary.

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

JONES DAY

AUGUST 2015

COMMENTARY

D.C. Circuit Prevents Disclosure of KBR's Internal Investigation Materials, *Again*

For the second time in as many years, the Court of Appeals for the D.C. Circuit struck down a district court order compelling KBR to turn over documents from an internal investigation conducted by KBR into allegations that it defrauded the U.S. government during the Iraq War. The district court initially ruled that KBR's internal investigation documents were not privileged because they were not prepared primarily for the purposes of seeking legal advice. Finding the documents privileged, the D.C. Circuit vacated that ruling and remanded to the district court, noting that the issue was "materially indistinguishable" from U.S. Supreme Court precedent in *Upjohn Co. v. United States*. But the district court, at the D.C. Circuit's invitation, entertained other timely arguments as to why the privilege should not attach, and once again it ordered disclosure of the internal investigation documents. The D.C. Circuit, however, disagreed and for a second time upheld privilege over the internal investigation documents, cautioning that the district court's reliance on the balancing test for Federal Rule of Evidence 612, the doctrine of "at issue" waiver, and the "substantial need" test "inject[ed] uncertainty into application of the attorney-client privilege and work product protection to internal investigations."

Background

KBR designated Vice President Christopher Heinrich as its Fed. R. Civ. P. 30(b)(6) witness on several identified topics, including a topic addressing any investigation or inquiry of the alleged fraud or any of the matters identified by the relator. At the outset of Heinrich's deposition, counsel for KBR offered a preliminary statement noting that KBR was making Heinrich available subject to claims of attorney-client privilege and work product protection.

During Heinrich's deposition, he testified that he reviewed the now-disputed documents relating to KBR's internal investigation in preparation for the deposition. On cross-examination by counsel for KBR, Heinrich testified that KBR had a contractual duty to report to the Department of Defense ("DoD") if it had reason to believe any violation of the Anti-Kickback Act may have occurred. He also explained that when KBR had made such reports to DoD in the past, that it had treated the investigation itself as privileged and never provided a copy of the investigation itself to the government.

Shortly after the deposition, KBR moved for summary judgment. KBR's memorandum in support of summary judgment acknowledged KBR's practice of making disclosures to the government where an investigation revealed reasonable grounds to believe a violation may have occurred. The memorandum also acknowledged that KBR intended for its investigations to be protected by privilege but noted that it had not asserted privilege over the fact that internal investigations have occurred or the fact that KBR had made disclosures to the government based on those investigations. Finally, the memorandum acknowledged that KBR performed an investigation related to the relator's claims and made no disclosure to the government following that investigation. The memorandum also attached excerpts from Heinrich's testimony and referenced the deposition language in the Statement of Material Facts to Which there is No Genuine Dispute.

Applying a balancing test, the district court on remand found that KBR had to produce the documents under Federal Rule of Evidence 612 on the basis that KBR waived privilege when Heinrich reviewed the documents in preparation for his deposition. The district court also found that KBR impliedly waived privilege under the "at issue" doctrine. After rejecting KBR's request to amend its pleadings to strike the sections that created a waiver, the district court issued a separate order finding that the documents were discoverable fact work product and the relator had shown "substantial need."

Waiver Based on Review in Preparation for Deposition

On appeal from the district court's second ruling, the D.C. Circuit found that the district court erred in applying a balancing test under Federal Rule of Evidence 612. The D.C. Circuit noted that the Rule 612 balancing test applies only where a document is used to refresh a witness's memory. In other words, the writing must have influenced the witness's testimony to be discoverable.

Heinrich did not consult the materials during his deposition, nor did he testify as to the substance of those documents or any other privileged element. Further, as noted by KBR's counsel during the deposition, while Heinrich reviewed the materials prior to the deposition, the company "would not concede that it was for the purpose of refreshing recollection so that he could testify because [KBR has] always consistently taken the position that those reports are subject to the company's attorney-client privilege and attorney work product." The D.C. Circuit agreed and refused to find testimonial reliance to justify application of the balancing test.

Moreover, the D.C. Circuit also held that, even if consideration of the balancing test had been appropriate, the district court erred in its application of that test. Noting that in most cases, 30(b)(6) witnesses who examine privileged materials before testifying will not waive privilege, the district court nonetheless found that fairness dictated disclosure here because of Heinrich's and KBR's repeated suggestion that the documents contain nothing. The D.C. Circuit rejected the district court ruling because it failed to give due weight to the privilege and protection attached to the internal investigation materials and because it would allow privilege claims over internal investigations to be routinely defeated by noticing a deposition on the topic of the privileged nature of the investigation. This result would directly conflict with *Upjohn*, which teaches that an uncertain privilege is little better than no privilege at all. The D.C. Circuit also found the relator's position that KBR erred by producing a 30(b)(6) witness that had actually reviewed the internal investigation materials "absurd" because such a rule would encourage parties to provide less knowledgeable corporate representatives.

