Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

By Tom Fox

A Guide to

Effective Internal Investigations

COMPLIANCE WEEK

Compliance Week, published by Wilmington Group plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives.

Table of Contents

Author's Note

Internal controls have long been an overlooked requirement under the U.S. Foreign Corrupt Practices Act. This book continues my series of short works designed to provide clear and useful guidance to the compliance practitioner on a topic specific to anti-corruption compliance. Thanks to Matt Kelly, editor at Compliance Week, for providing me a platform to publish my book, and to Aarti Maharaj, digital content editor, Compliance Week for keeping it fresh and real.

Part I – Introduction

The call, e-mail, or tip comes into your office: An employee is reporting suspicious activity somewhere across the globe. That activity might well turn into a Foreign Corrupt Practices Act issue for your company. As the chief compliance officer, it will be up to you to initiate the process that will determine, in many instances, how the company will respond to misconduct as it relates to the FCPA. This book is designed to give you all the steps you will need to consider going forward.

This scenario was driven home in an FCPA enforcement action brought by the Securities and Exchange Commission in July 2015 involving Mead Johnson Nutrition Co. The company performed two internal investigations into allegations that its Chinese business unit was engaged in misconduct that violated the FCPA. Unfortunately the first investigation performed in 2011 did not turn up any evidence of FCPA violations. It was not until 2013, when the SEC made an inquiry to the company, that Mead Johnson performed an adequate internal investigation, which uncovered FCPA violations. Marc Bohn, writing in the FCPA Blog, said, "Investigations that lack sufficient depth, resources, or forethought can pose significant risk because they increase the likelihood that something critical will be overlooked, potentially permitting misconduct to continue unabated."

Another example of a botched internal investigation comes from France, where in January 2011, the French carmaker Renault fired three top officials for allegedly selling secret information regarding the company's electric car program. These allegations were based upon information that supposedly came from an unknown informant. This information claimed that the three terminated officials had large Swiss bank accounts funded by monies, which came from the sale of this information. This unknown informant was paid for his information by two Renault security department employees and then allegedly paid onto another party, who eventually passed along some or all of the Renault payment to the informant.

Not only is the regulatory pressure great, there are serious litigation and public relations costs if you do not get your investigation performed correctly.

As reported in the *Wall Street Journal*, the inquiry began in August 2011, with an anonymous letter to company officials, that one of the now terminated employees was overheard "negotiating a bribe." By December, the company's security department had "assembled elements pointing to the existence of bank accounts in Switzerland and Liechtenstein." The accused employees were terminated in January 2011. Unfortunately for the company, the state prosecutor assigned to the case later said that his investigation showed that the three did not have bank accounts in those countries.

This bungled investigation led to the rather remarkable spectacle in March 2011 of the chief executive officer of the French car maker Renault apologizing on national television for the wrongful termination of three company officials for improper allegations of industrial espionage. In addition to this apology, he offered to meet the men and propose that they rejoin the company. They also would be offered compensation, "taking into account the serious hurt that they and their families have suffered." This mishandled investigation around allegations of bribery and corruption is a very large reason why companies need to get investigations done right. Not only is the regulatory pressure great, there are serious litigation and public relations costs if you do not get your investigation performed correctly.

Moreover, the risk of bribery and corruption has not lessened. Unfortunately, it does not appear companies have put in adequate compliance programs in place to protect themselves going forward. In its *12th Annual Global Fraud Survey*, EY noted some disturbing trends. Regarding the overall risks of bribery and corruption, the survey noted that 39 percent of respondents reported that bribery or corrupt practices occur frequently in their countries. Even with third parties generally recognized as the greatest compliance risk, the survey noted that only 59 percent of respondents report using an approved supplier database. Finally, and perhaps most troubling, was the reported finding that 15 percent of CFOs surveyed would be willing to make cash payments to win or retain business. All of these numbers make clear that internal investigations will be a critical component of a *best practices* compliance program going forward. This book will provide you with the tools to design and implement an effective internal investigation program for your company.

Part II – Investigation Planning

A. The Investigation Protocol

Your company should have a detailed written procedure for handling any complaint or allegation of bribery or corruption, regardless of how that allegation is communicated. The mechanism could include the internal company hotline, anonymous tips, or a report directly from the business unit involved. You can make the decision on whether or not to investigate in consultation with other groups such as the audit committee of the board of directors or the legal department. The head of the business unit in which the claim arose may also be notified that an allegation has been made and that the compliance department will handle the matter from there.

Through the use of such a detailed written procedure, you can work to ensure complete transparency on the rights and obligations of all parties once an allegation is made. This allows the compliance department to have not only the flexibility, but also the responsibility, to deal with such matters. Then you can assess and decide how to manage the matter.

In a presentation by Jay Martin, vice president, chief compliance officer, and senior deputy counsel for Baker Hughes Inc., and Jacki Trevino, senior consultant at SAI Global, titled, "FCPA Compliance Best Practices: Success Stories of Robust and Effective Anti-Corruption Compliance Programs in High Risk Markets," they presented the specifics of an investigation protocol.

The five steps were:

1. Opening and categorizing the case;
2. Planning the investigation;
3. Executing the investigation plan;
4. Determining appropriate follow-up; and
5. Closing the case.

You should notify the relevant individuals, including those on your investigation team and any senior management members under your notification protocols.

If you follow this basic protocol, you should be able to work through most investigations in a clear, concise, and cost-effective manner. Furthermore, you should have a report at the end of the day that should stand up to later scrutiny if a regulator comes looking. Finally, you will be able to document, document, and document—not only the steps you took, but also why you did; and what outcome was achieved.

Step 1: Opening and categorizing the case. This is the triage step. You should notify the relevant individuals, including those on your investigation team and any senior management members under your notification protocols. After notification, you should assemble your investigation team for preliminary meetings and assessments. Step one should be accomplished one to three days after the allegation comes to the attention of the compliance department, either through your reporting structure or other means.

Given the numerous ways that information about violations or potential violations of the Foreign Corrupt Practices Act can be communicated to the Department of Justice (DoJ), having a robust triage system is an important way that a company can bring the right number of resources to bear on an FCPA problem. A key consideration is making an initial determination of whether to bring in outside counsel to head up an investigation and a determination of the resources that you may want or need to commit to a problem.

Step 2: Planning the investigation. After assembling your investigation team, which should include some or all of the following disciplines: legal, forensic accounting, compliance, IT, and audit, the next step is to determine the required investigation tasks. These would include document review and interviews. If hard drives need to be copied or documents put on litigation hold or sequestered in any way, or if relationships need to be analyzed through relationship software programs or keyword search programs, this should also be planned out now. These tasks should be integrated into a written investigation or work plan so that the entire process going forward is documented. Also, if the investigation itself varies from the written investigation plan, such variation should be documented and an explanation should follow. Lastly, if international travel is required, consider and plan for it during this step. Step two should be accomplished within another one to three days.

Step 3: Executing the investigation plan. Under this step the investigation should be conducted and completed. I would urge that the interviews not be done until all documents are reviewed and ready for use. Care should be taken to ensure that an appropriate Upjohn warning is issued—that is, that the interview subject clearly understands that whoever is performing the interview represents the company and not the person being interviewed, regardless of whether the person is the target of the investigation. The appropriate steps should also be taken to preserve the attorney-client privilege and attorney work product assertions. Step 3 should be accomplished in one to two weeks.

Step 4: Determining appropriate follow-up. At this step, the preliminary investigation should be completed. You are now ready to move into the final phases of determining and implementing the appropriate remediation and closing the matter. In some investigations, it is relatively easy to determine when the work is essentially complete. For example, if the allegation is both specific and narrow, and the investigation reveals a compelling and benign explanation for the alleged conduct, then the investigation typically is complete and you are ready to convene the investigation team and the relevant business unit representatives. This group would decide on any appropriate disciplinary actions to take (including no action at all). Step four should be completed in one day to one week.

Beware that during this step, if there are findings of specific or discrete allegations of corruption and bribery, the company must decide how to handle such findings going forward.

Step 5: Closing the case. Under this final step, communicate the investigation results to the stakeholders and complete the case report. Everything done in the above steps should be documented and stored electronically and in hard copy format. The case report should be completed. This Step 5 should be completed in one day to one week.

Another approach was suggested by Carol Switzer, president of the Open Compliance and Ethics Group (OCEG), in its *GRC Illustrated Series* on anti-corruption issue management. OCEG has created a significant number of guides to illustrate various topics in compliance and ethics. They are very useful tools to present via visual information areas of compliance programs, which can be used to describe compliance processes. In the offering on anti-corruption issue management, Switzer laid out a four-step process that allows you to think about your approach.

> A company should investigate by collecting, reviewing, and analyzing the evidence.

A. Capture and Filter. A company should establish "multiple pathways" to receive tips on potentially corrupt activity. Further, a company should monitor high-risk activity and relationships based upon "identified factors including country, sales channel, and third-party compliance data." Some of these data sources could include continuous controls monitoring, controls violations that are noted, hotlines and informal intakes, third-party or customer reports, audits (both internal and external), interviews, third-party due diligence, or media reports of other companies, locations, sales models, or conduct.

These mechanisms could raise a number of issues that should be investigated more thoroughly. Such issues could include allegations of commercial bribery, customs and offset commitments, out-of-policy gifts, entertainment and travel, misreported accounting records, cash vendor disbursements and other high-risk transactions, charitable giving and commission payments, and unusually high or too-frequent facilitation payments.

B. Review. If an issue is raised, the first thing you need to do is secure your records to prevent the loss or destruction of any data, and to preserve attorney-client privilege to the best extent possible. Next you should triage and assess the threat and rank it by risk level. The third step should be to determine your reporting obligations within the company. If you have a pre-existing contingency plan, you should report to those persons listed in the plan for the level of risk assessed. From this step you should execute a defined plan for the identified risk level, and then refer the matter to the designated investigation and communication teams.

This approach emphasizes the need for high-level oversight, whether that is a corporate board of directors or something akin to the board of trustees at a college or university. Senior management and the board of directors need to be informed about potential issues of bribery and corruption early, and should be kept abreast of the investigation as it progresses and "take a hands-on approach to ensure protection of the organization and resolution of the issue."

