DO'S AND DON'TS ALL COUNSEL SHOULD KNOW ABOUT GOVERNMENT INVESTIGATIONS

Written & Presented by:
KIT ADDLEMAN, *Dallas*
Haynes and Boone

BARRETT HOWELL, *Dallas*
Bracewell LLP

Co-Written by:
RYAN MEYER
Bracewell LLP

State Bar of Texas
14th ANNUAL
ADVANCED BUSINESS LAW COURSE
November 17-18, 2016
Dallas

CHAPTER 16

TABLE OF CONTENTS

DO'S AND DON'TS ALL COUNSEL SHOULD KNOW ABOUT GOVERNMENT INVESTIGATIONS

By Barrett Howell, Kit Addleman, and Ryan Meyer

I. GOVERNMENT SUBPOENAS - INTRODUCTION

The receipt of a government subpoena can be an unsettling experience. But failing to properly respond to a government subpoena can be far worse not only for the company, but also the individuals involved in preparing the response. This article discusses initial steps and considerations when a company receives a government subpoena.

II. YOU JUST RECEIVED A GOVERNMENT SUBPOENA. NOW WHAT?

Who issued it? There are more than 300 federal agencies alone with administrative subpoena power. Congress has statutorily authorized these agencies to subpoena the production of documents, witness testimony, or both, without court review or approval. As soon as you receive a subpoena, you therefore first need to determine which agency issued it. The identity of the issuing agency will be clearly stated at the top of the subpoena, generally under the words, "UNITED STATES OF AMERICA."

In addition, it is important to note the each state has numerous agencies with administrative subpoena power. At the state level, it is not uncommon for these agencies to have combined civil and criminal authority. For instance, the Texas State Securities Board, which generally regulates the securities industry and securities offerings in Texas in the same space as the Securities and Exchange Commission ("SEC") on a national basis, possesses both criminal and civil authority whereas the SEC is only civil. These state agencies can, and sometimes do, cooperate with federal investigations and share documents received using their subpoena power, but they can also operate independently. Further, a civil agency such as the SEC may also cooperate and share information with other agencies, including criminal authorities. As a result, it is not uncommon for a company to deal with multiple subpoenas issued by federal and state investigative agencies operating on parallel tracks.

What do they want? The subpoena will require the production of documents and/or testimony. Most subpoenas contain a section just under the recipient's name that states "YOU MUST PRODUCE" and a section that states "YOU MUST TESTIFY." Either one or both of these sections will contain an "X," indicating what is required and will also set forth the date on which compliance is required.

While it may seem simple, it is important to note the difference between a subpoena *duces tecum* and a subpoena *ad testificandum*. Only in the latter case is someone's testimony actually being compelled. A subpoena *duces tecum* can only compel the recipient to produce documents. Even though a federal grand jury subpoena duces tecum (for instance) may state on its face that the entity or individual to which the subpoena is directed must appear before the grand jury at "X" date regarding "Y" subjects, the subpoena is actually only seeking the production of documents.

How much do they want? Most document subpoenas contain two attachments, the first provides instructions and definitions, and the second contains the actual document requests. By analyzing the attachments and the breadth of the materials being requested, you can typically determine the subject matter, relevant time period, and overall focus of the subpoena and the investigation. You should also start thinking about the likelihood of timely compliance with the subpoena deadline. If there are numerous document requests covering a variety of transactions over a multi-year period, it may not be possible to identify, collect, review, and produce the volume of responsive documents and information within the time required by the subpoena.

Should you call the government lawyer who issued the subpoena? Once you have an idea of the subpoena's subject matter, it is generally worth calling the government lawyer or agent whose name is listed on the subpoena. Of course, the most important question is whether your company is a target of the investigation or a third-party witness. While it never hurts to ask, the government is often unwilling to divulge this information during its investigative process, so it is generally safest to assume your company is or may become a potential target at some point during the investigation. At this stage, to the extent the government lawyer is willing to divulge any information regarding the investigation, it is likely to be only that your company is neither a witness nor a target, but a "subject" until the investigation develops further.