Implied or "At Issue" Waiver

The D.C. Circuit also rejected the district court's conclusion that KBR impliedly waived any protection over the documents in dispute because it actively sought a positive inference in its favor on what it claimed the internal investigation documents showed. The district court reasoned that KBR attempted to use its privilege claim as a sword and a shield by using the fact that it conducts investigations and makes disclosures when it has reasonable evidence of a violation to establish an inference that it had no reasonable evidence of a violation here, since it conducted an investigation but did

not make a disclosure. The district court further emphasized that KBR itself had put the materials "at issue" when it solicited Heinrich's testimony on the materials, attached excerpts from the testimony to its motion for summary judgment, referenced the deposition language in its statement of material facts to which there is no genuine dispute, and discussed the "investigative mechanism" in its brief.

Acknowledging that the attorney-client privilege cannot be used as both a sword and a shield, the D.C. Circuit also recognized that general assertions lacking substantive privileged content are insufficient to justify waiver. As to the deposition testimony and the statement of material facts, the D.C. Circuit found that "as a matter of logic—neither could possibly give rise to an inference that places the contents of the deposition at issue." The deposition is merely a record of what Heinrich said, not an argument, and the statement of material facts does not create any inferences to be made or contested in the statements alone. The D.C. Circuit did, however, recognize that waiver could occur during a deposition or statement of material facts where partial disclosure of privileged materials was made.

The D.C. Circuit went on to note that the reference to the investigation in the summary judgment memorandum presented a more difficult question because "a factfinder could infer that the investigation found no wrongdoing." Nonetheless, the D.C. Circuit rejected the district court's position that KBR was asking it to draw an "unavoidable" inference—that the investigation uncovered no wrongdoing. Instead, the D.C. Circuit opined that a different inference could be made—that the investigation showed wrongdoing but KBR made no report to the government. Further, the circuit court noted that because all inferences were to be drawn against KBR in its motion for summary judgment, the district court could not make any inference in KBR's favor based on the contents of the privileged documents. In other words, the district court was prohibited from even making the most favorable inference that it concluded was "unavoidable." In any event, the D.C. Circuit noted that the memorandum merely included a recitation of facts, not an argument or claim concerning the privileged materials.

"Substantial Need"

Finally, the D.C. Circuit disagreed with the district court's order directing KBR to produce certain portions of the report on the basis that the materials were nonprivileged fact work product discoverable based on substantial need. While agreeing with the district court on the law, and rejecting KBR's assertion that everything in an internal investigation is protected by the attorney-client privilege, the D.C. Circuit found that the district court misapplied the law to the documents it ordered to be disclosed.

The circuit court concluded that even a cursory review demonstrated that many of the documents were protected by the attorney-client privilege and that other documents contained the mental impressions of the investigators. Thus, the district court committed clear error in concluding that the materials were only fact work product. Because the district court failed to distinguish between fact and opinion work product, the circuit court did not reach the "substantial need" and "undue hardship" questions.

Recommendations

While the D.C. Circuit's ruling reaffirms the protections from disclosure provided by the attorney-client privilege and work product doctrine, as a matter of practice, counsel should carefully consider its approach before conducting any internal investigation. Counsel should be especially mindful that materials that qualify as work product, but that do not fall under the attorney-client privilege, may be subject to disclosure, especially when the materials constitute fact work product. Further, counsel should be careful in its public use of or reference to privileged or work product protected investigative materials so as to avoid impliedly waiving protection. Likewise, counsel should advise 30(b)(6) witnesses not to disclose the contents of such investigative materials when providing testimony. While statements regarding the existence of such materials generally will not result in waiver, revealing the substance of those materials likely will.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Peter F. Garvin III
Washington
+1.202.879.5436
pgarvin@jonesday.com

J. Andrew Jackson
Washington
+1.202.879.5575
ajackson@jonesday.com

Heather O'Shea
Chicago
+1.312.269.4009
hoshea@jonesday.com

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

Tina M. Tabacchi
Chicago
+1.312.269.4081
tmtabacchi@jonesday.com

Grant H. Willis Washington
+1.202.879.3847
ghwillis@jonesday.com

D. Grayson Yeargin
Washington
+1.202.879.3634
gyeargin@jonesday.com

Ryan P. McGovern and Mark R. Lentz, associates in the Washington Office, assisted in the preparation of this Commentary.

JONES DAY

SEPTEMBER 2015

COMMENTARY

SEC Brings Hiring Practices into FCPA Focus

The SEC recently fined Bank of New York Mellon ("BNY Mellon") nearly $15 million for allegedly violating provisions of the Foreign Corrupt Practices Act ("FCPA") by providing student internships to family members of foreign government officials in the Middle East.

Importantly, several other banks have publicly disclosed investigations into similar conduct.[1] It is unclear whether those banks will be subject to public enforcement action by the SEC, but there are certainly lessons to be learned from these investigations that apply far beyond the banking industry.

