Bloomberg Law Reports® Corporate Counsel

Government Agents Are in the Lobby. Do You Have a Plan?

John F. Cannon and Kathleen Marcus, Stradling Yocca Carlson & Rauth

Imagine the following: it's a beautiful Friday morning, and you're smiling as you drive to work. Sipping your coffee, you congratulate yourself on your good work. You have helped the company close the quarter on a high note. Business is up and so is the company's market share. What's more, the company's stock just reached a new high. With that thought, your grin broadens as you estimate the value of your options. Your hard work is about to pay off. Maybe you'll leave the office early tonight and celebrate. After all, you deserve it.

Unexpectedly, your cell phone rings.

"S-sir, there are some … some people from the government," your receptionist stutters, voice quivering. "They're in the lobby and they have some papers; they are saying they are going to search the building and want to take our computers. What do we do?"

What *do* you do? You're surprised, certainly. The government is likely counting on that reaction. But will your surprise deteriorate into panic? Will your panic lead to damaging decisions and imprudent actions? No, because *you* have a plan.

Recognizing the Risk

Most businesses underestimate the likelihood of this scenario. Yet the prospect of government agents advancing through your company's lobby is no longer as remote as in years past. The financial crisis of the late 2000s has reversed previous trends toward lighter regulation and laxer enforcement, creating an atmosphere of heightened oversight that no business executive or general counsel should regard lightly.

Concurrently, market events have spurred a raft of new legislation and regulation impacting a wide range of U.S. businesses. The 2010 Dodd-Frank Act, for example, has been described as "the biggest expansion of government power over banking and markets since the Depression."[1] According to the U.S. Chamber of Commerce, the Act will require 520 regulatory rulemakings, 81 studies, and 93 reports.[2] Moreover, with its creation of the Consumer Financial Protection Bureau, Dodd-Frank's reach may stretch "far beyond the financial services industry" to include companies "not primarily in the business of consumer finance."[3] All told, Dodd-Frank will reshape over a dozen regulatory agencies, many with enforcement powers.

Public anger over fallout from the financial crisis (e.g., lost homes, depressed 401k's, executive payouts, etc.) has also pressured agencies to enforce new and existing rules more aggressively. The Enforcement Division of the U.S. Securities and Exchange Commission ("SEC"), for instance, has a new leader, a new look structure, and several new initiatives that have led to some notable results, including the record-breaking $550 million settlement with Goldman Sachs.[4] Not surprisingly, the SEC brought more enforcement actions in 2010 than in any prior year,[5] ultimately demanding nearly $3 billion in penalties and disgorgement.[6]

Meanwhile, the Department of Justice ("DOJ") has entered a "new era of [Foreign Corrupt Practices Act ("FCPA")] enforcement," with several high-profile cases and record breaking penalties in 2010.[7] In fact, the number of enforcement actions brought under the FCPA in 2010 amounts to an 85 percent increase over 2009 FCPA cases.[8] In addition, the DOJ has begun targeting hedge funds and so-called expert networks with insider-trading allegations, often with cooperation from the SEC and other federal and state agencies, as illustrated by the recent *Galleon* case.[9] The DOJ has also assisted with unprecedented recoveries under the False Claims Act, which authorizes the DOJ to reward whistleblowers who reveal fraud committed against the U.S. In 2010, the federal government secured more than $3 billion in civil settlements and judgments under this Act, up 25 percent from the prior year and the second-largest yearly amount ever.[10] Criminal health care fraud investigations are receiving significant attention under the False Claims Act, with 1,116 new investigations in this sector in 2010, for a total of 1,787 criminal health care fraud investigations pending.[11]

The SEC and the DOJ are not the only enforcement arms of the federal government endeavoring to flex their enforcement muscle. The Office of Criminal Investigations of the Food and Drug Administration ("FDA") has publicly declared an intention to increase prosecutions of pharmaceutical and food industry executives. One such tactic is highly controversial — using a strict liability provision of the Food, Drug and Cosmetic Act.[12] This provision permits criminal convictions against executives that neither participated in nor knew of a violation, but whose position put them in a responsible relation to it. This provision has historically been used sparingly; however, the FDA has now publicly stated its intention to "increase the appropriate use of misdemeanor prosecutions."[13] Even though characterized as a "misdemeanor", sanctions can be severe: up to one year in prison for each count on which there is a conviction, as well as a fine of $100,000 or more.[14] The FDA has also teamed up with the DOJ on a cooperative basis to pursue criminal felony convictions of pharmaceutical executives on fraud charges related to marketing materials and obstruction of justice in connection with FDA investigations. One such investigation and prosecution, recently dismissed by a federal judge, was waged against an associate general counsel.[15]

State agencies have also been more inclined to scrutinize business practices. According to William Haraf, head of California's Department of Financial Institutions, Dodd-Frank will encourage additional enforcement actions by both state oversight agencies and state attorneys general.[16] Other initiatives, such as President Obama's collaborative federal and state Financial Fraud Enforcement Task Force, will no doubt foster such state-level action.

