The Metropolitan
Corporate Counsel®

www.metrocorpcounsel.com

Volume 20, No. 4 April 2012

Can You Survive A Fraud Investigation? A Practical Guide To Preparing For Government Investigations

Roderick L. Thomas and Mark B. Sweet

WILEY REIN LLP

Government investigations can have profound effects on a company. The mere initiation of an investigation can disrupt operations, discourage morale, and, in some cases, trigger reporting obligations. If those investigations become public, the effects can be even more serious. Customers can question the integrity of the company, investors can dump shares or challenge management, and lenders can tighten credit. For government contractors and others in highly regulated industries, the exposure can multiply quickly. Government agencies often consider suspension or debarment, for example, based solely on the allegations in a complaint.

With such extreme leverage, the Department of Justice (DOJ) has negotiated record-breaking settlements. One pharmaceutical company paid $3 billion to settle civil and criminal fraud allegations. An international contractor paid $800 million to settle Foreign Corrupt Practices Act (FCPA) allegations. A government contractor accused of misleading the General Services Administration during schedule negotiations paid $200 million in the largest ever procurement fraud settlement under the False Claims Act (FCA).

Roderick L. Thomas

Mark B. Sweet

Small businesses are frequently targeted by investigators, too – especially if they have received preferential treatment by government agencies. Many small businesses lack strong ethics and compliance programs, leaving them particularly exposed. Fewer revenue sources and higher debt ratios mean that even a minimal enforcement action can have a disproportionate impact on a small business.

With the stakes so high and the frequency increasing, preparing for government investigations is critical – it can make the difference between being a witness and being a target. If you do learn that your company is the subject – or worse, the target – of a government investigation, how you respond can be just as critical to minimizing any further exposure.

This article explains how to prepare for and respond to government investigations. First, we discuss the growing exposure to government investigations and recommend some proactive steps to identify and address high-risk areas before an investigation begins. Second, we explain common techniques investigators use for collecting evidence and offer tips for responding to each type. These ideas are designed to be a practical guide for corporate counsel and compliance officers who want to minimize the risk that their companies get ensnared in investigations and to know what initial steps to take if a government investigation unfortunately does occur.

This article, of course, does not cover every scenario. The playbook for subject companies is not one-size-fits-all. The issues at each company and in each investigation are unique. The size and resources of the organization may necessitate alternative approaches. In light of these variables and the consequences of mishandling an investigation, the prudent first step is to solicit guidance from counsel experienced in these areas.

I. The Growing Target List

Government investigations of corporate offenses are on the rise. Over the last five years, DOJ began investigating an average of 138 new civil FCA cases each year – a 60 percent increase over the previous five years. Whistleblowers standing in the shoes of the government filed an additional 478 *qui tam* cases per year on average during the last five years, including a record 638 in 2011. The Federal Bureau of Investigation, meanwhile, increased the number of pending fraud and financial crime investigations by 38 percent from 2005 to 2009. FCPA investigations have likewise skyrocketed. In some industries, government investiga-

Roderick L. Thomas *is Chair of Wiley Rein's White Collar Defense practice in Washington, DC. He specializes in criminal and civil fraud allegations, internal and government investigations, False Claims Act and Foreign Corrupt Practice Act matters. He can be reached at (202) 719-7035.*

Mark B. Sweet *is a Partner in Wiley Rein's White Collar Defense practice. He counsels clients on complex issues for government investigations, whistleblower complaints, and mandatory disclosures. Mr. Sweet has conducted a number of internal investigations and is experienced in interacting and negotiating with government agents. He can be reached at (202) 719-4649.*

Please email the authors at rthomas@wileyrein.com or msweet@wileyrein.com with questions about this article.

tions are becoming an unfortunate cost of doing business.

At the same time, the definition of what the government considers "fraud" or "criminal misconduct" is eroding. Most people think fraud involves intentional bad acts, but the threshold for intent under the False Claims Act is much lower. A company can "knowingly" submit a false claim or cause another to do so through reckless disregard or deliberate ignorance of the truth or falsity of its statements. In other words, when doing business with the government, a company's inattention to red flags, failure to follow standard operating procedures, or failure to track information that forms the basis of a certification can be viewed by the government as fraud.

Similarly, some regulatory schemes place strict liability on corporate officers for the conduct of their companies. Violations of the Food, Drug, and Cosmetic Act (FDCA), for example, can be criminally prosecuted. Under the responsible corporate officer doctrine, corporate executives with authority or responsibility to prevent violations can be charged with criminal misdemeanors even without consciousness of wrongdoing at the company. In 2011, the DOJ obtained 21 criminal convictions and $1.3 billion in criminal fines, forfeitures, restitution, and disgorgement under the FDCA.