In some investigations, you may be able to ask the government lawyer for the document authorizing the investigation. At the SEC, for example, you can request and receive a copy of the formal order of investigation upon making certain representations regarding the confidentiality of the document.

In addition to initial fact gathering, the preliminary call provides an opportunity to establish a good rapport with the government lawyer and to express the company's desire to comply to the best of its ability with the subpoena. Proper handling of the initial contact is critical, especially when the potential for criminal charges exists.

When and how should you try to narrow the initial scope of the subpoena? The government's initial document requests are often very broad in both time and scope. If there is a legitimate concern with the company's ability to timely comply with the subpoena, this should be mentioned during the initial call with the government lawyer. Most government subpoenas initially contain a short production deadline (for instance, the SEC's subpoenas generally seek production of documents within fourteen (14) days), so it is not unusual for agencies to grant an extension on the initial deadline. It may also be helpful to explain the types of documents and materials generated and maintained by the company, especially if the government will need specialized software to properly view the responsive documents or information (such as industry-specific file types or natively-produced accounting files). If the amount of material called for by the subpoena is extensive and the time necessary to collect and produce it will be lengthy, the company may want to offer to produce documents on a rolling basis, rather than reviewing and producing the entire universe of responsive documents in a single massive and delayed delivery. Making an initial production of quickly-accessible documents can help the company build trust and rapport with the investigating attorney and can help divide the task of document collection into more easily managed pieces.

Depending on the circumstances, the government may be willing to narrow the scope of the company's initial rolling production. The government's goal is to gather information relevant to its investigation as efficiently as possible. In most matters, the government welcomes input that furthers this goal and avoids document dumps of materials that are not particularly relevant to the investigation, although they may be responsive to the subpoena's initial scope.

III. YOU'VE DETERMINED THE SOURCE AND SCOPE OF THE SUBPOENA. NOW WHAT?

There are certain steps that should be taken and certain pitfalls that should be avoided whenever a company receives a government subpoena:

DO IMMEDIATELY SUSPEND ROUTINE DOCUMENT DESTRUCTION AND AUTOMATIC DATA DELETION PROCEDURES.

Once you have determined the source and scope of the subpoena, the next critical step is preserving potentially responsive documents and electronic information. Preservation is critical because the destruction of relevant information may be perceived by the government as lack of cooperation, or, in the worst case, obstruction of the government's investigation. The company should therefore promptly suspend any routine document destruction or automatic data (particularly email) deletion procedures. Although a subpoena will typically trigger the obligation to suspend document destruction, there are times when procedures should be suspended prior to receipt of the subpoena. Notice of a future investigation or internal whistleblowing are some examples of such situations.

Internal whistleblowing has become significantly more important, and more frequent, over the last several years. As part of the Dodd-Frank Act, the SEC established its Office of the Whistleblower to act as a clearing house for whistleblower complaints in the securities industry.[1] These whistleblowers can now be treated like *qui tam relators* in successful SEC actions over $1,000,000 as the law entitles them to be paid ten to thirty percent of the SEC's recovery. Dodd-Frank also allows the SEC to penalize companies for retaliating against whistleblowers, even in the absence of an enforcement action. For instance, the SEC recently fined a company $500,000 for terminating an employee who had, it was later determined, mistakenly claimed that the company's financial statements were misstated. Though the company's own investigation found no wrongdoing, and the SEC closed its investigation without pursuing an enforcement action related to reportedly misstated financial statements, the SEC still assessed the company with a $500,000 penalty for wrongfully terminating the employee-whistleblower.[2]

In some cases, it might be necessary to suspend routine destruction and automatic deletion procedures for the entire organization. In other cases, however, company-wide suspension may not be necessary based on the scope of the subpoena. You may need to identify individuals with potentially relevant information (i.e. "custodians") and, at a minimum, suspend routine destruction and deletion procedures with respect to their documents and electronic data.

DO CONSIDER WHETHER TO CAPTURE DATA FROM PHONES AND OTHER DEVICES.