Important Facts Noted by the SEC in the BNY Mellon Order

- The bank, without admitting or denying wrongdoing, agreed to pay $14.8 million—$8.3 million in disgorgement, $1.5 million in prejudgment interest, and a $5 million penalty to settle the charges. The investigation took more than four and a half years to complete.
- BNY Mellon was alleged to have violated the FCPA in 2010 and 2011 when employees of the bank agreed to provide valuable internships to family members of two officials affiliated with a Middle Eastern sovereign wealth fund. In this manner, the bank allegedly improperly provided a "thing of value" (i.e., internships) to government officials in order to win and retain business.
- The three recipients of the coveted intern positions—specifically, the son and nephew of one official and the son of a second official—were exempted from the otherwise rigorous hiring criteria for such positions and were allegedly unqualified.
- Though the interns lacked the requisite credentials and were never under consideration for becoming fulltime employees of the bank, several internal emails showed that BNY Mellon employees viewed the internships as important to keeping the sovereign wealth fund's business.
- Notably, in its order, the SEC alleged that the conduct by BNY Mellon employees in bestowing the internships not only violated the anti-bribery provision of the FCPA but also the internal accounting controls provision.
- Though the bank did have an FCPA compliance policy, it maintained few specific controls around the hiring of customers and relatives of customers. The SEC alleged the compliance controls therefore were inadequate to fully effectuate BNY Mellon's stated policy against bribery of foreign officials.

Takeaways from the SEC's Settlement with BNY Mellon

The SEC continues to broadly interpret "anything of value." This settlement demonstrates that the phrase "anything of value" is not limited to direct or indirect cash payments or travel benefits. As in the line of charitable contribution cases,[2] the SEC continues to look at nontraditional transactions—if the conduct falls within what it views to be the spirit of the FCPA. This case signals the SEC is on the lookout for any quid pro quo arrangement that directly or indirectly provides something of value to a foreign official as part of a scheme to obtain or maintain business.

Furthermore, the SEC reiterated that the internal controls provision has a far reach—BNY Mellon "failed to devise and maintain a system of internal accounting controls around its hiring practices sufficient to provide reasonable assurances that its employees were not bribing foreign officials in contravention of company policy."

Compliance program must consider all parts of the organization. All parts of an organization should be included in an FCPA compliance program. During the annual evaluation of FCPA compliance, BNY Mellon's internal—and perhaps external—audit should have evaluated the HR practices for compliance with the FCPA policies and procedures.

Training needs to be done regularly and across the organization: keep it updated, do it regularly, and use web-based or other alternative methods of training to make it more convenient. Consider all lines of business and support functions in your corruption risk assessment. Written policies and procedures must be supplemented by real compliance controls.

Compliance must avoid the "check the box" mentality. The U.S. government has warned that "[c]ompliance programs that employ a 'check-the-box' approach may be inefficient and, more importantly, ineffective."[3] The SEC, in this case and prior guidance, makes it clear that having sufficient FCPA policies in place is of little value if the organization does not monitor conduct to ensure the policies are being followed.[4] Here as elsewhere, the only thing worse than having no policy, is to have a policy—good or bad—that is not consistently followed. Adoption of the policy proves that you knew what the law requires, and ignoring the policy proves that your conduct was deliberate.

The SEC continues to be aggressive. The BNY Mellon order notes the many remedial measures that were put in place by BNY. However, the SEC brought the case and extracted a $5 million penalty and $8 million in disgorgement. It is relevant to note that the alleged misconduct relates to a business practice not clearly discussed in the FCPA Resource Guide. The lesson: there is little sympathy from the government regarding FCPA compliance missteps.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

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

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

David Woodcock
Dallas
+1.214.969.3681
dwoodcock@jonesday.com

Arielle S. Tobin, an associate in the Dallas Office, assisted in the preparation of this Commentary.

Endnotes

1 Enda Curran and Jean Eaglesham, "Regulators Step Up Probe Into Bank Hiring Overseas," *The Wall Street Journal* (May 6, 2014), http://www.wsj.com/articles/SB10001424052702303417104579546190553220338.

2 The Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission, *A Resource Guide to the U.S. Foreign Corrupt Practices Act* at 16-17, http://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf, "FCPA Resource Guide."

3 *Id*. at 57.

4 *Id*. at 58-62.

JONES DAY

MARCH 2015

COMMENTARY

Revisiting My Brother's Keeper: Latest Learning and Best Practices on Dealings with Third Parties under the FCPA

Over the past decade, one of the most common and perplexing questions posed by U.S. multinational corporations with respect to compliance with the Foreign Corrupt Practices Act ("FCPA") is, "Am I my brother's keeper?" Corporations and their personnel have long struggled, and continue to struggle today, to answer this question as it relates to third-party intermediaries, including distributors, resellers, service providers, and other business partners who may put the company in harm's way. In 2012, the issuance of the FCPA Resource Guide by the United States Department of Justice ("DOJ") and Securities and Exchange Commission ("SEC") shed some light on this question. Since then, lessons learned from specific cases and broad experience in this area merit renewed discussion of third-party dealings.