Small businesses are becoming the focus of government investigations more often, too. In government contracting, investigators have targeted businesses that falsely claim to meet eligibility criteria for preferential treatment and set-aside contracts, as well as companies that use eligible business as a "pass-through" to get access to set-aside contracts. Furthermore, the Small Business Association (SBA) Inspector General has pushed for legislation to make such fraud prosecutions even more attractive to prosecutors. The legislation would define the government's loss as the full amount paid on the contract – a steep penalty for cases in which the government may have obtained the full value of any goods or services it acquired.

II. Proactive Steps To Take

No matter how well intentioned a company may be, government investigations can be hard to avoid in the current enforcement climate. Fortunately, proactive measures can reduce the likelihood of an investigation and maximize your company's chances of getting through one unscathed.

A. Assess Risk Areas

To prepare for a possible government investigation, you must first understand where your risk is greatest. History can provide a good starting point. If the company has had problems before, make sure these have been addressed – on paper and in practice. If other companies within your industry have faced investigations, take a hard look at similar practices within your company. Finally, review universally risky activities, such as timekeeping and billing, interactions with the government, teaming with new partners and subcontractors, gifts, and business development. Each one should be subject to internal controls that minimize the risk of fraud or abuse.

Obviously, this list is not comprehensive. Each business's pressure points will vary depending on the structure of the company, the individuals who work there, and the nature of the industry. Once you understand the business and its risks, however, you can create or strengthen a compliance program to address the risk areas.

B. Strengthen the Compliance and Training Plan

A robust compliance and training plan is the foundation of assuring government investigators that a company is a good citizen. DOJ has identified a compliance program as one of the key factors it considers in whether to charge a company in a criminal case. In particular, the government considers whether the program is designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program. An effective plan can show that management treats ethics and compliance seriously and has taken reasonable measures to prevent misconduct. It can also show that the misconduct was isolated and distance the actions of an individual employee from those of the company. A toothless program, on the other hand, may be viewed by prosecutors as tacit encouragement by management to engage in misconduct to achieve business objectives. In the event misconduct occurs and a company is charged, the U.S. Sentencing Guidelines also consider an effective ethics and compliance plan as one way an organization can remedy a criminal harm.

The specific operating procedures of a compliance plan will depend on the nature of the business and applicable laws and regulations. Additionally, the depth of a compliance program may depend on the size of the company. At the core, though, all compliance programs should:

- Adopt and distribute a written code of conduct;
- Promote an ethical culture through executive oversight of compliance and regular communications on the subject;
- Assign responsibility for ethics and compliance to specific individuals with access to executive management of the company;
- Develop procedures to prevent and detect improper conduct, such as auditing and monitoring of business operations;
- Establish internal reporting channels, including an anonymous hotline, through which employees can report potential improper conduct or violations of company policy;
- Develop procedures to assess reports of improper conduct and, if credible evidence exists, disclose the improper conduct;
- Develop procedures to implement corrective action, including discipline for wrongdoers and steps to prevent recurrence;
- Screen principals of the company for prior misconduct;
- Train all employees – both new and experienced ones – on ethics;
- Require full cooperation in internal and external audits; and
- Plan to periodically re-evaluate the compliance program.

To make sure that risk areas are addressed and operating procedures are realistic and enforceable, get buy-in from business managers before implementing any compliance plan. For a plan to be permanent and effective, corporate management must set the right tone, making documented efforts to communicate to employees that ethics and compliance are important company values. Finally, to keep the plan relevant, update it to reflect recent events.

C. Review Other Internal Controls

Once the basic compliance and training plan are in place, counsel can help review other internal controls to ensure their adequacy for preventing fraud and other misconduct. For example, here are some practical suggestions for minimizing exposure to a government investigation:

- Design timekeeping and billing systems to have multiple layers of review

and minimal opportunities for manipulation;

• Restrict interactions with government officials to experienced managers and other employees trained in doing business with the government;

• Verify certifications and other statements to the government for accuracy;

• Monitor expenses for improper gifts and other things of value, or for any unusual or problematic activities;

• Set up document retention capabilities, such as software that allows for searching and copying, a flexible and retrievable backup system, and centralized storage of documents;

• Perform due diligence on new partners and subcontractors; and

• Review new business ventures for compliance and consistency with company ethics.