C. Resolution. This step involves a tri-parte approach. First, a company should investigate by collecting, reviewing, and analyzing the evidence. Pay attention to the issues that cannot be resolved quickly, those that may require re-assignment and notice to either senior management or the board of directors. Second, the company should execute a communications plan for management, employees, and external stakeholders. This communications plan should keep the appropriate level of management informed on the change in status of any issue throughout the investigation. Lastly, the company should obtain an independent report and resolve any signals of systemic violations, and ensure that unlawful conduct has been terminated and the appropriate disciplinary actions taken. This final step should present senior management with the requisite information to make business decisions about changes in business operations, and the discipline of employee, contractors, and business partners.

Additionally, the company should define the legal strategy it will pursue if a violation is determined. Under the FCPA, this could include an evaluation of whether the company should self-disclose to the Justice Department and/or Securities and Exchange Commission. Finally, the company needs to be prepared to defend its reputation. OCEG suggests that the company identify those who will speak on the company's behalf and to the extent possible have a consistent, controlled, and truthful message. This final point of the messaging emphasizes the need for communications in the soft skill toolkit of a compliance practitioner.

D. Continuous Improvement. The process should not stop at the conclusion of each issue resolution. OCEG suggests that a company conduct a root-cause analysis including "leadership weaknesses, culture issues, and flaws in the performance of management activities and controls." Patterns both in relationships and the aggregate should be analyzed and reviewed. Continuous controls monitoring of compliance internal controls should also be implemented.

B. The Fair Process Doctrine

At this point in your investigation, there is a concern you should consider—a concern that should guide many of the decisions that you will have to make going forward. It is the issue of procedural fairness. This is termed the "Fair Process Doctrine."

This doctrine generally recognizes that there are fair procedures (not arbitrary ones) in processes involving rights. Considerable research has shown that people are more willing to accept negative, unfavorable, and non-preferred outcomes when they arrive at processes and procedures seen as fair. Adhering to the Fair Process Doctrine will help you maintain credibility with the rest of the workforce and the regulators who review any investigation results going forward.

The first area is that of internal company investigations. If your employees do not believe that the investigation is fair and impartial, then it isn't fair and impartial. Further, those involved must have confidence that any internal investigation is treated seriously and objectively. I have written about several aspects of internal investigations to emphasize how to handle internal whistleblower complaints in light of the Dodd-Frank Act implications. One of the key reasons employees will go outside a company's internal hotline process is because they do not believe that the process will be fair.

If your employees do not believe that the investigation is fair and impartial, then it isn't fair and impartial.

This fairness has several components. One would be the use of outside counsel, rather than in-house counsel, to handle the investigation. Moreover, if a company uses a regular outside law firm, it may be that other outside counsel should be brought in, particularly if regular outside counsel has created or implemented key components of whatever is being investigated. Further, if the company's regular outside counsel has a large amount of business with the company, then that law firm may have a vested interest in maintaining the status quo. Lastly, the investigation may require a level of specialization that in-house or regular outside counsel does not possess.

As important as the Fair Process Doctrine is for all those reasons, still, I have come to believe it is more important in another area: the administration of discipline after any compliance-related incident occurs. Discipline must not only be administered fairly; it must be administered uniformly across the company for the violation of any compliance policy. Simply put, if you are going to fire employees in South America for lying on their expense reports, you have to fire them in North America for the same offense. It cannot matter that the North American employee is a friend of yours, or worse yet, a "high producer." Failure to administer discipline uniformly will destroy any vestige of credibility that you may have developed.

Part III – Selection of Investigative Counsel

In an article in the *Compliance and Ethics Professional Magazine*, August 2011 titled, "Foxes and Henhouses: The Importance of Independent Counsel," Dan Dunne, a partner at the law firm of Orrick Herrington & Sutcliffe, discussed what he termed a "critical element" in any investigation: a "fair and objective evaluation." Dunne wrote that a key component of this fair and objective evaluation is "the who question": who should supervise the investigation and who should handle the investigation? Dunne's clear conclusion is that independent counsel should handle any serious investigation.

Dunne lists three factors that should prompt a company to retain independent counsel for internal investigations of serious whistleblower complaints. First, for any corporate ethics policy to be effective, it must be perceived to be fair. If your employees do not believe that the investigation is fair and impartial, then it is not fair and impartial. Further, those involved must have confidence that any internal investigation is treated seriously and objectively.

Second, if regular outside counsel investigates their own prior legal work or legal advice, Dunne believes that "a plethora of loyalty and privilege issues" can come up in the internal investigation. It is a rare legal investigation where the lawyer or law firm that provided the legal advice, and then investigates anything having to do with the said legal advice, finds anything wrong with the prior counsel they have provided to the company. (If I am asked to investigate the quality of my own legal advice, I can probably tell you now that it was quality legal advice.) Dunne also notes that if the law firm that performs the internal investigation has to waive attorney-client privilege, it may also have to do the same for all its legal work for the company.

While general counsels and compliance officers may be up to speed on outsourcing critical inquiries, managers in business segments often are not; they frequently reply that they've "got someone" in the company who "takes care of that stuff."

The third point Dunne raises is the relationship of the regular outside counsel with regulatory authorities. If a company's regular outside counsel performs the internal investigation and the results turn out favorably for the company, the regulators may ask if the investigation was a whitewash. If a regulatory authority such as the SEC or Justice Department cannot rely on a company's own internal investigation, it may perform the investigation all over again with its own personnel. Further, these regulators may believe that the company, and its law firm, engaged in a cover-up. This is certainly not the way to buy credibility.

Mara Senn, a partner at the law firm of Arnold & Porter who specializes in FCPA investigations, has explained that the lawyer or law firm representing the company can go a long way toward establishing credibility. She noted that, "For those of us who regularly appear before the government, we already have credibility, and they understand that the client may or may not agree with recommendations we make, and they know that we'll be a straight shooter once we're in front of them." But it is more than the lawyer or law firm that brings credibility; the actions of the company matter as well. Of course this means the steps the company has taken, and its cooperation with the government during the pendency of the FCPA investigation, are what's important.

The late, great compliance practitioner Jim McGrath, writing in the *Internal Investigations Blog*, noted that despite the fact that using specialized investigation counsel is a best practice well worth the money, convincing decision makers on this point is difficult. This is particularly true when speaking with mid- or small-sized companies that are part of larger supply chains. While general counsels and compliance officers may be up to speed on outsourcing critical inquiries, managers in business segments often are not; they frequently reply that they've "got someone" in the company who "takes care of that stuff." It is clear, however, that such an approach will be more costly to a company in the long run. McGrath emphasized the need for independent counsel for serious corporate investigations.

Moreover, if serious allegations are made that your company's employees are engaging in criminal conduct, a serious response is required. Your company needs to hire good lawyers to handle any internal investigation. These lawyers need to have independence from the company, so do not call your regular corporate counsel. Hire some seriously good investigative lawyers. This may well mean you need *specialized* outside counsel.

McGrath and David Hildebrandt wrote about the use of specialized outside counsel to lead an independent internal investigation as compliance and ethics best practices in an article titled, "Risks and Rewards of an Independent Investigation," ACC Docket 29, no. 8 at 38 (Oct. 2010). This is based on the U.S. Sentencing Guidelines, where a scoring system is used to determine what a final sentence should be for a criminal act. Factors taken into account include the type of offense involved and the severity of the offense, as well as the harm produced. Additional points are either added or subtracted for mitigating factors. One of the mitigating factors can be whether an organization had an effective com-

pliance and ethics program. McGrath and Hildebrandt argue that a company must have a robust internal investigation to score well, too. Typically what the DoJ wants to see is a well-thought-out investigation protocol, which is followed in the investigation, with independent counsel; all well-documented so regulators can test any part of the investigation.

The authors suggest that in such a situation, a company should engage specialized counsel to perform the investigation, for three reasons. First is that the Justice Department will look toward the independence and impartiality of such investigations as one of its factors in favor of declining or deferring enforcement. If in-house counsel were heading up the investigation, the DoJ might well deem the investigative results "less than trustworthy."

A second reason came from the company's perspective. Many companies have sought protection of investigations behind the shield of the attorney-client privilege and attorney work-product doctrine. If an in-house attorney is used, many courts are skeptical of a company asserting the privileges because of the mixed responsibilities of counsel in a corporation; that of legal and business work. As noted by Russ Berland in an article in the *Society of Corporate Compliance and Ethics Magazine* titled, "How to Protect Compliance Risk Assessments From an Unwanted Disclosure," some courts "presume that in-house counsel engage in a substantial amount of non-legal work." Additionally, obstructionist attempts by corporations to assert the privilege improperly have led courts to refuse to allow the privilege to be asserted. Usually, however, a company will not face these arguments when it uses outside counsel.

Even if the company is willing to waive its attorney-client privilege, McGrath and Hildebrandt offer a third reason to use specialized outside counsel to handle an investigation. If a company's regular outside counsel were retained to conduct the investigation, the Justice Department might feel the results had less than full credibility because the law firm knew "who buttered its bread" and that the firm would not want to bring bad news to clients and endanger the ongoing business relationship. The authors end by concluding that employing specialized counsel comports with the expectations under the U.S. Sentencing Guidelines, gives a company the protections of the attorney-client privilege and the work-product doctrine, and "assures the government of the integrity of the internal investigation."

Part IV – The Investigation

A. Some Basic Steps

Many investigations can be in a crisis situation, where a company may have discovered something that it knows is bad but not how bad, or how widespread. Senn noted in the *FCPA Compliance and Ethics Report*, Episode 155, that the first thing to observe is that not every incident requires outside counsel. All kinds of issues can be handled efficiently by in-house counsel. Moreover, there will be other issues and corporate disciplines involved such as the Human Resources Department.

She explained that for a typical compliance blip that may happen, you do not need to call in an outside counsel right away. But if you do have indicia of larger problems, particularly if you are a public company, calling outside counsel is a good idea because you may have reporting obligations. She cautioned that even at this early stage, outside counsel does not have to be "boots on the ground" and may not be required to be intimately involved if the case is simple.

Further, bringing in outside counsel has several advantages. First, an independent review has more credibility. If you are working for the company in any capacity, the government simply will not believe as much that the investigation is independent. From the government's perspective (the SEC or Justice Department), it typically does not know the company involved in the investigation. Further, government regulators and enforcement officials are usually suspicious that a company is going to try to do what is right for the company. Of course there have been documented enforcement actions where companies have either destroyed documents or tried to hide things, such as witnesses or other evidence. In certain situations, an employee may look the other way, either purposefully or in ignorance of what he is seeing, and may take the investigation in the wrong direction. You want to avoid that kind of problem.