Cooperation between civil and criminal enforcement agencies has also become more common. On the federal level, Attorney General Eric Holder has underscored the importance of using "a full range of parallel criminal and civil enforcement resources to combat financial fraud."[17] Further, "the criminalization of securities enforcement and the blurring of the line between criminal and civil cases appears [sic] to be accelerating."[18] In a 2007 case, for instance, Chevron simultaneously settled civil and criminal FCPA-related issues with the U.S. Attorney for the Southern District of New York, the SEC, an office of the Treasury, and the Manhattan District Attorney.[19]

Other recent trends in enforcement include a broadening of investigative techniques used by government agents. Ambush interviews, search warrants and wiretaps are now employed against corporations and their officers suspected of violations of state or federal law. For the first time, moreover, the SEC has begun to enter into deferred and non-prosecution agreements with individuals who assist investigations. The SEC has also amended its rules to make orders of immunity from the DOJ (and thus the cooperation of otherwise liable parties) easier to obtain.[20]

Preparing for the Unexpected Visit

So, what do you tell the receptionist? Wouldn't it be reassuring if you could remind her that she has been trained for this contingency and that she should contact your designated company representative, a person charged with following a predetermined procedure? In this version of events, you've already taken the first steps toward keeping employees calm, business operations orderly, risk of liability and loss low, and interactions with authorities respectful. Alternatively, if you haven't prepared for this unexpected visit, you'll be forced to improvise, greatly increasing the chances of erroneous disclosure, property seizure, business disruption, reputational damage, and—where investigators find wrongdoing—liability, penalties and indictment.

Fortunately, businesses can take a few relatively simple steps to prepare for an unannounced visit from the government. These include: (1) understanding how to handle an ambush interview, (2) designating point persons and training appropriate personnel, and (3) developing a written "door knock" plan. The balance of this article discusses each of these measures in turn.

Understanding and Handling an Ambush Interview

Agents are trained to use the element of surprise in connection with witness interviews. It is not uncommon for agents to arrive unannounced at homes and offices (early in the day or in the late evening) asking questions designed to further their investigations. Sometimes the questions seek background information, but often the questions seek to solicit information that could be used against the interests of the target of the investigation. This type of questioning is known as an "ambush interview." The tactic provides no opportunity for preparation by prospective interviewees. To make matters worse, legal counsel is generally not present. Agents often appear cordial and curious initially rather than confrontational or hostile. They may politely disarm those whom they wish to interview, partly coaxing and partly intimidating individuals into talking. Often, unprepared employees readily submit to interview requests on the spot, desiring to be helpful or believing that by talking, they will convince the agents that everything is fine. They may also fear that if they decline an interview, they will seem uncooperative or evasive.

However, the law does not require individuals to submit to questioning under such circumstances. Indeed, neither search warrants nor subpoenas can compel an interview. Promises by agents of "off the record" interviews or suggestions of leniency are illusory. Quite simply, no benefit accrues to submitting to an ambush interview, only downside.

Preparation is critical for providing truthful, thoughtful, and complete information to agents. While it is unlawful to lie to or mislead government officers,[21] there is no need for an interviewee to pass along mere speculation or baseless rumors during questioning. Yet an ambush interview makes such offhand, unwitting over-disclosure more likely. Advance preparation, in contrast, shifts some control over the interviews back to the company and the interviewee, neutralizing the government's element of surprise.

Remember: a prudent person would never enter an important meeting or presentation without some preparation. A government interview should not be treated differently, no matter how informal it appears. Unprepared employees are much more likely to offer implausible or speculative explanations based on intimidation, surprise, panic, or discomfort. Damage from such missteps can result in the communication of erroneous, materially misleading, or inadvertent omissions and admissions, as well as the unintended waiver of confidential attorney-client privileged information.

