

# Knock, Knock. Who's There? The Government.

**Abbe David Lowell**  
**McDermott Will & Emery LLP**  
**Washington, D.C.**

**Obiamaka P. Madubuko**  
**McDermott Will & Emery LLP**  
**New York, New York**

## INTRODUCTION

It used to be (“the good old days of white collar practice”) that everyone acted orderly – businesses and their officials were asked for information; perhaps, there was a subpoena to tidy things up; interviews were scheduled; decorum prevailed. Well, if those days ever existed, they do not any more. The most well-known banking firm on Wall Street can now expect the same treatment as the “Bada Bing” club in *The Sopranos*.

It is a naïve company and its lawyers (if not worse than naïve), that is not understanding the changed world in which they live and are talking steps *before* they hear from Uncle Sam. Luckily, companies and their counsel do not have to engage in rocket science or re-invent the defense wheel to be ready.

In today's post-Enron/Madoff world, companies must face the reality that the prospect of dealing with a government investigation may not be as remote as it once was. Given the recent global economic crisis and the discovery of large scale fraud schemes (like Bernard Madoff's) that went undetected for years by law enforcement authorities, the era of government crackdowns on corporate fraud is in full bloom. Were allegations of routine corporate financial wrongdoing not frequent enough, a whole new law enforcement industry surrounding the Foreign Corrupt Practices Act is also thriving. Government investigations are now easier to initiate and the government has become more aggressive in terms of the investigatory tactics and procedures they employ. Techniques, like the execution of a search warrant, that were rarely done on “legitimate” businesses even ten years ago are commonplace. Given this new reality, companies must take stock of their readiness if the government were to come knocking at their door. Being prepared

and knowing how to respond to government investigators is critical. This paper will explore the various ways a government investigation can be initiated and provide practical advice for how companies can think ahead and prepare for a government investigation before it happens.

#### **A. How Government Investigations Begin**

More than ever before, companies (both large and small) need to think ahead and have a plan in place for how they would respond to a government investigation – whether it be in the form of a government subpoena or a call from an employee informing his supervisor that the government has raided the company or government agents are on-site requesting to interview company employees.

These types of government initiated contacts are becoming more routine in corporate America and the amount of government investigations has steadily increased in recent years. Just looking in the area of Foreign Corrupt Practices Act investigations, the U.S. government brought 74 enforcement actions in 2010, an 85% increase over the number brought in 2009.<sup>1</sup> In the area of False Claims Act investigations, the government had 1,116 new criminal health care fraud investigations involving almost 3,000 defendants in 2010 and federal prosecutors had a total of 1,787 criminal health care fraud investigations pending.<sup>2</sup> Last year, the U.S. government obtained \$3 billion in False Claims Act settlements, the largest since the government started tracking this information in 1986.<sup>3</sup> This figure is up more than 20% from settlements collected by the government in 2009. Given the recent changes in healthcare policy, it is of no surprise that healthcare fraud remains a top government enforcement priority, and that of the \$3 billion in 2010 settlements and judgments, \$2.5 billion relate to healthcare sector.<sup>4</sup> And with the passage of the Dodd-Frank Act in July 2010, corporate whistleblowers now have powerful financial incentives to report corporate fraud and wrongdoing to the government, which will inevitably lead to more government investigations.<sup>5</sup> The U.S. Department of Justice has also increased their “get tough” rhetoric against corporate fraud as can be seen by recent statements of high ranking prosecutors such as Assistant U.S. Attorney General of the Criminal Division, Lanny Breuer, who has been quoted as saying that “[c]harging individuals is part of a deliberate enforcement strategy to deter and prevent corrupt corporate conduct before it happens. And rest assured that we will seek equally tough sentences, including significant jail time if appropriate, to reinforce this message of deterrence.”<sup>6</sup>

There are many ways a government investigation can be started. For instance, it is not uncommon for the government to send out industry-wide “sweep letters” in an effort to curb or expose wrongdoing and for the government to make broad use of its subpoena power to fight corporate crime. And if it involves a matter of national security, the government can issue national security letters, which can request information from companies and their employees without having to meet traditional probable cause standards. Government investigators can also make voluntary requests for documents or execute search warrants and request interviews from employees or other individuals they think have knowledge of the matters they are investigating. In extreme cases, the government has initiated investigations using covert investigatory tactics, such as use of undercover agents, wire tapping or other surveillance methods. In some instances, arrest warrants are issued.