Second, complicated issues arise in cross-border situations. These include: privacy laws; labor laws; cultural and language issues. It can be very helpful, more cost effective, and important from a compliance perspective to have somebody who is experienced in those kinds of issues.

Finally is the issue of document preservation. Senn believes that "probably from the government's perspective, the most important aspect of setting up an investigation in a way that makes them feel comfortable is ensuring that

all data is locked down." Some questions that she believes counsel should ask: "Do you have hand-held devices? Where are all of your servers? What is your backup tape situation? Are you trained in forensically retaining information?" Her point is that wherever your company has data stored it needs to be secured, whether it is on individual cell phones, massive company servers, or with some third-party provider in the cloud.

Basically, you need to get into the technical nitty gritty. If you do not, you could end up having a situation where either information is compromised or there's a possibility or suspicion that information is lost. Unfortunately, that is the situation that leads to a prosecutor's imagination going wild. Senn ended her thoughts on this key point with the following: "The thing you want to do is just lock down that information, so if it ever comes to a point where the government says, 'Well, we want to kick the tires,' you can say, 'OK, don't worry. We've got everything you would have gotten otherwise'."

Stephen Martin, a partner at Baker & McKenzie, echoes this sentiment that when dealing with prosecutors—whether from the Justice Department, SEC, or state prosecutors—you and your company's credibility are paramount.

All of these steps can lead your company, through its investigation counsel, to gaining credibility with the DoJ and SEC. Senn made clear that the government will not only put you through your paces, but also test the vibrancy of your investigation protocol and steps you might take as an independent assessor. She said that "if they realize, or they think, that all you're doing is parroting what they consider to be the company line, and you haven't gone in and independently taken a look for yourself, you're just going to come off as less credible, as somebody that they can't really trust. That is definitely something that a company wants to avoid at all costs."

I really liked the way Senn phrased the next step: "You don't want to go too crazy" when scoping out the investigation. After getting the documents and technology locked down, try to figure out the bad actor(s). Depending on whether the investigation target is aware of his or her status, you may be forced into "somewhat of a stealth investigation, where instead of going full bore and sending out document holds and things like that, you want to essentially get that person's information and make sure that they're not going to do anything to their information. If there are a number of people you know are at issue, you want to lock that down, as well." This relates back to her remarks about securing all information, wherever it may be stored. But you should also remember instant messaging, text messaging, and other forms of communication such as smart phone apps like "What's App," which allow communication through smart phones but over the internet.

One of the questions that compliance practitioners often struggle with is when in the investigation process is it appropriate to discipline employees?

The next step is to collect the documents forensically and use the information gleaned from this step in the process to perform lay-of-the-land interviews, where you obtain enough information to have a basic understanding of the situation, who the key players are, and who may be involved in the incident. Senn also believes you can garner quite a bit of information from working with your client before the actual interviews begin. You can look at organizational charts and see the number of employees who could have touched the transaction(s) at issue, and also the countries involved. A review of the company's financial accounting systems is critical, so that you can assess how much will have to be done manually and in-country.

One of the questions that compliance practitioners often struggle with is when in the investigation process is it appropriate to discipline employees? This requires a case-by-case analysis. You should begin by taking any persons out of the responsible situation. Paid leave pending an investigation is one option. If you terminate them, they will be gone and you will have no control over them for initial interviews, follow-up interviews, or assistance. Additionally the government might want to interview that person. If you fired him or her, and that person has moved away or is now inaccessible to the government, it may well make the situation worse. Therefore, I advise keeping investigation subjects around; just prevent them from continuing to do any of the harm that they may have previously done.

B. A Few Words on Forensic Accounting

Your forensic accountant should be a part of your investigation team. With the right skills, such a member can bring an investigative mind that drives him or her to answer questions about what occurred, when and how it happened, and who was involved. Most lawyers, however, do not understand how forensic accounting is performed and how they can assist your compliance investigation going forward.

Forensic accountants collect and analyze accounting and internal controls evidence. They use this information to produce a fact-based report that can inform the decision-making process in investigations and dispute resolution. The by-products of a forensic accountant's work can include remediation strategies to help a company remedy procedural or internal controls gaps that allowed the underlying issue to occur. Inquiries into accounting and internal controls raise a host of technical issues that require specialized knowledge that forensic accountants can provide. This is a qualitative difference from internal audit, which more often looks at process to determine if it has been followed properly.

The objective of a forensic accounting assignment is to collect, analyze, and report on the facts surrounding a particular act that often has litigious, fraudulent, or criminal implications. Auditors also collect and analyze evidence, but an independent auditor's objective is to attest to the credibility of assertions that are under examination, such as the material accuracy of financial statements for which the audited company's management is responsible. Senn argues that a key role of the forensic accountant is to identify a concern and to notify company management about the issue or issues discovered.

As with a decision on tapping outside counsel to perform a compliance investigation, you will need to consider whether a forensic accountant should be retained as an outside consultant or hired as an employee. One critical reason to use an outside professional is so he or she will not be governed by management or influenced by potential biases within company. Lastly is the issue of privilege. If a forensic accountant is not assigned through your legal department or through outside counsel, you can forget even the chance of claiming privilege.

C. Ten Steps to Take in a Cross-Border Investigation

Senn and a colleague, Michelle Albert, published an article in the *FCPA Report*, titled "Internal Investigations, How to Conduct an Anti-Corruption Investigation: Developing and Implementing the Investigation Plan." This lays out 10 steps to consider for your investigation and provides some excellent pointers on some of the smaller, but critical, details in any cross-border investigation.

1. Offer Interview Translations

While most people know English to a certain extent and it is a common language nowadays, when you get into the detailed questions in an interview, employees may have enough English skills to make you assume they understand everything, when in fact they do not. You may ask a question, for example, about expense reports; maybe they understand conversational English, but there's no reason for them to know about technical topics such as expense reports. This makes it important to have someone present in the interview who speaks the witness's native language, and assume that sometimes you will need to call on that person. You should make it clear to the witness at the outset of the interview that you do not perceive a problem with their English and they understand the reason for the translator.

2. Avoid Cultural Pitfalls

Cultural pitfalls can be big deep holes that you know nothing about, but you can fall into pretty easily. One example is the issue of personal privacy, where most countries have a different concept of privacy, particularly about whether your work area is your own versus what really belongs to the company. In most states in the United States, employees fully understand that your employer can take anything from your office at any time, even if it is personal, because you've brought it to work. In many other countries this is not the case. Things at your desk generally are never touched or looked at by anybody else, and that's considered your sanctum where nobody else may enter. If you arrive and do a regular document sweep the way that you would proceed in the United States that could be perceived as horribly offensive to the employee. Senn cautioned you should seek local counsel's guidance to understand what needs to be done and also explain to you the best way to do it without offending people.

You do not want witnesses to begin the interview process with a negative view of you; you want them to be cooperative in the interview. This makes it in your best interest to follow local cultural norms. Otherwise, interviews can become embarrassing and awkward at times if you do fall into one of these cultural pitfalls.

3. Observe Data Privacy Restrictions

Most American lawyers are aware of different data privacy restrictions and requirements in countries governed by the European Union and the United States. Some of that is related to employee and employment law; whether or not they have ownership of certain information, and then other parts of the law that really do have to do with data privacy,

which means personal information that (no matter what form it is in) cannot be disseminated. But here the point under this best practice is that your analysis and response must go much further to satisfy the Justice Department if you want to claim that you cannot get certain information out of a country because of data privacy restrictions.

For instance, if you have personal data that you routinely send across national borders, yet when an investigation begins you claim that you cannot take it out of that same country (such as Germany), the Justice Department will take a dim view of that claim. Further, even if a data privacy law is on the books, yet the country does not enforce the law, that could work against any data privacy claim as well. So you will need to be prepared to present persuasive evidence on this issue if you try and make such a claim.

4. Comply With Labor Requirements

Similar to the long-standing Weingarten right of unionized employees in the United States to have a representative present for interviews, in many countries outside the United States there are works councils and similar analogs in other countries where, basically, the works council is responsible for the interactions between the employers and the employees. Moreover, employees have certain statutory or labor code-based rights as employees, regardless of whether they are members of a labor union. These rights can drill down into the types of questions that you can ask, or even prevent you from meeting with or interviewing certain employees.

> In some jurisdictions such as the Scandinavian countries, the regulators call politely and ask, "Can we make an appointment? We'd like you to come by."

This means you may well have to work through works councils to make sure that the way you ask the questions, and those present for the company, are acceptable. If you do not have this pre-approval, the works council may be able to prevent you from meeting with certain employees. For each area where you operate, you must engage the local legal counsel to determine what is the best way to work with the works council (or similar types of organizations) to ensure that you do what you must to complete your investigation.

5. Be Aware of Other Local Requirements

Points three and four certainly lead into best practice No. 5. It is incumbent that you work with local counsel in the country you are performing the interviews to gain an understanding of witness rights and your obligations during any investigation. This is because there are many ways a U.S. lawyer would approach an investigation that could be problematic in other jurisdictions. Some examples include taking pictures of, or physically removing documents from, a location; those practices might be restricted in other countries. You certainly need advice and counsel on what is legal and what might not be going forward.

6. Put Form in Native Translations

In the countries that have strict data privacy laws, sometimes the only way an investigation can collect an employee's personal information is to obtain affirmative assent. Such information might include work documents, work e-mails, or similar information. Senn cautioned that in this situation it is even more important to put the consent form in the native language. You do not want the employee later to claim that he did not understand the consent form or believed he was executing something different. It can be critical that you have informed consent because, if you don't, that consent could well turn out to be void.

7. Preserve the Attorney-Client Privilege

Attorney-client privilege is a communication between an attorney and a client for the purpose of seeking legal advice. This privilege exists to ensure that people are not afraid to go to their lawyer. The U.S. rule is relatively straightforward. It applies to both in-house and outside counsel.