No compliance plan is foolproof, but these steps will show a corporate commitment to ethical conduct. If the government does come knocking at your door, your company will be well positioned to respond to the investigation.

III. Global Principles

Regardless of how the government pursues its investigation, companies should abide by some global principles:

• Consult legal counsel before responding to any government investigation. In criminal cases, the company and its employees have a constitutional right to do so. Counsel can often work with government attorneys or agents to narrow the scope of requests, negotiate with agents executing a warrant to ensure an orderly process, glean additional insights from early discussions with investigators, and get a head start on assessing the company's exposure to liability.

• Be truthful and accurate in any statements to the government. Failure to do so could expose the company and its employees to separate criminal liability. *See* 18 U.S.C. § 1001.

• Never do anything to impede or obstruct a government investigation, such as deleting, concealing or altering relevant documents. Again, such actions could expose the company to separate criminal liability. *See* 18 U.S.C. § 1505.

Beyond these principles, the company's response should be tailored to the circumstances of the investigation and the way in which the government pursues its investigation. Since each investigation is unique, it may be necessary to deviate from these suggestions or take additional measures, depending on the circumstances.

IV. Subpoenas For Documents

Most government investigations of fraud, kickbacks, gratuities and other improprieties by corporations begin with a subpoena for documents from a grand jury or the inspector general's office of an agency. If a company receives a subpoena, it can take several steps to respond effectively. First, with assistance from counsel, immediately

• Assess the scope of the subpoena, identify potential sources of documents, and preliminarily determine the difficulty in collecting, reviewing and producing these materials by the stated deadline.

• Instruct employees to preserve all potentially responsive materials, including both electronic and paper documents. The best way to do this is to issue a written document preservation notice to any relevant employees that supersedes the company's regular document retention policy. The company should make sure its information technology department is aware of the need to preserve documents and suspend routine deletion of old files or emails and recycling of old backup tapes.

Once these immediate steps have occurred, begin formally responding.

• Let counsel contact the government attorney or agent listed on the subpoena. Counsel can affirm the company's intent to cooperate with the investigation and identify himself or herself as a point of contact for future requests or inquiries, including employee interviews. Additionally, counsel can learn as much as possible about the investigation, including whether the company is a target, subject, or witness at that time. While government officials are sometimes reluctant to share much about an investigation or identify a company as a target, they may shed light on what they expect the company to provide. If any requests are unreasonably broad or demand more than can be produced by the deadline, counsel can work with the government to narrow or prioritize the requests and/or set a reasonable schedule for production.

• Appoint a custodian of records who will be responsible for compliance with the subpoena. This employee should manage and track preservation, collection, and production efforts. At the end of the process, the custodian of records should be prepared to describe these efforts, either in a certification or in testimony, if the government requires it.

• Start collecting potentially relevant documents. In collecting electronic materials, consider whether to make forensic copies, use in-house capabilities to copy or search, and/or instruct employees to collect their own materials. The best plan will depend on the demands of the government, the reliability of each option, the technological capabilities of in-house staff and systems, and, of course, cost. Key players may require special treatment.

V. Civil Investigative Demands

Another form of inquiry the government may use is a civil investigative demand (CID). Long a staple of antitrust investigations, CIDs are becoming common in the False Claims Act cases due to recent changes in the law. Like a subpoena, a CID can require production of documents with a certification that a response is complete. Additionally, CIDs can demand written answers or oral testimony, under oath, to questions about the documents or information at issue. CIDs give prosecutors nearly all of the tools of civil litigation discovery – access to relevant documents, knowledgeable employees, and sworn statements – at the earliest stages of an investigation.

Given the resemblance of CIDs to litigation discovery, recipients should consult with counsel before responding. In addition to the steps recommended above for responding to subpoenas, CID recipients should consider engaging counsel to conduct a quick internal investigation. CIDs often demand factual statements and explanations for documents that a whistleblower or investigator may have selected. An internal investigation can provide the context for these documents and allow the recipient to make informed statements about the meaning of any facially problematic documents. CIDs give prosecutors the power to develop evidence and bind the recipient quickly – a respondent must move just as quickly to marshal the facts and assess exposure.

VI. Investigative Interviews

Sometimes law enforcement agents will contact employees directly to learn more about the company. These interviews may occur at the office, at employees' homes, or at nearby public sites, such as a local coffee shop. Often interviews

are unannounced. A company may request advance notice of any interviews, but the government may choose not to inform the company before interviewing lower-level and former employees.