#### **B. Be Prepared For the Unexpected**

Given that government investigations are on the rise, all companies should prepare for the unexpected and have a plan in place in advance that includes information about document retention, protocols for talking to government investigators, assurances about providing counsel for employees and other safeguards to protect corporate interests.

The government response team should include a point person to refer all government related inquiries to and a training component so that all employees know their rights and how to deal with government

investigators. The plan should also contain a media crisis strategy to outline how the company plans on managing communications with the public, its stakeholders, and the government during a pending government investigation. The company should maintain an organized filing system and have a document retention policy in effect, which can reduce or minimize the amount of time and resources the company will spend in responding to a government subpoena or other document request. It is equally important, however, that there be a point person assigned to handle document preservation issues and to issue a document retention or litigation hold notice should a government investigation begin. Finally, the plan should recognize and provide for the maintenance of backup copies of critical files to prevent information loss in the event of a government raid.

Because government investigations are not generally something companies expect will happen to them, many companies fail to plan for such an event and are caught off-guard when they find themselves approached by government investigators. Without any training or guidance, their employees can panic or respond without thinking things through. A hasty or uncoordinated response can result in doing more harm than good and can lead to more headaches, questions or further government intervention. To avoid these pitfalls, companies should adopt a government investigation response plan, train its employees on interacting with government agents and designate appropriate persons for each function noted above.

While government investigations can be initiated in many ways, there are generally three typical approaches: (1) subpoena or document request; (2) request for interviews; or (3) government search warrant or raid. With each approach, the constant principle is that there are ways a company can and should prepare itself in advance for these government initiated contacts. Remember, being prepared for such a contact is not an admission or concession that the company has engaged in any wrongdoing.

### **C. Responding to Government Subpoenas**

Once a government subpoena is received, it should be immediately forwarded to legal counsel to coordinate the response. Legal counsel needs to determine the scope and timing of the subpoena and whether any modifications are needed. The scope of the government's authority in issuing the subpoena also needs to be determined. If it is a grand jury subpoena, legal counsel responding to the subpoena should contact the lead prosecutor to determine whether the company is a Target, Subject or Witness of the government's investigation. The time, effort and cost it would take to respond to the subpoena will also need to be estimated. In each case, counsel should identify the type, amount and location of the relevant documents being requested and identify who within the company has knowledge about these documents or the subject matter contained in the subpoena. Counsel should also weigh the costs and benefits of compliance versus non-compliance, although in most cases, responding to the subpoena is the preferred course of action. Upon receipt of the subpoena, counsel should also institute a litigation hold memorandum to ensure that all relevant documents are being preserved as well as to suspend any document destruction policies that could affect the requested documents.

Failing to produce or preserve relevant documents can expose a company to significant liability. Courts have sanctioned companies millions of dollars for failing to properly preserve and/or produce relevant documents, including records that are in an electronic format such as text messages, email, backup tapes or metadata. In recent years, the federal courts have issued very high penalties to companies that fail to abide by these rules. For example, in 2008, a federal court in California sanctioned Qualcomm over \$8.5 million, which included the full amount of defendant Broadcom's attorneys fees, for intentionally hiding, recklessly ignoring and failing to produce relevant documents.<sup>7</sup> The court went further and found Qualcomm's attorneys in violation of their ethical violations by ignoring warning signs that their client's document search was inadequate. Thus, in investigations where outside counsel is retained, outside counsel must retain full control over the document collection, review and production process to avoid ethical and monetary sanctions for them and their clients.<sup>8</sup>

In addition to monetary sanctions, discovery abuses during a government investigation can result in default judgments, adverse inference instructions, and a loss of affirmative defenses.<sup>9</sup> In the recent “Shot-Show” case involving the arrest of 22 security vendors at a Las Vegas gun show in January 2010, one of the defendants recently filed a motion to dismiss in January 2011, alleging that the government destroyed or failed to preserve text messages between the FBI and a key informant that would have been relevant and material to the defense.<sup>10</sup>

To avoid these negative consequences, companies should adopt a document collection protocol that includes a written set of guidelines for staff responding to the subpoena to follow. These guidelines should call for the initiation of litigation holds and other document preservation protocols to ensure the preservation of all relevant and responsive records. Second, the protocol should include a timetable regarding the collection, review and production of documents to the government as well as safeguards to ensure the protection of confidential and privileged documents (*e.g.*, production of privilege logs for documents withheld from the production based on privilege and the identification of confidential materials and stamping produced documents produced Confidential). As the document review progresses, reviewers should identify and mark all “key” and “privileged” documents for further review. The entire process should be overseen by experienced counsel and not delegated to a junior attorney. Employees who possess relevant documents should also be asked to sign declarations that they have conducted thorough searches of their files, email, computer disks, storage areas and other workspaces for responsive documents. Documentation of the areas searched should be kept by counsel handling the production.