The rules outside the United States can be quite different, and perhaps a little bewildering. In many European countries no privilege exists for an in-house counsel, so if a general counsel of a company speaks to the president or chief executive officer, there is no privilege under basically any circumstances in Europe. Moreover, other jurisdictions have different laws, each with a slightly different parameter, leading to different attorney-client expectations. Senn gave one such example: If your client company is headquartered in Germany and your in-house contact is the general counsel, you cannot use the GC as a point person to help you conduct the interview the way you might with in-house counsel in the United States, because German executives do not have attorney-client privilege.

8. Prepare for Local Enforcement Actions

Most American lawyers are aware that increasingly, other countries are growing more aggressive in their enforcement actions for bribery and corruption, sometimes based upon local and domestic anti-bribery laws. With current cooperation treaties (both formal and informal), you should anticipate that information regarding bribery and corruption will reach the ears of multiple governments. This increases the odds of local enforcement action against your client while you are investigating matters around an FCPA claim.

This is another area where your local counsel should be aware of the different ways local enforcement agencies handle matters. For instance, some countries such as China like to perform dawn raids. Law enforcement shows up, they roust suspects from their homes (and, yes, sometimes even from their beds) and arrest them. Or they raid the office and seize documents.

In some other countries, however, a dawn raid almost never happens. So again, local counsel can give you an idea of what the "typical" raid would look like. In some jurisdictions such as the Scandinavian countries, the regulators call politely and ask, "Can we make an appointment? We'd like you to come by." While this might not occur if the local government officials are concerned about potential destruction of evidence, different countries have different traditions of what they do, so you must ensure that your company is prepared for whatever may come to pass.

9. Prepare for Security Risks

This refers to personal security and health safety. Examples might be when you go into war-torn countries. Or consider the recent situation when Ebola erupted in Western Africa or Central Africa. If you are conducting an investigation in such ravaged areas, you should not send your employees to Liberia at that time to interview people. The same can be true in war-torn countries such as Syria. Further, one should always be aware of political instability or even the risk of political instability, which could arise at any time. Here you can think of Iraq and the fluidity of the situation involving Iraq, the Kurds, and ISIS.

The better plan would be to remove the people you are interviewing and bring them to you or to a local hub outside of the affected areas. That avoids a host of issues, such as the expense of hiring security guards to escort witnesses everywhere they go. You must make a judgment call as to where and whether these potential threats need to be addressed in some way.

10. Protect Whistleblowers

The U.S. government has made clear that it expects whistleblowers to be protected from retaliation. Further, the U.S. Sentencing Guidelines make clear that part of an effective compliance program includes a publicized system for employees or agents to report potential or actual criminal conduct without fear of retaliation. These guidelines apply to all U.S. companies, both domestic and international. If your company retaliates against foreign whistleblowers, the U.S. government can take that into account—which could be viewed in a negative way, meaning that you don't have an effective compliance and ethics program.

D. The Role of the Board of Directors

A separate issue for any significant FCPA investigation is the board of directors' involvement. Many boards do not have the same rigor when overseeing an investigation, which should be conducted or led by the board itself. The consequences of this lack of foresight can be problematic, because if a board mishandles an investigation, the consequences to the company, its reputation, and value, can all be quite severe. While many of the issues a board should consider are similar to those previously highlighted, their focus is a bit different from the CCO or compliance practitioner's perspective.

In an article in *The Corporate Board* magazine titled "Successful Board Investigations" by David Bayless and Tammy Albarrán, the authors recognize that the vast majority of investigations will be handled or directed by in-house counsel. If, however, a board gets more involved, the investigation must be handled with great care and skill. The authors note that, "While this task is fraught with peril, there are a number of steps a board can take to ensure the investigation accomplishes the board's goals, which will enable it to make informed decisions, and withstand scrutiny by third parties" because this third-party scrutiny—in the form of regulators, government officials, judges, arbitrators, or plaintiffs' counsel in shareholder actions—will come to bear on any investigation commissioned by a board of directors.

The authors state five key goals that any investigation led by a board of directors must meet. They are:

- **Thoroughness.** The authors believe that one of the key, and most critical, questions that any regulator might pose is just how thorough an investigation is; to test whether the regulator can rely on the facts discovered without having to repeat the investigation itself. Regulators tend to be skeptical of investigations where limits are placed (expressly or otherwise) on the investigators, either in what is investigated, or how the investigation is conducted. This question can kill a potential settlement immediately. Particularly if the regulator involved views a probe as insufficiently thorough, its credibility is undermined.

- **Objectivity.** Here the authors write that any investigation "must follow the facts wherever they lead, regardless of the consequences. This includes how the findings may impact senior management or other company employees. An investigation seen as lacking objectivity will be viewed by outsiders as inadequate or deficient." I would add that in addition to the objectivity requirement in the investigation, the same must be had with the investigators themselves. If a company uses its regular outside counsel, that may be viewed with some skepticism, particularly if the company is an important client of the law firm involved, either in dollar amounts or in number of matters handled by the firm.

> Many boards do not have the same rigor when overseeing an investigation, which should be conducted or led by the board itself.

- **Accuracy.** As in any part of a best practices anti-corruption compliance program, the three most important steps are to document, document, and document. This means that the factual findings of an investiga¬tion must be well-supported. If they aren't, the authors believe that the investigation is "open to collateral attack by skeptical prosecutors and regulators. If that happens, the time and money spent on the internal investigation will have been wasted because the government will end up conducting its own investigation of the same issues." This is never good, and your company may well lose what little credibility is left and squander any goodwill it may have generated by self-reporting or self-investigating.

- **Timeliness.** Certainly in the world of FCPA enforcement, an internal investigation should be done quickly. This has become even more necessary with the tight deadlines set under the Dodd-Frank Act whistleblower provisions. But a public company has other considerations, such as an impending SEC quarterly or annual report that may need to be deferred absent as a timely resolution of the matter. Lastly, the Justice Department or SEC may view delaying an investigation as simply a part of document spoliation. So timeliness is crucial.

- **Credibility.** One of the realities of any FCPA investigation is that a board-led investigation is reviewed sometimes years after the initial events and investigation. So not only is there opportunity for Monday-morning quarterbacking, but quite a bit of post-event analysis. So the authors believe that any board-led investigation "must be (and must be perceived as) credible as to what was done, how it was done, and who did it. Otherwise, the board's work will have been for naught."

To help manage these five issues the authors have seven tangible considerations they suggest that a board of directors follows to help make an investigation successful. These seven considerations are listed as follows.

1. Consider whether you need independent outside counsel.

The authors consider that the appearance of partiality "undermines the objectivity and credibility of an investigation." That means you should not use your regular counsel. The authors cite the SEC analysis of how independent board members explain the need for independent counsel. They state that the SEC "considers the following criteria when determining whether (and how much) to credit self-policing, self-reporting, remediation, and cooperation," which will consist of the following factors:

- Did management, the board, or committees consisting solely of outside directors oversee the review?
- Did company employees or outside practitioners perform the review?
- If outside persons, have they done other work for the company?
- If the review was conducted by outside counsel, had management previously engaged such counsel?

- How long ago was the firm's last representation of the company?
- How often has the law firm represented the company?
- How much in legal fees has the company paid the firm?

2. Consider hiring an experienced "investigator" to lead the internal investigation.

If a board is leading an investigation, I would argue that by definition the matter must be serious. The authors say that your investigation should be led by a lawyer with significant experience in conducting internal investigations; a strong background in criminal or SEC enforcement; and substantive experience in the particular area of law at issue. The traits are needed so that your designated counsel will think like an investigator, not like an in-house lawyer or civil litigator.

3. Consider the need to retain outside experts.

In any FCPA or other anti-corruption investigation, you will need a variety of subject matter experts (SMEs) instead of a compliance professional. The authors correctly recognize that "if there are accounting issues, forensic accountants might be needed. For instance in the Johnson and Johnson DPA, the Justice Department specified each internal company audit team include "qualified auditors who have received FCPA and anti-corruption training." In this day and age, an electronic discovery consultant is often required and can be a cost-effective option for gathering and processing electronic data for review." These types of investigations will most probably be cross-border as well, and this will require other varieties of expertise. Martin and Trevino say, "The lowest bid may not necessar¬ily be the best for a particular investigation. While cost is important, understand the limitations of each consultant and, with input from your investigator, determine which consultant best meets your goals."

> Your board might also avoid the fate that befell several well-known companies that are now in the middle of public multimillion-dollar FCPA investigations.

4. Analyze potential conflicts of interest at the start and during the investigation.

The authors see two types of conflicts of interest that may emerge during an investigation. First is the situation where the law firm conducting the investigation is the same firm that provided counsel earlier that might have led to the problem in the first place. During an internal investigation, the lawyers may be hired by, and represent, the board or its committee. The second situation occurs when a lawyer or law firm jointly represents the board and its employees; regulators have become increasingly concerned with joint representations. Moreover, "The trickier question is what to do when there simply is a risk that representing one client could limit the lawyers' duties to the other." So in these situations, joint representation may not be appropriate.

5. Carefully evaluate whistleblower allegations.

With the advent of the Sarbanes-Oxley and Dodd-Frank Acts and retaliation policies, taking the allegations of whistleblowers seriously is paramount. This does not mean trying to find out who the whistleblowers might be to punish or stifle them, even if they are located outside the United States and therefore do not have protections under these laws. They can still get hefty bounties. The authors recognize that companies can come to grief when "companies run into problems when whistleblower allegations are discounted, if not outright dismissed, especially if the whistleblower has a history of causing trouble or is perceived as incompetent. When this type of whistleblower makes a claim, it is easy to presume ulterior motives." While such motives might exist, it does not matter in the investigation, as regulators "are very wary of boards that do not satisfactorily evaluate a whistleblower's complaint based on a perception of the whistleblower himself, as opposed to the substance of the complaint."

6. Request regular updates from outside counsel, without limiting the investigation.

These types of investigations are long and expensive. They can easily spin out of cost control. But by trying to manage these costs, a board might be perceived as placing improper limits on the investigation. According to Bayless and Albarrán, the "goal is to strike the right balance between the cost of the investigation and its thoroughness and credibility." To do so, the authors advise that flexibility is an important ingredient. A board can begin the project with an

agreed initial scope of work and then "revisit the scope of work as the investigation progresses. If conduct is discovered that legitimately calls for expanding the scope of the investigation, then the board can revisit the issue at that point. Put another way, the scope of what to investigate is not a static, one-time decision. It can, and usually does, evolve." By seeking regular updates and questioning counsel on what they are doing and why, directors can manage costs, while at the same time ensure that the investigation is sufficiently thorough and credible.