The presence of law enforcement agents can be unnerving and intimidating. Accordingly, a company should prepare its employees for this possibility and advise them of their rights and obligations. Specifically, the company should consider advising employees that

- It is the employee's choice whether to speak with the government agents. An employee has a right not to submit to an interview with the agents. If the employee decides not to do so, he or she should politely, but firmly, decline to be interviewed.
- If an employee does choose to answer questions, he or she must always tell the truth, no matter how casual or innocuous the conversation. Failure to do so could result in separate criminal liability for the employee and the company.
- The employee has a right to understand the agent's questions, and to fully and carefully explain any answers. The employee should not guess or speculate about matters of which he or she is not certain.
- Each employee is entitled to consult legal counsel before consenting to an interview and to have legal counsel present for any interview. The company's legal counsel can advise the employee of his or her options for personal counsel and be available to attend the interview.
- The employee should obtain a copy of any statement he or she signs.
- If the employee receives a subpoena for testimony, he or she should be able to, in most instances, have the date or time of the appearance changed if necessary.

VII. Search Warrants

When evidence may be fleeting, law enforcement agents can obtain a warrant to search a corporation's facilities and seize any relevant materials. This may include computers, servers, local storage media (*e.g.*, thumb drives or compact discs), and paper documents. If possible, a company subject to a search warrant should contact counsel when the agents arrive or as soon as possible thereafter. Additionally, the company should consider the following measures:

- To avoid confusion, designate one person to deal with the government agents and consider relocating or sending home employees who are not essential to the search.
- Review and copy the search warrant and supporting affidavit, if the affidavit is available. The company has a right to do so under Federal Rule of Criminal Procedure 41(f). Take careful note of the scope of the warrant. The company may ask the agents to wait until the warrant and supporting affidavit have been completely reviewed before the search begins, although the agents are not required to wait or even to provide a copy of the warrant until the end of the search.
- Identify all government agents participating in the search.
- Monitor the agents to make sure they limit their search to the scope of the warrant. You are not required to agree or consent to searches of areas beyond the scope of the warrant. You may do so in the spirit of cooperation, but keep in mind that additional searching may subject the company to further scrutiny and exposure.
- Note everything the agents examine or take, and, as much as possible, record the agents' questions and employees' responses. If agents are moving on multiple fronts, consider asking select employees to assist counsel by taking detailed notes as well.
- Do not interfere, however, with the agents' search of the area described in the warrant. Similarly, instruct employees not to interfere with the search – either by physically getting in the way or by concealing, moving or altering materials.
- Direct employees to cooperate with the search, but advise them that they are not required to answer questions unrelated to the search.
- Ask the agents to allow the company to copy any materials the agents take. Explain that the company may need these records for its continuing business operations.
- Obtain a complete inventory of all property taken *before* the agents leave the facilities. The company has a right to this inventory under Federal Rule of Criminal Procedure 41(f).

VIII. Wires And Phone Taps

More aggressive techniques for collecting evidence – such as tapping phones, using undercover agents and recording conversations through wires – have been historically rare in white collar cases. These tactics, however, are becoming more common for investigators. In 2010, DOJ charged 22 individuals with violations of the Foreign Corrupt Practices Act for a scheme to bribe a supposed foreign government official. In addition to executing search warrants, the FBI gathered evidence through undercover agents who posed as sales agents for a fictional African official. The government touted its indictments as the first large-scale use of undercover law enforcement techniques to uncover FCPA violations, although it has since struggled to convict any of the defendants.

In 2011, the government prosecuted Raj Rajaratnam and other executives at the Galleon Group hedge fund for insider trading and conspiracy based on evidence gathered through wiretaps. The Rajaratnam conviction resulted in the largest penalty ever assessed against an individual for insider trading.

The nature of these investigative tactics leaves little chance to respond. If you become aware of wiretaps or other aggressive investigative methods, contact counsel immediately to discuss options for proceeding.

IX. Conclusion

This primer only provides some general suggestions for how to prepare for and respond to a few common government investigative techniques. Since each investigation is unique, and a company's response can greatly affect its legal strategy, we recommend consulting with legal counsel as soon as possible upon receiving a subpoena, learning that government agents are interviewing current or former employees, being served with a search warrant, or responding to any type of government investigation.

* * *

This article represents the views of the authors and should not be construed as providing legal advice or legal opinion. Readers should consult their attorneys with any specific legal questions about these matters.