The FCPA and the "Agency" Doctrine

As applied to organizations and corporations, the FCPA governs the extraterritorial activity of all U.S. issuers and companies, along with their non-U.S. subsidiaries, affiliates, joint venture partners, and agents. In an effort to prevent, and to criminalize, willful ignorance of FCPA violations, the statute contains express provisions prohibiting corrupt payments made by a third party on a company's behalf. As will be discussed further below, the extent of a company's liability for the corrupt actions of third parties requires an analysis of that relationship, most importantly as to the potential creation of an agent relationship. Should that third party be determined to be an agent of the parent company, the DOJ and SEC, as reflected in the Resource Guide, would take the position that the FCPA will reach the acts of those agents undertaken within the scope of their duties intended to benefit the company. A review of just a few enforcement actions made public since the release of the Resource Guide serves to highlight the practical implications of this policy for U.S. multinationals.

In April 2013, the DOJ and SEC announced the resolution of a matter that illustrates a dual-threat involving foreign agents. A U.S.-based provider of drilling services admitted to using a freight forwarder to fraudulently avoid the payment of Nigerian customs duties and tariffs on equipment exported to that country. Compounding the company's wrongdoing, the U.S. company then provided more than $1 million to an agent in order to corruptly influence a Nigerian government panel reviewing the avoidance of those duties and tariffs. Using this money to entertain members of the government panel, the agent was able to reduce the fine levied by the Nigerian government on

the U.S. company from almost $4 million to just $750,000. The U.S. company entered into a deferred prosecution agreement ("DPA") with the DOJ to pay nearly $12 million in penalties and more than $4 million in disgorgement and prejudgment interest in a related SEC resolution. This matter underscores the risk of attempting to insulate the company through the use of foreign third parties to engage in misconduct on its behalf.

In July 2013, the DOJ announced the superseding indictment against two former executives of a multinational energy company and its U.S.-based subsidiary. The charges, which include violations of the FCPA and money laundering statutes, stem from a systematic bribery scheme that made corrupt payments to Indonesian officials in order to secure a $118 million power-supply contract to the country. According to the charges, the bribes were paid out through the deliberate use of consultants, who were retained specifically to funnel payments to officials in order to win the contract. A seemingly damning series of emails recounts the executives' frustration with the lack of headway made by one consultant and the hiring of a second consultant. Of particular note with respect to the hiring of this second consultant, it appears that the company did not adhere to its standard practice of paying consultants on a pro rata basis and instead made one large payment up front in order to facilitate the corrupt payments to the Indonesian officials.

In November 2013, three subsidiaries of a multinational oil services company that publicly trades in the U.S. pleaded guilty to violating the FCPA, among other crimes. Court documents indicate that the company failed to establish an effective system of internal anticorruption controls, despite the high corruption risk present in its industry and global operations. Thus, when employees of a subsidiary set up a joint venture in Africa with local foreign officials, the company failed to detect the joint venture's role as a conduit to funnel corrupt payments to these officials. In another scheme, employees of a different subsidiary in the Middle East awarded improper discounts to a distributor who supplied the company's products to a government-owned national oil company. These discounts, in turn, were used by the distributor to generate bribes to officials at the state-owned company. The multinational agreed to pay more than $252 million in penalties and fines to the DOJ, SEC, and a host of other U.S. agencies.

In December 2013, a Ukrainian subsidiary of the Archer Daniels Midland Company ("ADM") pleaded guilty to violating the FCPA and agreed to pay more than $17 million in criminal fines. The charges related to a years-long system wherein the subsidiary paid third-party vendors, which bribed Ukrainian government officials for unearned tax refunds. The corrupt payments were brought to the attention of ADM executives, but that knowledge did not result in any enhanced antibribery controls at the company or its subsidiaries. ADM itself entered into a non-prosecution agreement ("NPA") and agreed to pay more than $36 million in disgorgement and prejudgment interest to the SEC as a result of this failure to maintain an adequate compliance regime.

In July 2014, the SEC announced that it had charged Smith & Wesson Holding Corporation with violating the FCPA. As set forth in the SEC's order instituting a settled administrative proceeding, Smith & Wesson hired third-party agents to assist with sales of firearms to law enforcement agencies in Pakistan, Indonesia, Turkey, Nepal, and Bangladesh. In the course of this relationship with these third parties, Smith & Wesson employees endorsed and authorized their agent's provision of gifts (including firearms as "test" samples) and cash payments to officials in order to consummate the sales. Ultimately, the SEC order found that Smith & Wesson violated the antibribery, books and records, and internal controls provisions of the FCPA. These findings were based, at least in part, on the absence of any due diligence performed on these third-party agents, as well as the lack of internal controls over the payment of commissions to these agents and provision of firearms as "test" samples. Smith & Wesson agreed to pay $2 million in disgorgement, prejudgment interest, and penalties. Smith & Wesson also agreed to a two year period of self-reporting and, as part of its demonstrated remediation efforts, terminated its entire international sales staff.