7. Consider whether an oral report at the conclusion of the investigation is sufficient.

While there may be instances where, due to complexity and the nature of allegations involved, a written report is necessary, the authors believe from their white-collar defense experience at Covington & Burling that sometimes an oral report delivered to a board is better than a written report. A written summary "may be easier to follow and appear to be the logical conclusion to an investigation, [but] it is an expensive and time-consuming endeavor, and it comes with great risk." The authors indicate three reasons for this position.

First, it is much easier to waive attorney-client privilege by mistake if a written report falls into the wrong hands.

Second, once those findings and conclusions are written, they may become "set in stone. If later information comes to light that impacts the report's conclusions, altering the conclusions may undermine the credibility of the entire investigation. So, retaining flexibility to change the findings if further information is later learned is a real advantage of an oral report."

Third and finally, "it takes time to prepare a well-written and thorough report. When an internal investigation must be conducted quickly, spending time to prepare a written report may not be an efficient use of time." For all of these reasons, and perhaps others, an oral report presented to the board and documented in the board of director meeting minutes may be sufficient.

The authors conclude their piece stating, "By keeping in mind the issues addressed above, the board will be better prepared for the investigation and readily able to exercise good judgment throughout the review. A well-conducted investigation by the board may spare the company further disruption and costs associated with follow-up investigations by the regulators, or at the very least minimize the company's exposure."

I would only add that by following some of the prescriptions set out by Bayless and Albarrán, your board might also avoid the fate that befell several well-known companies that are now in the middle of public multimillion-dollar FCPA investigations. Just as companies need to be prepared for such matter, boards need to be prepared as well.

Part V – Whistleblower Issues

As noted by both Senn and the issues listed for board consideration, the subject of whistleblowers has grown more important since the passage of the Dodd-Frank Act in 2010—and indeed based upon events, SEC speeches, and enforcement actions in 2015. Therefore, considerations around whistleblowers, how you treat them, and their protection are matters you must consider in your investigation.

A. The Protection of Whistleblowers

The Dodd-Frank whistleblower provisions not only allowed payment of a bounty for information that leads to an SEC enforcement action; they also protect employees from retaliation. Sean McKessy, chief of the SEC's Office of the Whistleblower, said in a statement: "For whistleblowers to come forward, they must feel assured that they're protected from retaliation and the law is on their side should it occur. We will continue to exercise our anti-retaliation authority in these and other types of situations where a whistleblower is wrongfully targeted for doing the right thing and reporting a possible securities law violation."

The difficulties faced by whistleblowers on Wall Street have been well documented. In an article in the *Financial Times*, titled "Wall Street Whistleblowers," William Cohen wrote about three such persons. One was Oliver Budde, a former legal adviser for Lehman Brothers, who was quoted as saying, "When the tone at the top is, 'Anything goes,' anything will go." Eric Ben-Artzi, a former analyst at Deutsche Bank, was quoted as saying, "They accused me of trying to bring down the bank." Peter Sivere, a former compliance officer at JPMorgan Chase, was quoted as saying, "I

wish I had known that the house always wins." All three men had tried to blow the whistle internally. They were not only rebuffed; they suffered retaliation.

Cohen also quoted Jordan Thomas, a former SEC enforcement official now in private practice at the firm of Labaton Sucharow, where he heads the firm's whistleblower practice. Thomas believes that the anonymous reporting provisions of the Dodd-Frank Act will help protect whistleblowers. He said, "Essentially most whistleblower horror stories start with retaliation. And to be retaliated against, you have to be known. The genius of Dodd-Frank was it created a way for people with knowledge to report without disclosing their identity to their employers or the general public. That has been a game changer because now people with knowledge are coming forward with a lot to lose, but they have a mechanism where they can report this misconduct without fear of retaliation or blacklisting." Thomas also said that the SEC's awarding of $14 million to a whistleblower "whose identity has remained unknown, despite efforts by the media to uncover it, sends a powerful message that whistleblower identities will be protected."

> "Whistleblowers can be victims of retaliation even if they are ultimately proved wrong, as long as they have a 'reasonable' belief that the company was doing something wrong."
>
> Jordan Thomas, Partner, Labaton Sucharow

In April 2015, the SEC announced a "maximum whistleblower award payment of 30 percent of amounts collected in connection with *In the Matter of Paradigm Capital Management, Inc. and Candace King Weir.*" The whistleblower award of $600,000 was paid for the firm's retaliation against the whistleblower after "key original information that led to the successful SEC enforcement action. The whistleblower in this matter suffered unique hardships, including retaliation, as a result of reporting to the Commission." While this was not the first SEC whistleblower award, it was the first where a portion of the award was credited for retaliation against the whistleblower.

This award to a whistleblower caps a stunning run for whistleblowers who have brought information forward under the Dodd-Frank whistleblowing provisions. First was the KBR pre-taliation fine and the cease-and-desist order. In this matter, KBR was fined for having language in its internal employee confidentiality agreement (CA) that required employees to go to the company's legal department before releasing certain confidential information to outside parties such as the SEC.

The SEC held that such restrictions violated the whistleblower protection Rule 21F-17 enacted under the Dodd-Frank Act. "KBR required witnesses in certain internal investigations interviews to sign confidentiality statements with language warning that they could face discipline and even be fired if they discussed the matters with outside parties without the prior approval of KBR's legal department. Since these investigations included allegations of possible securities law violations, the SEC found that these terms violated Rule 21F-17, which prohibits companies from taking any action to impede whistleblowers from reporting possible securities violations to the SEC." This was despite zero evidence that KBR had actually used such language or restrictions to prevent any employees from whistleblowing to the SEC.

In another part of the SEC press release regarding the KBR case, Ceresney said, "By requiring its employees and former employees to sign confidentiality agreements imposing pre-notification requirements before contacting the SEC, KBR potentially discouraged employees from reporting securities violations to us. SEC rules prohibit employers from taking measures through confidentiality, employment, severance, or other types of agreements that may silence potential whistleblowers before they can reach out to the SEC. We will vigorously enforce this provision."

Then there is the case of former Halliburton employee Tony Menendez, who was profiled by Jessie Eisinger in the article "The Whistleblower's Tale: How an Accountant Took on Halliburton." The report highlights a whistleblower who took his concerns to government regulators and was then outed by the company as the SEC whistleblower and retaliated against.

Interestingly, the SEC took no action on the whistleblower claims. The company then argued on appeal that "since the SEC hadn't brought any enforcement action, his complaint about the accounting was unfounded." Now there is an appellate court holding that if whistleblowing was a "contributing factor" only to the retaliation, a company can be found guilty of retaliation as well. Further, the employee is not required to prove motive. Well-known whistleblower expert Jordan Thomas also explained in the Eisinger article, "Whistleblowers can be victims of retaliation even if they are ultimately proved wrong, as long as they have a 'reasonable' belief that the company was doing something wrong."

B. Compliance Professionals and Lawyers as Whistleblowers

In April 2015 the SEC paid a whistleblower reward of around $1.5 million (the exact amount wasn't disclosed) to a compliance officer. The name of the whistleblower was not released. In a press release the SEC said, "The award involves a compliance officer who had a reasonable basis to believe that disclosure to the SEC was necessary to prevent imminent misconduct from causing substantial financial harm to the company or investors."

Andrew Ceresney, director of the SEC's Division of Enforcement, was quoted in the press release as saying, "When investors or the market could suffer substantial financial harm, our rules permit compliance officers to receive an award for reporting misconduct to the SEC. This compliance officer reported misconduct after responsible management at the entity became aware of potentially impending harm to investors and failed to take steps to prevent it."

This award makes clear that the SEC will treat compliance professionals as all other whistleblowers when making an award based upon the fine or penalty. In a December 2014 article, titled "When Should Internal Auditors and Compliance Officers Become SEC Whistleblowers," Daniel Hurson wrote, "Prior to this award, it had generally been thought the SEC would continue to discourage such awards on the rationale that it would not want to encourage employees whose job it was to prevent corporate legal and ethical violations to profit from simply doing their jobs."

Hurson wrote that this initial whistleblower payment to a compliance practitioner marked a change in SEC policy because, "It has generally been understood that compliance officers and internal auditors are not permitted to receive whistleblower awards because information they reported to a superior constituting allegations of misconduct was not to be considered 'original information' under the Dodd-Frank Act and SEC rules."

There was nothing in the SEC's statement or any of the commentary on the whistleblower award to indicate that the compliance professional involved was a lawyer. An equally delicate issue, however, is whether a lawyer can be a whistleblower. In an article in the *Westlaw Journal Securities Litigation & Regulation* entitled, "Is the SEC encouraging unethical whistleblowing by counsel?" Nick Morgan and Haley Greenberg from the law firm of DLA Piper explored this issue. Lawyers are also governed by their state bar associations on their ethical obligations, which include confidentiality and loyalty to a client. Morgan noted, "The Dodd-Frank bounty provisions further exacerbated the conflict between federal securities whistleblower law and state attorney ethics requirements by giving attorneys financial incentives to breach attorney-client confidentiality."


Morgan

Three state bar organizations (Washington, California, and New York) have questioned whether SEC regulations trump state bar ethical obligations regarding attorney whistleblowers. Indeed in New York, the authors noted "the New York County Lawyers' Association committee on professional ethics responded to the development by releasing a formal opinion. It concluded that New York lawyers, presumptively, may not ethically serve as whistleblowers for a bounty against their clients under Dodd-Frank, because doing so generally gives rise to a conflict between lawyers' interests and those of their clients."

What happens when federal law conflicts with state regulations regarding a lawyer's ethical obligations? Morgan reported, "No court has yet found that SEC regulations pre-empt state ethics rules governing lawyers' communications with their clients. In cases in which conflicts of state and SEC law have appeared, federal courts have been receptive to arguments based on lawyers' ethical obligations under state law and have balanced the state and federal interests. While the Dodd-Frank bounty provisions increase the incentives for attorneys to act as whistleblowers at their clients' expense, it is unclear whether those incentives outweigh the risks and burdens associated with taking such actions. Aside from the ethical issues, whistleblowers more often than not go uncompensated and incur significant burdens for their trouble, decreasing whatever temptation some attorneys may feel."