Designating Point Persons and Training Personnel

Companies can best manage the risks posed by ambush interviews by designating a few trusted employees at each office location to serve as point

persons if agents arrive. Teaching these individuals how to respond to a visit from the government can be as routine and uneventful as a fire drill if presented in a matter-of-fact manner. Importantly, point persons should understand that government inquiries are now a reality for many lawfully-run businesses — and probably as likely as any natural disaster for which training is commonplace.

Businesses should appoint a minimum of two employees (a primary and a secondary) at each office, so at least one will be always be available during operating hours. These persons should be employed at the manager level or above, since this role requires professionalism, judgment, and leadership. The primary duties of point persons include: (1) acting as the sole representative of the company until legal counsel or senior management arrives,[22] and (2) following an appropriate, pre-determined "door-knock" plan, as described below.

In addition, companies should provide some basic instruction to most other employees. Receptionists and others must be advised to refer agents to the company's designated point person. If solicited for an interview, an employee should know of his or her right to decline politely and request that a meeting be coordinated through the company's designee. The point person (or legal counsel) can work with agents to schedule any interview for a convenient time and place. If an agent grows hostile or insistent upon an immediate interview, the point person should immediately contact the company's legal counsel, assuming counsel has not been alerted already. Counsel can speak to the agents either in person or over the telephone to diffuse the situation.

Developing a "Door Knock" Plan

Once agents arrive, the designated point person must quickly determine whether the agents possess a search warrant (for searches conducted pursuant to a criminal investigation) or a civil order signed by a judge (for non-criminal searches). These are the *only* documents that secure the government's right to enter and search your premises. Different procedures should be followed depending on the presence or absence of these documents.[23]

"Door Knock" Plan 1: Responding to a Warrantless or Order-less Visit

Government officers sometimes arrive at a business or home without a warrant or court order. In these cases, the agents may attempt to serve a subpoena or they may simply have questions.

If an agent appears in the lobby to serve a subpoena, the receptionist should alert the designated point person for service of process. The point person should simply accept the subpoena, ask for business cards from the agents and notify the agents that the company's counsel will be in touch with either the lead agent or the attorney issuing the subpoena. While a subpoena requires a response, the date for such response is typically several weeks away and no immediate action is required. Documents and information responsive to the subpoena should not be collected at the time of service or in the presence of the agents. Do not evade service of the subpoena. Evading service does little more than irritate the agents and cast suspicion on the evader and/or company. Once the subpoena has been delivered, the designated point person should courteously ask the agents to leave the premises. At this point, having informed the agents that the company will communicate only through counsel, the designated employee should cease all discussion with the agents. The point person should then immediately contact legal counsel.

Agents may also arrive at a business without a subpoena, and instead simply state that they would like to be invited in so they can ask a few questions. The agents may ask for individuals by name, title, or job description. Sometimes agents simply request to speak to someone knowledgeable about the industry. They may also ask to view documents or records pertaining to operations, inventory, or other matters. In these instances, the receptionist (or whomever the agents first solicit) should imme-

diately alert one of the point persons designated by the company for this contingency. The receptionist, or the point person, should then contact the company's legal counsel. The point person should escort the agents to a conference room or private office and obtain an understanding of what the agents are seeking. Of course, all interactions should be respectful and polite. If confronted with an interview request or a series of questions, the designated employee should politely decline and respectfully ask that all interviews and other requests be coordinated through the company's counsel. The point person should stress that the company will cooperate fully, but with the assistance of counsel, whose name may be provided. The designated employee should collect business cards, record the contact information of each agent, and represent that the company's legal counsel will contact the agents shortly.

Once the agents have left the company's premises, legal counsel should consider whether to distribute an "information and advice of rights" memorandum to employees who may be approached by agents when not on the company's property. It is not uncommon for agents to appear unannounced at the homes of employees of all levels seeking information either before or after appearing at their place of business. Accordingly, advising employees of their rights and the company's suggestion that interviews be coordinated through counsel is a critical next step. Otherwise, ambush interview tactics thwarted at the office can simply be deployed at the homes of unsuspecting employees. Of course, if the agents identify specific employees while at the office, counsel should notify those individuals promptly.

If the company has multiple offices in regions across the country or the world, careful consideration should be given which offices should be notified and how deeply in to the employee pool communications should be distributed. If the decision is made to inform multiple offices, designate an employee, preferably within the in-house counsel staff, as the point person to coordinate communications and questions from regional management and employees.