And finally, in December 2014, a U.S.-based company, along with its wholly owned Chinese subsidiary, entered into a $135 million settlement with both the DOJ and SEC for violating the books and records and internal controls provisions of the FCPA. The factual allegations stated that in order to secure a license for direct sales under newly instituted Chinese regulations, the Chinese subsidiary gave $8 million in payments and gifts to government officials. In addition, the DOJ and

SEC alleged that the Chinese subsidiary made these payments to secure favorable media coverage—and to suppress negative media coverage—that would have decreased the likelihood of any license approval. At the time the settlement was announced, the DOJ and SEC made clear that the U.S. company initially attempted to hide the improper payments made by its subsidiary and ceased the activity upon receipt of a whistleblower complaint.

The International Arena: Local Enforcement on the Increase

The playing field for multinational companies has grown immeasurably more complex over the past several years, not only as a result of U.S. enforcement actions but also due to the increase in both the number of foreign countries passing similar anticorruption statutes and the upswing in enforcement of bribery laws already on the books. Brazil presents an excellent example of both of these paradigms.

First, in August 2013, the nation passed a landmark anticorruption law that governs the conduct of Brazilian companies, either within Brazil or abroad, as well as the operations of foreign-owned entities in Brazil. The law took effect in January 2014 and enforcement activity will continue to be closely watched to determine both the law's efficacy and the resolve of the Brazilian government to pursue prosecutions.

Second, even before the passage of the anticorruption law, the Brazilian enforcement authorities were clearly beginning to press harder in conducting bribery investigations. In November 2011, the Brazilian aircraft company Embraer SA, which trades publicly on the New York Stock Exchange, announced in a filing that it had received an SEC subpoena seeking information related to possible FCPA violations. This news was followed by disclosure of a joint investigation by U.S. and Brazilian authorities into bribery allegations stemming from Embraer's sale of aircraft to at least three other countries. The company stated that it was cooperating with agencies from both the U.S. and Brazil. The Embraer investigation, then, not only predates the new Brazilian anticorruption law, but it also would appear to provide precedent for future collaboration between Brazil and enforcement agencies from other nations.

India stands out not only as another economic power on the rise, but also as a nation with an apparently increasing commitment to pursuing corruption charges against third-party intermediaries acting on behalf of foreign multinationals. In June 2013, the Central Bureau of Investigation ("CBI") filed bribery charges against the Indian representative of a German defense manufacturer. The bribes were reportedly funneled through a U.S.-based third-party intermediary in order to corruptly influence the proposed blacklisting of the German firm by Indian government contractors. CBI's pursuit of corruption allegations is unlikely to wane anytime soon, as in 2013 the Indian government began aggressively investigating Italian and British firms for bribery related to a multimillion-dollar defense deal. The recent passage of the Lokpal Bill will also add to the recent anticorruption trend in India, as the law will establish an independent authority with a mandate to inquire into corruption allegations against public officials.

When it comes to violations of the FCPA, China has long ranked as one of the countries with the highest risk of corruption activity. Yet due to a high-visibility anticorruption campaign by the Chinese government, violations of the FCPA and U.S. law no longer remain the sole concern of multinational corporations operating in China.

No case better illustrates this fact than the Chinese Ministry of Public Security's investigation into the British global pharmaceutical company GlaxoSmithKline ("GSK"). The Chinese authorities allege that GSK funneled millions of dollars to government officials, doctors, and hospitals in order to secure prescriptions of the company's drugs. These payments were funneled through travel agencies in the form of trips, entertainment, and cash. Like many corruption investigations in China, the alleged GSK misconduct was likely revealed through one or more whistleblowers within GSK's China operations.

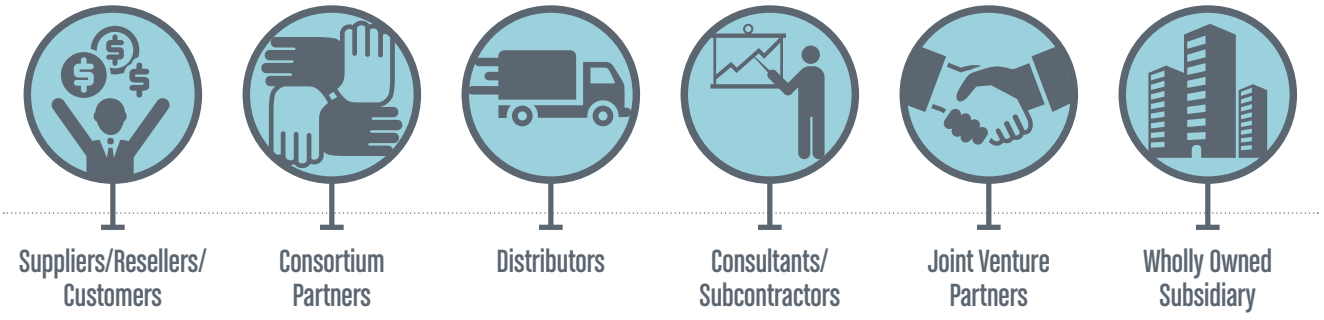
The Chinese government ultimately imposed a fine of nearly $500 million for these bribery allegations in September 2014, but this will surely not be the last such financial penalty imposed for this type of conduct. Throughout 2014, there was a clear signal that the Chinese authorities are continuing to investigate foreign pharmaceutical companies, with several

companies making public announcements that their China offices had been searched and their employees interviewed. In almost every case, the corrupt payments were made to doctors through third parties and concealed as research grants, consulting fees, or remuneration for conducting clinical trials.