Part VI – After the Investigation

A. The Decision to Self-Disclose

Quantifying the benefits of disclosing a potential FCPA violation to the federal government has always been difficult. At least for the Justice Department, its basic analysis for calculating penalties comes from the U.S. Sentencing Guidelines. As stated in the FCPA Guidance, "To determine the appropriate penalty, the 'offense level' is first calculated by examining both the severity of the crime and facts specific to the crime, with appropriate reductions for cooperation and acceptance of responsibility, and, for business entities, addi-tional factors such as voluntary disclosure, cooperation, pre-existing compliance programs, and remediation."

The Sentencing Guidelines, §8C2.5(g) state that an overall fine can be reduced through the following:

(g) Self-Reporting, Cooperation, and Acceptance of Responsibility

If more than one applies, use the greatest:

(1) If the organization (A) prior to an imminent threat of disclosure or government investigation; and (B) within a reasonably prompt time after becoming aware of the offense, reported the offense to appropriate governmental authorities, fully cooperated in the investigation, and clearly demonstrated recognition and affirmative acceptance of responsibility for its criminal conduct, subtract 5 points; or

(2) If the organization fully cooperated in the investigation and clearly demonstrated recognition and affirmative acceptance of responsibility for its criminal conduct, subtract 2 points; or

(3) If the organization clearly demonstrated recognition and affirmative acceptance of responsibility for its criminal conduct, subtract 1 point.

Both the Justice Department and SEC consistently state in speeches and other public commentary the benefits of self-disclosure. In every speech or presentation that they make, they always extol the benefits of self-disclosure. The SEC's Ceresney offered some remarks at CBI's Pharmaceutical Compliance Congress on the issue of self-disclosure. Ceresney's remarks underscore why, from the regulators' perspective, it is in a company's interest to do so. It emphasizes the self-monitoring that allows companies to better prevent, detect, and then remediate such violations. Of course it does assist the SEC in combating securities violations as well. This is why I believe regulators will continue to find ways for not only facilitation of whistleblowing but to also encourage cooperation by companies in all phases throughout the investigation and enforcement process. He ended this section of his remarks with a warning that I believe succinctly provided the SEC's position on self-reporting: "Companies that choose not to self-report are thus taking a huge gamble because if we learn of the misconduct through other means, including through a whistleblower, the result will be far worse."

1. Benefits of Voluntary Disclosure

a. Monetary Benefits

I believe that there are clear, substantive, and discrete benefits to voluntary disclosure, which a company can receive from the Justice Department and SEC. If there was any doubt to the financial benefits to this decision, they were answered in the Johnson and Johnson deferred-prosecution agreement. Listed under the section "Relevant Considerations" was this reason why the Justice Department favored a DPA:

a. J&J voluntarily and timely disclosed the majority of the misconduct described in the [Criminal] Information and Statement of Facts;

So self-disclosure was one of the reasons that the Justice Department entered into the DPA. Perhaps more importantly, however: The self-disclosure brought to J&J a monetary benefit with a tangible reduction in its overall fine and penalty. The DPA reported a reduction by 5 points of the company's overall Culpability Score with the following:

(g)(1) The organization, prior to an imminent threat of disclosure or government investigation, within a reasonably prompt time after becoming aware of the offense, reported the offense, fully cooperated, and clearly demonstrated recognition and affirmative acceptance of responsibility for its criminal conduct; -5

It is not possible to determine from the DPA how much of the reduction was due to the self-disclosure and how much was due to the improved conduct thereafter. The precise language, however, makes clear that the Justice Department places a real value on such self-disclosures. Companies should take this as a clear sign that, at the end of the day, it will be better to self-disclose.

b. Credibility Benefits: Creation of Leverage

One of the points that noted white-collar defense lawyer and FCPA commentator Mike Volkov often makes is, "Clients lost all leverage when they enter the voluntary disclosure process." I believe that there are significant leverage benefits gained by self-disclosure. Stephen Martin, a former federal prosecutor and now partner at Baker and MacKenzie, says the most important thing that a company can bring to the table when negotiating with the government is credibility. *Credibility benefits can start with self-disclosure.* If a company self-discloses and then cooperates with the government during the investigation, that can lead to a monetary reduction in the overall fine and penalty. But more than monetary benefits, self-disclosure creates the "leverage" that the company wants to do the right thing, even if an FCPA violation has occurred within the company.


Martin

Mary Shaddock Jones, former assistant general counsel and director of compliance for Global Industries, has spoken about her experiences with a multiyear FCPA process that had its genesis from the Panalpina case. While many companies caught up in the Panalpina matter were assessed fines and penalties, after a thorough internal investigation, neither the SEC nor the Justice Department chose to take action against Global Industries. Jones speaks about going through negotiations with the Justice Department, how she personally made presentations about the robust nature of the GI compliance program, and how she and the company's general counsel led a worldwide investigation team to determine if whether any additional problems existed after the Panalpina matter came to light. Jones emphasizes the complete cooperation by GI and "leveraging" the vigorous nature of its compliance program to the SEC and DoJ.

The best example of this leveraging I can bring forward is the result achieved by RAE Systems Inc. last year. RAE received a non-prosecution agreement after having actual knowledge of FCPA violations in two majority-owned joint ventures in China. Even though RAE failed to engage in due diligence on one joint venture acquisition, failed to take effective remedial measures with a second joint venture after it became a corporate subsidiary, and had *actual knowledge* of FCPA violations, RAE did not receive a criminal charge against it.

Why? In its letter agreeing to the NPA, the Justice Department noted: *"non-prosecution agreement based, in part, on the following factors: (a) RAE Systems' timely, voluntary, and complete disclosure of the facts described in Appendix A; (b) RAE Systems' thorough, real-time cooperation with the Department and the U.S. Securities and Exchange Commission ("SEC"); (c) the extensive remedial efforts already undertaken and to be undertaken by RAE Systems; and (d) RAE Systems' commitment to submit periodic monitoring reports to the Department."*

I believe that this is "leveraging" that a company can bring to negotiations when it self-discloses an FCPA violation; the RAE matter would appear to provide specific evidence of the benefits of such corporate conduct. The NPA reports that RAE had actual knowledge of FCPA violations, yet no criminal charges were filed. Further, no ongoing external corporate monitor was required. Clearly RAE engaged in actions during the pendency of the investigation that persuaded the Justice Department not to bring criminal charges.

2. Arguments Against Self-Disclosure

Some commentators, notably Mike Volkov, have cautioned that any decision to self-disclose should be well considered, and if the issue can be resolved through an internal investigation, subsequent remediation, and ongoing monitoring to make sure it does not happen again, self-disclosure many not be warranted.

Arnold & Porter's Senn takes this idea a step further. Senn says that self-reporting should be "the exception and not the rule." She first pointed to the "structure of self-reporting. The thing that I think gets lost in the shuffle is there's absolutely no legal obligation to self-disclose in FCPA cases, at all. There may be other disclosure obligations, because of a public company or what have you, but under the law of the FCPA, and under criminal law, no company has an affirmative duty to self-disclose."

Senn explained that unlike in antitrust or cartel cases, where the first company to self-report gets immunity, "it's a totally different structure in the FCPA area for many reasons (most of which are appropriate), but you don't get immunity, you get cooperation credit." This cooperation credit is based on the U.S. Sentencing Guidelines cited above, but Senn said, "The problem is, a lot of these calculations are very, very opaque. Under the Sentencing Guidelines, you

get a 5-point decrease if you self-report, cooperate, and accept responsibility. You get 2 points off if you cooperate and accept responsibility, and then just 1 point for accepting responsibility. Under this system, supposedly, self-disclosure standing alone is worth 3 points, and each of the other ones are worth 1."

This leads her to believe that "in my experience, you get almost as much credit, if not as much credit, for cooperating with the government once they come to you, even if you didn't disclose in the first place. The myth is that self-disclosure is some kind of really big bump in cooperation credit. I think, in practice, that really doesn't bear water." She added, "This idea of credibility by self-disclosing is so intangible, and it's not quantifiable."

> "The problem is, a lot of these calculations are very, very opaque. Under the Sentencing Guidelines, you get a 5-point decrease if you self-report, cooperate, and accept responsibility."
>
> Mara Senn, Partner, Arnold & Porter

Senn even described a visual way to of the point, by describing an *X* and *Y* axis that creates four squares: "On one axis, you have the seriousness of the potential violation, and then the likelihood of discovery on the other axis. In both of these areas, both the seriousness and the likelihood of discovery, I draw the line to be more rational, but it may be different, than the traditional norm."

What about the numerous ways an FCPA violation or issue can be reported now (whistleblower hotlines, bounty rewards, other parties naming your company, and so forth); should that play a role in the calculus to self-disclose? Senn said, "I think that the likelihood of the discovery issue is really, really important if you think that companies get a lot of credit for self-reporting. If you don't think that, which I don't think that they do particularly, then really the focus is on cooperation and not so much on the self-reporting itself."

Even with the widespread knowledge of Dodd-Frank whistleblower awards and protections, Senn believes that "most employees really don't realize they can get money from the government if they are whistleblowers on these sorts of things. I don't think it's been particularly well publicized, and obviously employers are not training their employees to explain to them that they can be whistleblowers."

She even pointed to the recent statistics from the SEC report on whistleblowers, stating, "If you look at the latest SEC whistleblower report, only 4.3 percent of the tips reported were FCPA cases. It's not like people are hitting down their door with all these FCPA cases."

I found Senn's thoughts on the issue of self-disclosure certainly an interesting way to consider this most complex and significant issue. For all the criticism of "FCPA Inc." and the FCPA Paparazzi, it also demonstrates the importance of having counsel well versed in both the legal issues of the FCPA and representing a company before the government in the event that your business is under investigation.

B. Cooperation and Remediation

Extensive cooperation is now expected as a minimum in any self-disclosed FCPA investigation. Yet companies continue to be applauded for their efforts and rewarded with reduced fines and penalties as well. Two significant FCPA enforcement actions where this was made clear were the Parker Drilling deferred-prosecution agreement and the Ralph Lauren non-prosecution agreement.