#### **D. Responding to Government Requests for Interviews**

While the issuance of a government subpoena can be disruptive if not handled effectively, the presence of government agents at the worksite can be even more unsettling if the company has not thought out an approach for dealing with the government in advance. The reason for the visit can be multi-fold – the government can be investigating some conduct of the company, an employee of the company, a competitor or a third party the company does business with. Requests for employee interviews can occur at the place of business or at the employee’s home or by phone. In any event, it is important to train your employees on how to handle this situation if it were to arise.

First, employees confronted by a government agent should always ask for identification and get the contact information for the agent, including the agency they work for, contact number, their business card, and/or badge numbers if applicable. Employees should remain polite and courteous but exercise caution. Some employees may feel intimidated by the government investigator even if they have done nothing wrong. Others may feel nervous or excited and become overly talkative to their or the company’s detriment. The pitfalls of not having a government investigation response plan in place in advance are that employees could provide inaccurate or conflicting information that could lead to more government intervention and questions. Employees may also inadvertently waive important corporate legal rights by providing information that may be protected by privilege or privacy laws. The worst consequence of not having a coordinated response is that the government may interpret the response wrongly – it may be viewed as being not upfront, lacking in credibility or worse yet, as an obstruction of justice.

Thus, in addition to asking for proper identification, employees should know that they have the right to decline the interview or to request that counsel be present when they are interviewed. They should also immediately report the government contact to the company’s legal counsel and seek advice before consenting to an interview, particularly if the subject of the interview involves their work for or at the company. They should learn the purpose of the government investigator’s visit and know that they do not have to provide any documents without a subpoena and that, in some cases, doing so may violate their obligations to the company and/or waive some of the company’s legal rights. They should also

contemporaneously (or shortly after the interview) document the government contact in detail (*e.g.*, questions asked and answers given). All of these precautions should be outlined in an employee's handbook or included in employee training sessions.

The employees most likely to be the first point of contact for government investigators (*e.g.*, front desk receptionists or security guards) should also be trained on these protocols so that they know how to direct such requests – ideally, to legal counsel. Company personnel responsible for dealing with government agents should find out who the agent has contacted at the company in the past and work out a procedure for future contacts so they can be coordinated. The company representative in charge with dealing with the government should also find out under what authority the agent is acting (*e.g.*, U.S. Code provision, state or other federal statute, or other law). In any event, employees dealing with government agents with regular contact with the company (*e.g.*, auditors or other government compliance personnel) should be cautious if they receive questions that are outside the normal course of past inquiries, as this too may signal that the government may be contemplating to initiate an investigation.

### **E. Responding to Government Search Warrants or Raids**

This is the most stressful type of government contact because an unsuspecting employee is usually approached, without notice, by a government agent or agents who hand him or her a very official looking document that gives these agents the right to search certain areas of the company and to take certain information from the company without the company's consent. Employees are then usually rounded up by the agents conducting the search and sequestered to a certain area while the search is in progress. In some cases, some of the agents will attempt to interview these employees while the search is underway. This scenario can be very intimidating and an unprepared employee can panic or feel completely helpless. This is why it is important that employees are trained on what they can do and, importantly, what their rights are when dealing with government agents.

Employees should know who to call if approached with a search warrant and who is in charge of handling such situations. The company should designate a point person at each facility or location where the company has operations who can be responsible for handling search warrants or government inquiries. Employees should also know that they can decline requests to be interviewed by government agents and can request to have counsel present during any interviews they agree to. Employees should not interfere with the government's enforcement of the search warrant in any manner and to direct the warrant to a senior manager and refrain from conversations with the agents. The search warrant response team point person should request a log or inventory of everything the government seizes, identify all the government agencies and personnel present during the raid and, if possible, obtain their contact information, and monitor the search as it is progressing. The point person should be professional and courteous to government investigators and document anything the government seizes that is privileged, confidential or critical to business operations.