Oh Brother, Who Art Thou?

For a multinational seeking to manage its third-party business relationships and mitigate risk associated with anticorruption enforcement, the above review of recent enforcement actions portrays a daunting landscape in need of the most careful navigation. Fortunately, these actions, as well as the guidance propounded by the DOJ and SEC, do provide a roadmap to avoiding the potential FCPA perils accompanying a company's use of third-party intermediaries.

In answering the frequent question—"Am I my brother's keeper?"—a company first must answer this question: "Who is my brother?" In practical terms, this means that the company must assess the nature of those third-party relationships in order to determine whether an agency has been created. This stage of the analysis is critical, as it not only provides a useful gauge to measure the potential risk posed by the third party's conduct, but the results of this analysis also will govern the compliance program that should be implemented with respect to that third party. A handy yardstick in conducting this analysis is the amount of control retained and exercised by the parent company over the third party, regardless of the type of person or entity involved (e.g., subsidiary, distributor, consultant, contractor). The formal contractual arrangements that established this relationship are but one factor in need of close review, as the day-to-day interactions between the parent company and third party are equally important in determining control and, as a result, potential liability. Below is a chart outlining possible business relationships established by a multinational during the course of its overseas operations:



For those third-party relationships falling to the left-hand side of the chart, the parent company is, in comparison to those relationships toward the right of the chart, generally less likely to have maintained the level of knowledge and control that would give rise to the creation of an agency relationship. The arrangements depicted toward the right of the chart are typically more formalized and part of the parent company's routine business operations in the foreign country, and as such generally more likely to create an agency relationship.

Thus, while each relationship of course must be evaluated in light of the circumstances involved, the key danger zone in assessing the existence of an agency relationship often lies in the middle of this chart—third-party intermediaries such as distributors, consultants, and subcontractors. As borne out by the above review of anticorruption enforcement actions, these are the third-party relationships most likely to run afoul of bribery and corrupt payment statutes. As with any fact-based assessment, the more detail that is obtained with respect to the analysis, the better the results. Thus, a parent company should carefully review the contractual terms of the consultant or distributor (or, preferably, use a company-standard set of contracts containing anticorruption provisions), the method and frequency of payment, the scope of the duties and responsibilities undertaken by the third party, any required periodic reporting on expenditures and sales by the third party, and the level of technical or logistical support provided by the parent company. Ultimately, though, the inquiry should steer back to the question of control: How much authority does the parent company maintain to direct the activities of this third party?

All in the Family

When designing a system of compliance measures relating to anticorruption, it is useful to keep one eye on the above chart. For those less risky business relationships on the far

left of the chart, experience suggests that monitoring and compliance with anticorruption laws is perhaps best managed by the business operations personnel who have the most frequent contact with the third party. Indeed, in many overseas settings, these "third parties" are in fact customers of the parent company; the exercise of audit rights or insistence on mandatory compliance training, then, could obviously be seen as an onerous and possibly counterproductive method of enhancing compliance.

In those instances where the relationship does not lend itself to these more probing compliance steps, the parent company should certainly consider the need for heightened internal due diligence with respect to those third parties. Such steps can include consistent and regularly reviewed payment terms for those third parties, additional scrutiny on the third party's claimed expenses (especially for travel, entertainment, and leisure), and required documentation as proof that work has actually been performed. The following chart, when used along with the companion chart on page 4, can help a company to plot out the most effective course in avoiding anticorruption violations and maintaining an effective system of compliance.

Thus, when introduced at the lowest and most personal level, the least intrusive of these compliance measures are likely to result in a heightened awareness of anticorruption with the third party. By providing notice of a company's anticorruption policy and requiring an annual certification that the third party will comply with that policy, the parent company has, at the very least, initiated a conversation between the third party and the company's representative about the need to maintain a corruption-free business model. For most relationships between the company and its customers or consortium partners, this may prove to be sufficient. Whether the parent company will need to adopt additional internal controls relies to a large degree on the risks presented with respect to the third party: Does the company's industry, geographic area of operations, or the third party itself (e.g., a consultant who advertises close ties to government officials) merit additional scrutiny from the parent company? As for those relationships with tighter parent company control and direction, such as a wholly owned subsidiary or a joint venture, a stricter regime of compliance measures may be necessary after accounting for these same risk factors.