If the decision is made to notify a group of employees, counsel should consider informing the company's employees of the following:

1. Government agents are currently conducting an investigation or inquiry.
2. The company intends to cooperate fully.
3. The government may contact employees while at work or at home.
4. The company encourages employees to coordinate with company counsel prior to any interview.
5. The company intends to preserve all its privileges, so employees may not discuss privileged matters with the government, and any questions regarding whether information is privileged should be directed to company counsel.
6. False statements to the government carry criminal penalties, so any responses provided during an interview must be truthful and complete.

Notably, such a memorandum can be substantially prepared in advance and distributed immediately after agents visit. The obvious benefits of circulating such a memorandum include: mitigating the pressure employees may feel to submit to interviews, alerting employees of their rights, and encouraging all interviews to be coordinated through counsel. However, a company must take care not to overreach in an effort to control the investigation. For example, companies should not direct employees to refuse to cooperate with government agents. Instructing employees that they may not, under any circumstances, communicate with the government could be perceived or interpreted as obstruction of justice, which is a crime.[24]

When companies have more than a few employees who could be subject to an interview, careful consideration should be given to broad offers to pro-

vide legal counsel to each person the government contacts. There are practical issues to consider, such as cost, coordination and insurance coverage; legal issues to consider, such as conflicts, indemnification rights and obligations; and strategic issues, such as the level and business importance of the employee, and optics to the government.

"Door Knock" Plan 2: Responding to a Search Warrant or Civil Court Order

Additional procedures and protections are necessary when agents arrive with a warrant or civil court order authorizing a search and/or seizure. As noted, a properly executed and valid search warrant or civil court order are the *only* means by which government agents may search a company's premises and seize its property. Thus, designated employees must be trained to decline searches and seizures absent a warrant or civil court order. Further, any person claiming to be an agent with a warrant or civil court order should be asked to produce official identification and provide a copy of the warrant or civil court order.

Again, the receptionist (or whomever the agents first solicit) should notify the company's designated employee immediately after learning that agents have arrived on the property. The point person should next contact legal counsel who can then contact appropriate outside counsel.

Importantly, agents do not have to wait for counsel's presence to execute a warrant or civil order. Consequently, designated employees must be trained to manage a government search until counsel arrives. This means that point persons must be familiar with a number of additional procedures and protections.

First, designated employees must understand that the company has the right to review a warrant and retain a copy of the warrant. If the affidavit in support of the warrant is not attached, the designated employee should ask for a copy. The same is true for any civil complaint, application, motion or related order. Affidavits or other evidence are frequently filed under seal and may be unavailable, but a copy should be requested nonetheless. Further, all warrants must specifically identify the place to be searched and generally set forth time limits for a search (e.g., a warrant may specify that it is for daytime searches only). Finally, all warrants have an expiration date.

Accordingly, in the absence of legal counsel, a designated employee must read a warrant or civil order carefully to ensure that it grants the authority to search a company's premises. While it is a crime to obstruct an agent in the lawful exercise of his or her duties,[25] asking questions and requesting a copy of the warrant do not rise to the level of obstruction. Indeed, failure to confirm the legitimacy and scope of a warrant needlessly places a company at risk.

Second, designated point-persons should observe the course of a search, but no one may interfere with its progress. Indeed, the point person should ensure that nearby employees are expressly instructed not to stall the agents, interfere with their search, or otherwise impede the performance of their duties. Office traffic around the agents should be minimized. This benefits the company as well as the agents, since all conversations between agents and employees will be documented and possibly used by the government at a later date. If multiple agents are required to conduct the search at several locations within a facility, the point person should ask the agents not to conduct their search without a designated employee accompanying them throughout the property.

Third, if not already evident, the designated employee should inquire with the lead agent whether the government has any personal search warrants for any employees. If so, the point person should note the identities of such employees. However, the point person should be advised that subjects of personal warrants need only assist agents in locating items specified in the applicable warrant. Such subjects do not have to submit to questioning. Employees who are not subject to personal search

warrants may leave the premises at any time. In the event that a search warrant covers the entire office space, non-essential employees in the location subject of the search can simply be dismissed for the day.

Fourth, the point person should take detailed notes concerning any confiscated property, including any unique identification numbers and the condition and location of seized items. Although all federal and state agents must leave an inventory of confiscated items, these government-produced inventories generally only summarize taken property. For example, an inventory list may simply state "file" or "computer." Thus, every effort should be made to generate a more detailed and comprehensive list.

Fifth, the designated employee should be aware that warrants regularly authorize the seizure of electronic information. This could include entire computers, laptops, computer disks, hard drives, storage devices, mobile phones, and other electronic devices — all of which may contain substantial amounts of information outside the scope of the warrant. If possible, therefore, the point person should review the warrant closely to hold agents to as strict an interpretation as possible. The point person may be able to work with the agent in charge to avoid wholesale confiscation, as opposed to copying, of electronic information. If agents attempt to take items critical to the company's operations, point persons should attempt to negotiate a compromise that will not cripple the company's business.