To recap, in order for companies to effectively respond to the execution of a government search warrant, they should take the following steps: (1) designate a search warrant response team in advance; (2) call legal counsel immediately upon receiving the warrant; (3) identify the lead government investigator and all involved government agencies and personnel; (4) obtain a copy of the warrant and review it to determine its scope and locations to be searched; (5) monitor the search as it is being executed and document everything that is seized. Note if any seized items are privileged, confidential, or critical to business operations; and (6) instruct your employees to remain calm and to cooperate with the government investigators executing the search. In most cases, it will involve the employees staying out of the investigators' way. Taking these simple steps can help bring calm and order to an otherwise stressful situation.

## **F. Dealing With Whistleblowers**

Companies also need to think ahead and prepare for how to deal with whistleblowers. In today's heightened enforcement environment, whistleblowers have been given powerful financial incentives to report suspected wrongdoing directly to the government. In many cases, this will result in the initiation of a government investigation without the company having much time to respond or to even be aware that there is an alleged problem in the first place before being initially contacted by government investigators. Certain precautions must be taken to deal with employees who choose to bypass internal reporting methods and instead report alleged misconduct directly to the government.

In order for companies to avoid future liability, particularly in light of enhanced whistleblower protections under new legislation like the Dodd-Frank Act of 2010, companies need to tread carefully when dealing with whistleblowers. Under Dodd-Frank, whistleblowers are entitled to receive between 10-30% of any monetary sanction over one million dollars that the government collects if they provide original information of a securities or commodities law violation to the government. Employees who are whistleblowers that have been retaliated against or otherwise discriminated against based on their decision to file a report are also empowered under Dodd Frank to bring a federal lawsuit to obtain reinstatement, back pay, attorneys fees and other costs. Thus, when dealing with a suspected or known whistleblower, companies should take the following precautions:

- DO document (in real time) all interactions with this employee;
- DO ensure that all decisions involving this employee's terms and conditions of employment are supported by legitimate business reasons;
- DO take claims made by this employee seriously – investigate them to the extent warranted by the facts; and
- DO make the employee sign a statement in the exit interviews detailing any alleged wrongdoing he or she is knowledgeable about.

In order to encourage compliance and internal reporting, companies should work towards nurturing a culture of compliance among their workforce. This can be achieved by setting the tone at the top and having in place a robust compliance program. Giving employees incentives to report suspected violations internally or to voice compliance concerns early on is also critical. Incentives like the use of hotlines, employee surveys or other anonymous reporting methods are to be encouraged. Companies can also incentivize compliance by stressing confidentiality to those who make reports and by promptly investigating reported concerns. Companies should make a concerted effort to communicate with the whistleblowers about the Company's response to their complaint to the extent possible. Companies should also strengthen their anti-retaliation protections for employee whistleblowers and train their employees on these protections. Employees who file accurate internal reports or voice compliance related concerns should be rewarded with additional compensation or other perks, as should supervisors or managers of divisions or business units where compliance is shown to be a key driver.

Companies should also not fall victim to common pitfalls when dealing with whistleblowers – meaning that managers or other employees should not take actions that could put the company at risk for whistleblower lawsuits. Such actions would include retaliating against a whistleblower based on the employee's decision to file a report, whether internal or external. To the extent that the company wishes to take disciplinary action against an employee found to have engaged in wrongdoing (regardless of whether they filed a report) or against an employee who is found to have purposely filed a false report, companies should be sure that any disciplinary action taken is well-documented, supported by legitimate

business reasons, and that any disciplinary or termination decisions made against this employee or other key employee-witnesses in a pending government investigation are not hastily undertaken. Companies should also not pre-judge the complaint based on the person making the complaint. Complaints made by known whistleblowers should be investigated based on the facts presented and not based on the reputation of the person making the complaint.

## Conclusion

In order to ensure that your company is prepared in the event of a government investigation, you need to have a plan in place *in advance* that outlines the steps you should take to deal with various types of government initiated contacts. In addition to designating a team to respond to government investigators, companies should ensure their files are well organized and have a document retention policy in place. They should train their employees in how to respond to various government initiated contacts so that they know their legal rights when dealing with government investigators and can avoid any situation where a claim of obstruction could be made. Companies need to have a coordinated response and retain counsel for their employees, as needed, and importantly, determine whether an internal investigation is needed and, if so, who should conduct the investigation. By following these steps, companies can manage and navigate themselves safely through any government investigation.