So when asked, "Am I my brother's keeper?," arriving at an answer requires care and analysis and, most critically, the exercise of judgment. Perhaps the most important first step that a company's leaders can take is asking the question in the first place. Since the answer requires ever more inquiry, and ever more thought, the process of seeking that answer may not turn up a simple "yes" or a "no." What will be answered during that process, though, is what really matters to a multinational company facing a complex, global array of interweaving anticorruption requirements: Are we at risk and, if so, what steps can we take to protect ourselves?

Further Information

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Authors

Karen P. Hewitt
San Diego

Theodore T. Chung
Chicago

Hank Bond Walther
Washington

Justin E. Herdman
Cleveland

Authors Karen Hewitt, Ted Chung, Hank Walther, and Justin Herdman are former federal prosecutors and members of Jones Day's global Corporate Criminal Investigations Practice, which defends corporations in government inquiries and in conducting internal corporate reviews around the world. Ms. Hewitt, Partner-in-Charge of the Firm's San Diego Office, was the United States Attorney for the Southern District of California. Mr. Chung was an Assistant United States Attorney in the Northern District of Illinois and is currently the Practice Leader for Jones Day's Corporate Criminal Investigations practice. Mr. Walther was Chief of the Department of Justice Health Care Fraud Unit and, before that, Deputy Chief of the FCPA Unit. Mr. Herdman was an Assistant United States Attorney in the Northern District of Ohio and, before that, a prosecutor in the Manhattan District Attorney's Office.

Lawyer Contacts

Henry W. Asbill
Washington
+1.202.879.5414
hasbill@jonesday.com

James C. Dunlop
Chicago
+1.312.269.4069
jcdunlop@jonesday.com

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

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

Shireen M. Becker
San Diego
+1.858.314.1184
sbecker@jonesday.com

Randy S. Grossman
San Diego
+1.858.314.1157
rsgrossman@jonesday.com

Thomas P. McNulty
Chicago
+1.312.269.4142
tpmcnulty@jonesday.com

Brian A. Sun
Los Angeles
+1.213.243.2858
basun@jonesday.com

Jean-Paul Boulee
Atlanta
+1.404.581.8456
jpboulee@jonesday.com

Justin E. Herdman
Cleveland
+1.216.586.7130
jherdman@jonesday.com

Matthew D. Orwig
Dallas / Houston
+1.214.969.5267 / +1.832.239.3798
morwig@jonesday.com

Hank Bond Walther
Washington
+1.202.879.3432
hwalther@jonesday.com

Charles M. Carberry
New York / Washington
+1.212.326.3920 / +1.202.879.5453
carberry@jonesday.com

Brian Hershman
Los Angeles
+1.213.243.2445
bhershman@jonesday.com

Daniel E. Reidy
Chicago
+1.312.269.4140
dereidy@jonesday.com

James R. Wooley
Cleveland
+1.216.586.7345
jrwooley@jonesday.com

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

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

Peter J. Romatowski
Washington
+1.202.879.7625
pjromatowski@jonesday.com

Roman E. Darmer
Irvine
+1.949.553.7581
rdarmer@jonesday.com

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

Kerri L. Ruttenberg
Washington
+1.202.879.5419
kruttenberg@jonesday.com

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

Weston C. Loegering
Dallas
+1.214.969.5264
wcloegering@jonesday.com

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

SEC Names Erin Schneider as Associate Regional Director in San Francisco Office

FOR IMMEDIATE RELEASE
2015-16

Washington D.C., Jan. 28, 2015 — The Securities and Exchange Commission today announced that Erin E. Schneider has been named the Associate Regional Director for enforcement in the San Francisco office.

Ms. Schneider began working in the San Francisco office in 2005 as a staff attorney and became an Assistant Regional Director in 2012. She has served as a member of the Division of Enforcement's Asset Management Unit since its inception in 2010. In her new role, Ms. Schneider will oversee the San Francisco office's enforcement efforts for northern California and the Pacific Northwest.

"Erin is a savvy, accomplished, and dedicated investigator and manager," said Andrew J. Ceresney, Director of the SEC's Division of Enforcement. "I am pleased that she will continue her distinguished record of service in this new role in San Francisco."

Jina L. Choi, Director of the San Francisco Regional Office, added, "Erin is an outstanding lawyer who has been instrumental in the success of the San Francisco office. Her judgment, critical thinking, and work ethic are widely respected throughout the office. She is going to do an excellent job leading our talented enforcement staff."

Ms. Schneider said, "It has been a great privilege to work alongside so many talented, creative, and hardworking investigative and trial attorneys for the past 10 years. I am honored by this appointment and look forward to continuing the San Francisco office's strong tradition of tough but fair enforcement in complex and cutting-edge cases as well as its effective collaboration between examination and enforcement staff."