Sixth, when drafting a "door-knock" plan, a company should also consider whether a point person should be directed or permitted to send a communication to all company employees while a search is ongoing. Such a statement would disclose to employees that the company is cooperating with the investigation and would direct employees not to interfere with the agents' activities, communicate unnecessarily with the agents, or enter areas where the agents are working. By acknowledging the existence of a search and providing general instructions to employees, a company can minimize gossip and anxiety. However, any communication to employees should probably be limited in scope. At this stage, a company will know too little to justify any company-wide messages about the nature, purpose, or consequences of the search.

Finally, because counsel may not be present from the beginning of an unexpected search, a point person must also understand the basic principles of attorney-client privilege. For example, if a warrant calls for the seizure of electronic information that may contain attorney-client communications (such as an executive's correspondence with counsel or draft contracts), then the company must assert its privilege as soon as possible to reduce the risk of unintentionally waiving the privilege.

At a minimum, the point person must know where and how the company stores potentially privileged material. The designated employee should then be able to explain why a particular computer, for instance, may contain privileged information. This in turn should enable the point person to seek segregation of the material. Notably, once a point person makes an assertion of privilege, agents should not be permitted to review the content of the communications in question. If the agents maintain that the warrant encompasses such information, then the point person should request that the device containing such information be separated and sealed until a privilege determination can be made at a later time.

Whenever a dispute over privilege arises, it will be necessary to reach an agreement with the agent or government attorney in charge of executing the warrant. If a reasonable agreement cannot be reached, the company may be required to obtain an immediate audience with the judge who issued the warrant to resolve the issues of scope and privilege protection. In the meantime, the items in question must remain segregated.

Once agents have completed their search of the premises and departed, a number of steps should be taken, as enumerated below.

1. The company's counsel should consider distributing an "information and advice of rights" memorandum, as discussed in connection with the first "door knock" plan above.
2. The company's counsel should interview each person with whom the agents interacted, marking all interview notes as work product and privileged. These interviews should focus on debriefing the persons involved and gathering information about what employees may have overheard the agents discussing and what the agents appeared most interested in obtaining.
3. Based on the point person's notes, the company should create a thorough and descriptive index of all property seized in connection with the search, including each item's condition and location. This list should be marked as work product for legal counsel.
4. For public companies, consideration should be given as to whether public disclosure of the search is required under applicable securities regulations. If disclosure is required, or advisable, then such disclosure should be limited to a concise statement of facts that is free from speculation. The disclosure should note that the company is cooperating with the investigation.
5. Counsel should consider whether notice of the incident or other action is required under any contract, such as a lender agreement, or any other statute or regulation, depending on the industry.
6. Senior management and the board should be advised of the day's events in detail. Legal counsel must be present at this meeting and included in correspondence to preserve privilege and work product protections.
7. The company should consider contacting crisis-management and/or public relations consultants regarding appropriate strategic initiatives to mitigate perceived damage to business relationships and customer impressions.
8. The company should review applicable insurance policies to determine whether these policies provide coverage for search-related costs and possible related future expenses.
9. The company should meet with experienced outside counsel to manage the process as it unfolds, particularly with respect to conducting an internal investigation and minimizing civil and criminal liability.
10. If specific individuals appear to be targeted or implicated, the company should review its indemnification obligations, which may be found in several locations, such as within applicable bylaws, state-of-incorporation requirements, and employment and indemnification agreements.

Make a Plan Now

Every prudent business plans for disasters, both natural and otherwise. Companies almost universally prepare for the possibility of flood, fire, terrorism, earthquake, tornado, hurricane, and other catastrophe through insurance and advance planning. In many cases, an ounce of preparation averts a pound of misfortune. The same applies to unexpected visits by the government.

As discussed above, companies can greatly reduce the risks associated with a surprise government investigation by taking three simple steps: (1) understanding ambush interviews and how to handle them, (2) designating and training personnel to respond to unannounced government visits, and (3) developing a written set of "door knock" proce-

dures for the various scenarios under which government agents may arrive at a business.

The bottom line is that when the receptionist calls with news of agents in the lobby, turning your car around, racing home and hiding under your bed is not an option. After all, the government knows where you live. Planning and preparing is truly your best option.