---

<sup>1</sup> See Melissa Aguilar, *2010 FCPA Enforcement Shatters Records*, Compliance Week, January 4, 2011. “The number of FCPA enforcement actions jumped 85 percent in 2010, shattering the prior record set in 2009, according to data tracked by the law firm Gibson Dunn & Crutcher. The Department of Justice and the Securities and Exchange Commission brought a combined 74 FCPA enforcement actions in 2010, far surpassing any prior year in the statute’s 33-year history. The SEC brought 26 enforcement actions, beating a previous high of 20 actions in 2007, while the DoJ filed 48 cases, demolishing 2009’s record 26 actions, according to GDC’s 2010 Year-End FCPA Update. Eight of the top 10 monetary settlements in FCPA history occurred in 2010.” *Id.* at 1.

<sup>2</sup> See *id.*

<sup>3</sup> See U.S. Department of Justice, *Department of Justice Recovers \$3 Billion in False Claims Cases in Fiscal Year 2010*, Nov. 22, 2010, available at <http://www.justice.gov/opa/pr/2010/November/10-civ-1335.html>.

<sup>4</sup> See U.S. Department of Justice, *Health Care Fraud and Abuse Control Program Annual Report FY 2010*, The Department of Health and Human Services and The Department of Justice, Jan. 2011, available at <http://www.justice.gov/dag/pubdoc/hcfareport2010.pdf>.

<sup>5</sup> See Jean Eaglesham and Brooke Masters, *US to pay big sums for Wall St tip-offs*, Financial Times, Aug. 8, 2010, available at <http://www.ft.com/cms/s/0/efa8a32a-a31a-11df-8cf4-00144feabdc0.html#axzz1CMjqDxGt>; see also Dave Clarke, *Dodd-Frank law has led to increase in tips-official*, Reuters, Feb. 4, 2011, available at <http://www.reuters.com/article/2011/02/04/sec-whistleblower-idINN0423691220110204>.

<sup>6</sup> Statement of Lanny Breuer, Assistant Attorney General, Criminal Division to Compliance Week 2010 (May 26, 2010). This sentiment was echoed by the Federal Bureau of Investigation’s Assistant Director, Kevin Perkins, who said in January 2010 that “[i]nvestigating corruption at all levels is the number one priority of the FBI’s Criminal Division. In this era of global commerce, the FBI is committed to curbing corruption at home or overseas.”

<sup>7</sup> See *Qualcomm v. Broadcom Corp.*, 05 Civ. 1958-B, 2008 WL 66932, at \*9 (S.D. Cal. March 5, 2009).

<sup>8</sup> See *In re Sept. 11th Liab. Ins. Coverage Cases*, 243 F.R.D. 114 (S.D.N.Y. 2007) (imposing sanctions of \$1.25 million because defendants and its counsel found to have deleted ESI and delayed production of relevant

---

documents); *Coleman Holdings, Inc. v. Morgan Stanley & Co., Inc.*, CA 03-5045 AI, 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005) (awarding \$850 million in punitive damages based, in part, on defendants' failure to search backup tapes); *see also Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 430 (S.D.N.Y. 2004) (awarding \$20.2 million in punitive damages based on UBS' willful deletion of responsive email).

<sup>9</sup> *See Arista Records LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124 (S.D.N.Y. 2009) (precluding assertion of affirmative defense for "strong evidence of severe wrongdoing" including wiping the hard drives of seven employees and later dismissing defendant's motion for summary judgment as moot and granting plaintiff's summary judgment motion in full); *see also Smith v. Silver Smith & Frampton/Vail Assocs. Real estate, LLC*, No. 06-cv-02206-JLK, 2009 WL 482603 (D. Colo. Feb. 25, 2009) (adverse inference granted where documents destroyed well after litigation hold notice had been put in place); *Atlantic Recording Corp. v. Howell*, No. CV-06-02076-PHX-NVW, 2008 WL 4080008 (D. Ariz. Aug. 29, 2008) (default judgment granted after party permitted the "brazen destruction of evidence").

<sup>10</sup> *See* Abigail Rubenstein, *US Says Deleted Texts Held No Evidence In FCPA Case*, Law360.com, Jan. 28, 2011, available at <http://www.law360.com/whitecollar/articles/222172>.