Both companies provided extensive cooperation to the DoJ and SEC throughout the pendency of their respective investigations. In the Ralph Lauren NPA, the Justice Department detailed the company's conduct, allowing that Ralph Lauren had demonstrated an "extensive, thorough, and real-time cooperation with the department, including conducting an internal investigation, voluntarily making employees available for interviews, making voluntary document disclosures, conducting a worldwide risk assessment, and making multiple presentations to the department on the status and findings of the internal investigation and the risk assessment." In the Parker Drilling DPA, the DoJ acknowledged "the company's cooperation, including conducting an extensive internal investigation and collecting, analyzing, and organizing voluminous evidence and information for the department."

In addition to extensive cooperation, a company should also aggressively remediate any deficiencies that led to the violation(s). The Ralph Lauren NPA acknowledged "the company's early and extensive remedial efforts already undertaken—including conducting extensive FCPA training for employees worldwide, enhancing the company's existing FCPA policy, implementing an enhanced gift policy as well as other enhanced compliance, control and anti-corruption

policies and procedures, enhancing its due diligence protocol for third-party agents, terminating culpable employees and a third-party agent, instituting a whistleblower hotline, and hiring a designated corporate compliance attorney—and to be undertaken, including enhancements to its compliance program as described in Attachment B (Corporate Compliance Program)."

Parker Drilling also engaged in extensive work to create a gold standard compliance program all the while undergoing its own internal investigation. According to the DPA, "the company has engaged in extensive remediation, including ending its business relationships with officers, employees, or agents primarily responsible for the corrupt payments, enhancing its due diligence protocol for third-party agents and consultants, increasing training and testing requirements, and instituting heightened review of proposals and other transactional documents for all the company's contracts."

Parker Drilling also hired a full-time chief compliance officer and counsel who reports to the chief executive officer and audit committee, "as well as staff to assist the chief compliance officer and counsel." Lastly, and I hope that you remember this from the Morgan Stanley declination, Parker Drilling implemented "a compliance-awareness improvement initiative and program that includes issuance of periodic anti-bribery compliance alerts."

Senn has made clear that whether you decide to self-disclose or not, your company must fully remediate the issue it has. She suggested that a company should act as if it will draw government scrutiny: "The best way to go about it is to assume—act as if—the government is breathing down your necks on this very issue and fully remediate. The nice thing is they can decide what that means, 'fully remediate'."

Does this require a systemic look at the company's operations on a global basis, particularly in view of Assistant Attorney General Leslie Caldwell's recent admonition not to "boil the ocean" in the context of your FCPA internal investigation? Senn replied, "It used to be that in the government's view, fully remediating meant go to 10 different countries, even if there's no suspicion of any activity going on, just to make sure that everything's OK. They're now backing away from that and, in fact, they're saying that the private sector is the one that started that whole trend, which is not quite consistent with history."

Recognizing that there is always a risk that the government will come knocking, either via a whistleblower or other mechanism, Senn related, the need to have as robust a program as possible, one you detected and then remediated aggressively. The recent SEC enforcement action involving Mead Johnson would seem to bear this advice out, as the company had an internal investigation in 2011 over conduct that violated the FCPA and did not self-disclose this violation, while ending the conduct; yet, the company was not penalized by the SEC in its final enforcement action.

> In addition to extensive cooperation, a company should also aggressively remediate any deficiencies that led to the violation(s).

Senn went on to explain, "What you want to do is show to the government, 'We understand the problems that caused this, and we got to the root of them. Either it's a bad apple, and we got rid of that bad apple, or it was really a failure of compliance structures, and we've fixed that part of the compliance structures. In fact, we've added more, just to double check and make sure that in this particular area or similar areas, depending on what it is, we will detect, prevent, and if we detect something, we will remediate.' The government, can feel comfortable that you did what they would have asked you to do anyways. That doesn't always have to be onerous, sometimes it is depending on the scope of the issue, but that's what I would say about that."

Senn listed several actions that a company could engage in to demonstrate that it had taken solid remediation steps. Obviously, a company can "bulk up its compliance program." She added that it is important that a company demonstrate action taken against the nefarious party or parties. Certainly a company can fire people. But do not forget lesser forms of discipline, including docking pay or suspension without pay or other steps short of termination. I would add that you should consider the FCPA Guidance on this final point where it notes, "A compliance program should apply from the boardroom to the supply room—no one should be beyond its reach. The Justice Department and SEC will thus consider whether, when enforcing a compliance program, a company has appropriate and clear disciplinary procedures, whether those procedures are applied reliably and promptly, and whether they are commensurate with the violation."

The recent SEC enforcement action involving Goodyear was another example of the extent to which remediation can reduce your fine and penalty going forward. The SEC went out of its way to list all of the steps the company took in the cease-and-desist order that ended the matter. When the company received the initial reports about the bribes, "Goodyear promptly halted the improper payments and reported the matter to Commission staff."

Moreover, the company also cooperated extensively with the SEC. As noted in the order, "Goodyear also provided significant cooperation with the Commission's investigation. This included voluntarily producing documents and reports and other information from the company's internal investigation, and promptly responding to Commission staff's requests for information and documents. These efforts assisted the Commission in efficiently collecting evidence, including information that may not have been otherwise available to the staff."

On the point of internal remediation, regarding an entity in Kenya where Goodyear was a minority owner in a local business, the company got rid of its corrupt partners by divesting its interest and ceasing all business dealings with the company. Goodyear is also divesting its Angolan subsidiary. The order noted that Goodyear had lost its largest customer in Angola when it halted its illegal payment scheme. The company also took decisive disciplinary action against the company employees, "including executives of its Europe, Middle East, and Africa region who had oversight responsibility, for failing to ensure adequate FCPA compliance training and controls were in place at the company's subsidiaries in sub-Saharan Africa."

On the point of internal remediation, regarding an entity in Kenya where Goodyear was a minority owner in a local business, the company got rid of its corrupt partners by divesting its interest and ceasing all business dealings with the company.

Finally, in a long paragraph, the SEC detailed some of the more specific steps Goodyear took in remediation. These steps included:

- Improvements to the company's compliance function not only in sub-Saharan Africa but also worldwide;
- In Africa, both online and in person training was beefed up for "subsidiary management, sales, and finance personnel;"
- Regular audits were instituted by the company's internal audit function, which "specifically focused on corruption risks;"
- Quarterly self-assessment questionnaires were required of each subsidiary regarding business with government-affiliated customers;
- For each subsidiary, management certifications were required on a quarterly basis regarding controls over financial reporting; and annual testing of internal controls;
- Goodyear put in a "new regional management structure, and added new compliance, accounting, and audit positions;"
- The company made technological improvements to allow it to "electronically link subsidiaries in sub-Saharan Africa to its global network."

These changes were not limited to improvement of Goodyear's compliance function in Africa only. At the corporate headquarters, Goodyear created the new position of "vice president of compliance and ethics, which further elevated the compliance function within the company." This was the first time Goodyear had a C-Suite-level position for compliance and helped to demonstrate the company's commitment going forward to give compliance not only heightened visibility but a seat at the senior management table. The company also committed to expanding online and in-person training at the corporate headquarters and other company subsidiaries. Finally, the company instituted a new "Integrity Hotline Web Portal, which enhanced users' ability to file anonymous online reports to its hotline system. With that system, Goodyear is also implementing a new case management system for legal, compliance and internal audit to document and track complaints, investigations, and remediation."

The specific listing of the compliance initiatives or enhancements that Goodyear pushed after its illegal conduct came to light is certainly a welcomed addition to SEC advice about what it might consider some of the *best practices* a company may engage in around its compliance function. Moreover, this detail provides the compliance practitioner with strategies that he or she might use to measure a company's compliance program going forward. The continued message of cooperation and remediation as a way to lessen your overall fine and penalty continues to resonate from the

SEC. The previously mentioned Mead Johnson enforcement action was another recent SEC enforcement action where the company received credit for its cooperation and remediation.

C. Factors for an NPA for an Individual in an SEC Enforcement Action

In 2010 the SEC released its Enforcement Cooperation Initiative, which established a series of incentives for individuals and companies to assist the SEC in ongoing investigations and during the pendency of enforcement actions. As a part of this Initiative, the SEC released a Cooperation Policy Statement that described four factors the agency would consider to "determine whether, how much, and in what manner to credit cooperation." The four factors were:

a. How much assistance the individual provides, which includes offering voluntary cooperation to the SEC at the outset of the investigation without conditions and having good knowledge of the underlying facts and circumstances.

b. The importance of the underlying matter. This could mean it is the first enforcement action in an area, industry, or discipline but it could also point to the severity of the violation and monetary penalties or recoupment for victims of the crime.

c. The SEC's interest in holding the individual accountable, which is always paramount. However if a cooperator's actions maximize the SEC's law enforcement interests by facilitating the quick and successful resolution of its enforcement action or stop an immediate harm, it will be given additional credence.

d. The prior background of the cooperating individual. It is important that the cooperator is not "an associated person of a regulated entity, a fiduciary for other individuals or entities regarding financial matters, or an officer or director of any company." Moreover the cooperator's internal employment records will also be considered, particularly if the individual does not have any black marks in the way of prior disciplinary actions on his record.

Part VII – Some Evidentiary Considerations

A. Miranda and the FCPA: Do You Have the Right to Remain Silent?

Is concealing information from company lawyers conducting an internal FCPA investigation a federal crime? The *FCPA Blog* raised this question in the context of a company's internal investigation regarding an alleged violation of the FCPA. Even if the company attorneys handling the investigation provided the now standard corporate attorney *Upjohn* warnings, how does a company attorney asking questions morph into a *de facto* federal agent during an internal company investigation regarding alleged FCPA violations—and is the attorney thereby required to provide a *Miranda* warning to employees during an FCPA investigation?


Margolis

In a paper titled "Navigating Potential Pitfalls in Conducting Internal Investigations: Upjohn Warnings, 'Corporate Miranda,' and Beyond," Craig Margolis and Lindsey Vaala, of the law firm Vinson & Elkins, explored the pitfalls faced by counsel (both in-house and outside investigative) and corporations when an employee admits to wrongdoing during an internal investigation, where such conduct is reported to the U.S. government and the employee is thereafter prosecuted criminally under a law such as the FCPA. Margolis and Vaala also reviewed the case law regarding the *Upjohn* warnings, which should be given to employees during an internal FCPA investigation.