Ms. Schneider has investigated and litigated significant enforcement actions involving a variety of securities law violations. Some examples include:

- An accounting fraud case against a Silicon Valley company that included the return of $2.5 million in CEO bonuses and stock profits under the clawback provision.
- An enforcement action against a Bay Area hedge fund manager for misappropriating millions of dollars in side-pocketed assets.
- Charges against private investment fund managers and others stemming from an investigation of secondary market trading in pre-IPO companies.
- A jury trial in San Jose, Calif., that found a Silicon Valley CFO liable for a fraudulent stock option backdating scheme.

Prior to joining the SEC staff, Ms. Schneider worked as a litigation associate in the Washington D.C. and San Francisco offices of Gibson, Dunn & Crutcher LLP, and as an auditor at PricewaterhouseCoopers LLP. Ms. Schneider earned her bachelor's degree in business administration from the University of California at Berkeley in 1995, and her law degree cum laude from the University of California's Hastings College of the Law in 2001.

Edward J. Westerman, CPA, CFE

Senior Managing Director — Forensic & Litigation Consulting

edward.westerman@fticonsulting.com

One Front Street

Suite 1600

San Francisco, CA 94111

Tel: +1 415 283 4251

CERTIFICATIONS

Certified Public Accountant

Certified Fraud Examiner

PROFESSIONAL AFFILIATIONS

American Institute of Certified Public Accountants

Association of Certified Fraud Examiners

California Society of Certified Public Accountants

EDUCATION

M.B.A., Finance, University of Wisconsin

B.S., Accounting, Marquette University

Edward Westerman is a Senior Managing Director at FTI Consulting and is based in San Francisco. He has more than 20 years of experience providing consulting services regarding forensic accounting, auditing, internal controls, corruption and compliance, and financial damages.

Mr. Westerman is engaged by counsel representing companies and board of director committees to conduct internal investigations in connection with subpoenas, government inquiries, and whistleblower allegations concerning accounting and financial reporting fraud and misappropriation of assets. These projects have been in the US as well as foreign jurisdictions and have pertained to revenue recognition, reserves, stock option granting practices, embezzlement, insider trading, registration issues, and financial reporting disclosures. He has assisted with materiality assessments, financial restatements, and internal control and remediation measures.

In addition, Mr. Westerman is regularly retained in various securities litigation and white collar defense matters surrounding auditing, technical accounting issues and alleged fraud. Throughout his career, Mr. Westerman has also provided assistance to counsel, buyers and sellers regarding working capital adjustments, post-closing balance sheet adjustments, earn out calculations, and breach of reps and warranties. He has served as the neutral accounting arbiter adjudicating these disputes.

Mr. Westerman also has significant experience quantifying financial damages in large class action, breach of contract, wrongful termination, and other commercial disputes.

Mr. Westerman has testified at deposition, arbitration, and state court and has served as an arbiter, special master, and third party neutral in various engagements. During his career, he has participated in numerous speaking panels and other presentations regarding forensic accounting topics.

Prior to joining FTI Consulting, Mr. Westerman was a Managing Director, Leader of the Forensic Accounting practice, and Executive Director of the Litigation, Forensics & Finance business segment of LECG. He was also a Partner in the Forensic Accounting practice of Deloitte & Touche.

John C. Tang

Partner, Jones Day

Securities Litigation & SEC Enforcement

jctang@jonesday.com

San Francisco
1.415.875.5892
1.415.875.5700 (F)

John Tang represents companies, directors, and officers in SEC enforcement matters, internal investigations, and shareholder litigation. He also counsels clients regarding corporate governance, Rule 10b5-1 trading plans, and D&O insurance. He has advised numerous audit committees and independent directors on fiduciary duties, internal controls, compliance, public disclosures, and other issues.

Prior to joining Jones Day, John was co-chair of the securities litigation group at an international law firm, where he also served as firmwide chair of recruiting. He was previously based in Silicon Valley, and has represented public and private companies across the tech sector and in a range of other industries. John's experience also includes matters involving US-listed Chinese companies and their executives, and China-based operations of multinational corporations.

John is a frequent speaker on a variety of securities litigation and enforcement topics. He is also the former board president of the Asian Law Alliance, a San Jose-based nonprofit organization that provides legal services, community education, and advocacy programs to the Asian Pacific Islander community in Silicon Valley.

Areas of Focus

SEC Investigations & Proceedings

Internal Investigations, Corporate Compliance Programs & Employee Misconduct

Securities Fraud Class Actions

Shareholder Derivative Actions

Honors & Distinctions

2015 *Northern California Super Lawyers* – Securities Litigation

Recognized in *Benchmark Litigation*, with the 2015, 2014, 2013, and 2010 guides citing him as a "star" in securities and professional liability, and the 2008 guide noting that he is "terrific in securities"

Recognized in *Legal 500 US* (2008) for securities litigation

Languages

Conversant in Mandarin and Cantonese

Education

Columbia University (J.D. 1996); Yale College (B.A. 1991)

Bar Admissions

California and New York

Clerkships

Law Clerk to Chief Judge Edward N. Cahn, U.S. District Court, Eastern District of Pennsylvania (1997-1998)