John F. Cannon is a shareholder at Stradling Yocca Carlson & Rauth and is the Chair of the firm's securities litigation practice. Mr. Cannon has more than twenty years experience representing publicly traded and other regulated companies, hedge funds, investment advisors, banks and broker dealers in connection with enforcement matters before the SEC, FINRA, the FCC, the FDA, the FTC, state regulatory agencies and the civil and criminal divisions of the DOJ. Mr. Cannon also has extensive experience defending securities class actions, shareholder derivative actions, merger and acquisition litigation and conducting internal investigations.

Kathleen M. Marcus is a shareholder at Stradling Yocca Carlson & Rauth, with a practice emphasizing government investigations and compliance counseling. Ms. Marcus manages investigations before the SEC, FINRA, the FCC, the FDA and the DOJ, including qui tam suits. Additionally, Ms. Marcus assists companies by conducting internal investigations and provides counseling on corporate governance and compliance issues. Previously, Ms. Marcus served as Senior Counsel in the Division of Enforcement of the SEC in Washington D.C. She also taught classes concerning SEC Enforcement at the University of Notre Dame Law School and the University of Toledo College of Law.

---

1 Damian Paletta & Aaron Lucchetti, Law Remakes U.S. Financial Landscape, WALL ST. J., July 16, 2010.

2 Congress Misfires on Financial Overhaul: Further Tightening of Credit Expected, FREE ENTERPRISE (Sept. 2010).

3 U.S. CHAMBER OF COMMERCE (last visited Apr. 24, 2011).

4 Sewell Chan & Louise Story, Goldman Pays $550 Million to Settle Fraud Case, N.Y. TIMES, July 15, 2010.

5 Year-by-Year SEC Enforcement Statistics, U.S. Sec. & Exch. Comm'n Newsroom, Office of Pub. Affairs.

6 U.S. Sec. & Exch. Comm'n. FY 2010 Performance and Accountability Report (2010).

7 Lanny Breuer, U.S. Assistant Attorney General, Dep't of Justice Criminal Div., Address at the 24th National Conference on the Foreign Corrupt Practices Act (Nov. 16, 2010).

8 *See* Melissa Aguilar, *2010 FCPA Enforcement Shatters Records, Compliance Week,* January 4, 2011.

9 Press Release, U.S. Attorney S. Dist. of N.Y., Hedge fund billionaire Raj Rajaratnam found guilty in Manhattan federal court of insider trading charges (May 11, 2011).

10 Fraud Statistics: Overview, U.S. Dept. of Justice, Civil Documents & Forms (under "False Claims Act Statistics").

11 Melissa Aguilar, *2010 FCPA Enforcement Shatters Records, Compliance Week*, January 4, 2011.

12 *See* 21 U.S.C. § 331.

13 Letter from Margaret A. Hamburg, Commissioner of Food and Drugs, to Sen. Charles E Grassley (March 4, 2010).

14 *See* 21 U.S.C. § 333 ("shall be imprisoned for not more than one year") and 18 U.S.C. § 3571 (which supersedes the FCDA and authorizes fines of $100,000 for a Class A misdemeanor).

15 *United States v. Stevens*, No. RWT 10cr06942011, 2011 BL 88102 (D. Md. Mar. 23, 2011).

16 William S. Haraf, Commissioner, Dep't of Fin. Inst., Statement at Joint Informational Hearing on the Dodd-Frank Wall Street Reform and Consumer Protection Act: Initial Reactions, Initial Steps and Likely Impacts (Mar. 23, 2011).

17 Eric Holder, U.S. Attorney General, Dep't of Justice, Address at the Western Regional Financial Fraud Enforcement Task Force Summit (Dec. 10, 2010).

18 Thomas O. Gorman, SEC Trends 2011: Close Cooperation, SEC ACTIONS (Jan. 28, 2011).

19 United States v. Chevron Corp., Case No. 07-cv-10299 (S.D.N.Y. Filed Nov. 14, 2007).

20 Peter J. Henning, Post-Madoff, S.E.C. Rethinks Enforcement, N.Y. TIMES, Jan. 14, 2010.

21 18 U.S.C. § 1001 (2010).

22 If feasible, the role of point person may be best filled by a member of senior management or the company's in-house counsel. However, this article assumes that at least in some cases such individuals will not be availa-

ble to assume the duties of point person on a day-to-day basis.

23 Unless otherwise indicated, this article refers to both search warrants and civil orders as "warrants."

24 18 U.S.C. §§ 1501-1520 (2010).

25 *Id*.