Employees who are subject to being interviewed or otherwise required to cooperate in an internal investigation may find themselves on the sharp horns of a dilemma. They may face either (1) cooperating with the internal investigation; or (2) losing their jobs for failure to cooperate by providing documents, testimony, or other evidence. Many U.S. businesses mandate full employee cooperation with internal investigations or those handled by outside counsel on behalf of the company. These requirements can exert a coercive force, "often inducing employees to act contrary to their personal legal interests in favor of candidly disclosing wrongdoing to corporate counsel." Moreover, such a corporate policy

may permit a company to claim to the U.S. government a spirit of cooperation in the hopes of avoiding prosecution in "addition to increasing the chances of learning meaningful information."


Vaala

Where the U.S. government compels such testimony, through the mechanism of inducing a corporation to coerce its employees into cooperating with an internal investigation, by threatening job loss or other economic penalty, the in-house counsel's actions may raise Fifth Amendment due process and voluntariness concerns because the underlying compulsion was brought on by a state actor, namely the U.S. government. Margolis and Vaala noted that by using corporate counsel and pressuring corporations to cooperate, the government is sometimes able to achieve indirectly what it would not be able to achieve on its own: inducing employees to waive their Fifth Amendment right against self-incrimination and minimizing the effectiveness of defense counsel's assistance.

So what are the pitfalls if private counsel compels such testimony and it is used against an employee in a criminal proceeding under the FCPA? Margolis and Vaala point out that the investigative counsel, whether corporate or outside counsel, could face state bar association disciplinary proceedings. A corporation could face disqualification of its counsel and the disqualified counsel's investigative results. For all of these reasons, I feel that The FCPA Blog summed it up best when it noted, "*the moment a company launches an internal investigation, its key employees—whether they're scheduled for an interview or not—should be warned about the 'federal' consequences of destroying or hiding evidence. With up to 20 years in jail at stake, that seems like a small thing to do for the people in the company.*"

B. The Parameters of the Attorney-Client Privilege

The recent trial of former PetroTiger co-Chief Executive Officer Joel Sigelman has brought the parameters of the attorney-client privilege to the fore again recently. As part of its undercover operation the FBI wired up the PetroTiger general counsel, Gregory Weisman, and instructed him to meet with Sigelman to discuss payments from the company to the wife of an official of the Columbian state-owned energy company, Ecopetrol.

Sigelman's counsel sought to have the video and audio recordings of this meeting suppressed based upon the attorney-client privilege that generally protects open communications between lawyers and their clients, where the client seeks legal advice. To determine whether Sigelman has a valid claim, one first must understand the parameters of attorney-client privilege. In an article presented in a Texas State Bar presentation titled, "The Evolving Attorney-Client Privilege: Business Entities," Court of Appeals Justice David Keltner wrote that under U.S. federal law, attorney-client privilege applies when the following are present:

1. A client seeks legal advice or a lawyer's services;
2. The person to whom the communication is made is a lawyer or his or her representative;
3. The communication relates to a fact disclosed from a client (a representative) to a lawyer (a representative);
4. Strangers are not present;
5. A client requires confidentiality.

The significance of meeting each of these five criteria is critical. If all are met, according to Keltner, "absent privilege, once the attorney-client privilege is properly invoked—the privilege is absolute."

The failure to meet criteria one is what doomed former co-CEO Sigelman's efforts; he was not seeking legal advice. It was former GC Weisman who flew to Sigelman's home to confront him over the fact that the FBI had come to his house asking questions about the payments made in Columbia. Finally, it is important to note that the attorney-client privilege belongs to the corporation, not to any one individual.

Neither Sigelman nor Weisman tried to claim another related, yet different privilege; the attorney-work product privilege. In his article, Keltner noted, "The attorney-client privilege and the attorney-work product doctrine are often asserted interchangeably. While there is some overlap between the two, the attorney-client privilege is significantly different than the attorney work-product doctrine."

Moreover, as codified in the Federal Rules of Civil Procedure, attorney-work product privilege "provides a qualified protection to materials prepared by party's counsel or other representative in the anticipation of litigation." The

doctrine exists because it permits lawyers to "work with a certain degree of privacy, free from unnecessary intrusion by opposing parties …"

Unlike the attorney-client privilege that belongs to a client, work-product immunity may be asserted either by the lawyer or the client. Keltner noted that while the attorney-client privilege is included in the Rules of Evidence, the work-product doctrine is included in the Rules of Civil Procedure in the series relating to discovery.

The attorney-client privilege, however, can be waived. While there is a general recognition that "only an authorized agent of a corporation may waive the privilege of the corporation," Keltner advises that the "most frequently encountered instances of losing the privilege through selective disclosure" are in responding to a government investigation; supplying information to a government agency; information disclosed in certain SEC filings or other required financial disclosures; in certain circumstances disclosures to external corporate auditors or accounting responses; any disclosure made to a third party not affiliated with a lawyer; and insurance disclosures.

How should we apply the above to the situation faced by former co-CEO Sigelman? Was he simply meeting with his lawyer or was he seeking legal advice? As reported by Joel Schectman in a *Wall Street Journal* article titled, "Secret Informant Recordings To Be Allowed in PetroTiger Case," the trial court distinguished having an attorney-client relationship from attorney-client privilege.

Schectman reported, "a judge in U.S. District Court in Camden said last week that merely having an attorney-client relationship isn't enough to make all conversations privileged—a client needs to be actively seeking legal advice. 'I cannot find a shred of indication that Weisman is there with the intention of giving legal advice to Sigelman,' Judge Joseph Irenas said, 'or the converse, that Sigelman was seeking legal advice from Weisman'."

Indeed it appeared that the corporate attorney was asking the co-CEO what to do. In the recorded December 2012 conversation, Sigelman was not seeking legal advice or even counsel from Weisman—if anything he was offering it. The FBI had turned Weisman into a cooperating witness and sent him to Sigelman's Miami apartment, asking Sigelman what he should do. As a cooperating witness and not known to Sigelman, he was secretly wearing a hidden camera on his body. According to court documents, Sigelman advised Weisman to calm down "regroup, go on vacation, collect yourself, come out [expletive] strong." It was clear from the tenor of the conversation that Sigelman was not asking Weisman for advice but Sigelman was giving advice to his lawyer."

Unlike the attorney-client privilege that belongs to a client, work-product immunity may be asserted either by the lawyer or the client.

The trial court did not opine on the question of who the client was in this situation. My experience is that most CEOs think of a general counsel as their personal lawyer. That view is misplaced, as a GC works for a company and the client is the corporation. While the court did not have to reach the question of who the client was in the Sigelman/Weisman meeting, the trial court might well have allowed the current corporate owners of PetroTiger to waive any privilege asserted by a former co-CEO. Schectman quoted Derek Andreson, a lawyer specializing in the Foreign Corrupt Practices Act, that attorney-client privilege "is often misinterpreted as broader than it is."

Did the FBI take advantage of some special type of relationship between Sigelman and Weisman? As reported in the *WSJ* article, in his brief attempting to suppress the evidence, Sigelman's counsel said, "Messrs. Sigelman and Weisman had a 'long-standing attorney-client relationship, one that fostered candor and trust between them—as any good attorney-client relationship should. The government took advantage of this trust'." Well, that would seem to be the nature of wiring up cooperating witnesses; if they cannot engender trust with those people they are surreptitiously recording, they are of little use to authorities.

As Mike Volkov has written in a wider review of the assertion of the attorney-client privilege: "The courts have responded with real antagonism to this over-assertion, or slap-happy, privilege claims. The courts are frustrated when they look behind these broad claims and find no basis whatsoever for a privilege claim, especially when it comes to compliance-generated information. Defense counsel also have routinely claimed privilege over e-mails which have an attorney cc'd, but the purpose of the communications had nothing to do with seeking legal advice. As can be seen from a number of important trial judge decisions, defense counsel are losing credibility rapidly with their broad privilege claims."

For the attorney-client privilege to be of use to you, certain hard work must be done to establish the attorney-client privilege in the corporate context. The five criteria listed by Keltner must be fulfilled for the privilege to apply. Simply having a chat with your lawyer or even the company's lawyer will not invoke the privilege or protect you.

Part VIII – Conclusion

In July 2015, the SEC released its enforcement action against the Mead Johnson Nutrition Corp. One interesting facet of this FCPA enforcement action was that the company had engaged in an internal investigation in 2011 of allegations of bribery and corruption in its Chinese business unit, but not developed any evidence of an FCPA violation. In 2013, when the SEC came calling with allegations based on a whistleblower, the company did another investigation, which turned up the nefarious conduct.

Marc Bohn, writing in *The FCPA Blog* in the article, "Mead Johnson: Lessons About Enforcement Practices and Expectations to Self-Report," said "In Mead Johnson's case, the company's failure to identify evidence of improper payments in 2011 suggests that the initial investigation may have lacked sufficient scope or resources, and the company's subsequent failure to promptly notify the SEC of that prior investigation when approached by the agency in 2013 suggests that it had not anticipated how to respond." I believe this means investigations that lack sufficient gravitas can pose significant risk because they increase the likelihood that something critical will be overlooked, potentially permitting misconduct to continue. But of equal significance is that it may well cost what Stephen Martin says is the most important thing you have when the government comes knocking—credibility, as such a lack of a serious response may give the appearance that your business is not truly committed to compliance.

Mead Johnson is but the latest case that demonstrates that companies must have a robust investigation protocol in place, and then perform a competent investigation when the facts and circumstances so require. Anything less could well communicate a lack of commitment to compliance and lead to greater penalties from regulators.

About the Author

Thomas Fox has practiced law for more than 30 years. He has been a trial lawyer in private practice, a general counsel in the corporate world, and is recognized as one the leading experts on the Foreign Corrupt Practices Act (FCPA) and compliance programs relating to both the FCPA and other anti-corruption laws.

He is the author of two prior award-winning books on the FCPA: *Lessons Learning on Compliance and Ethics* and *Best Practices Under the FCPA and UK Bribery Act*. He blogs daily on all things FCPA on his award winning blogsite, *The FCPA Compliance and Ethics Blog*, and podcasts on all things anti-corruption on *The FCPA Compliance and Ethics Report*.

Fox writes for a variety of anti-corruption compliance magazines and publications, and is a featured columnist for Compliance Week.