The company should consider whether it needs to capture forensic images of any company computer hard drives, phones or other electronic devices. Depending on the size of the company, it would be best to already have in place procedures addressing the need to obtain information from an employee's electronic storage. For example, every company should have a policy that addresses any devices that are owned by the employee but may contain company information such as where a company utilizes a "bring your own device" practice. Additionally, such procedures may include a tracking system for the company's computers so that devices repurposed from one employee to another can be tracked over time and retrieved if necessary. Depending on the company's industry – such as covered entities and business associates under the Health Insurance Portability and Accountability Act

("HIPAA") – a required tracking system may already be in place. Do not assume that just because a device previously used by a potentially relevant custodian has been "wiped" by the company's IT that all (or even most) information related to that custodian has actually been removed.

DO CONSIDER WHETHER PRIOR OR DEPARTING EMPLOYEES MAY HAVE RESPONSIVE INFORMATION.

If an employee with potentially relevant information leaves the company during the pendency of an investigation or while the company is responding to a government subpoena, at a minimum any company-issued computer or electronic device used by that individual should be forensically imaged before it is redeployed. If the company's resources allow for it, it is best for this image (or images) to be performed by an outside forensic IT consultant to maintain a chain of custody and avoid subjecting the company's personnel to additional discovery.

DO TALK TO THE GOVERNMENT BEFORE DISTRIBUTING PRESERVATION NOTICES.

Distributing preservation notices to employees might seem like a logical step in complying with the company's preservation obligation. Before sending such a notice, however, you should discuss potential confidentiality concerns with the government. For instance, if the investigation involves suspected insider trading, the government may want to avoid putting the target on notice of the investigation by sending a detailed preservation notice.

To the extent it is appropriate, the preservation notice should inform the appropriate employees of their preservation obligations and prohibit them from deleting or modifying any potentially relevant information. The preservation notice should also instruct employees as to how potentially relevant information will be collected. The preservation notice should not go into detail about the investigation (or litigation) or the company's role in the matter. It is generally best practice to avoid mentioning the specific facts leading to its issuance and instead simply instruct the employees on their obligations and duties.

DO CONSIDER CONDUCTING AN INTERNAL INVESTIGATION.

Responding to a government subpoena generally requires some level of internal investigation. The investigation may be limited to simply identifying, preserving, and collecting documents responsive to the government's subpoena, or the company may need a more in depth assessment of its potential risk exposure. Determining the appropriate magnitude of an internal investigation can be complicated by the fact that the government rarely divulges whether the company is a potential target or third-party witness. Of course, even when a company begins the investigative process as third-party witness, it does not guarantee that the company or its senior officials will not subsequently become a targets.

An internal investigation assists the company in analyzing the potential criminal or civil liability for the entity and its officers and employees. Perhaps even more importantly, an internal investigation may provide the company an opportunity to: 1) stop any ongoing violations or improper conduct and take action to discipline or terminate any wrongdoers; and 2) implement remedial measures that could potentially mitigate liability exposure and prevent the underlying circumstances from arising again in the future. If a company effectively investigates its own misconduct, it may stand a better chance of convincing the government to forego conducting its own investigation, reduce the scope of its investigation, or allow the company to be more involved in its investigation. In addition, if the government's investigative findings resemble the company's investigative findings, then the government may agree to a lesser sanction or perhaps even no sanction at all.

Determining when an internal investigation should be conducted by in-house counsel versus outside counsel will vary by situation. Two significant factors that assist in determining whether independent outside counsel is required include:

- The seriousness of the alleged conduct and the possible risk exposure;
- The seniority and positions of any individuals who may have been involved in the conduct under investigation; and
- The connection between the investigating lawyer and witnesses. Assess whether the potential witnesses include people the investigating counsel regularly interacts with, reports to, or include someone who might otherwise have even a perceived influence on the independence of the investigation. The possibility of a close relationship between lawyer and witness is particularly important in light of the Yates Memorandum's (the "Yates Memo") increased focus on investigating and prosecuting individuals.[3]

IV. YOU'VE DECIDED TO CONDUCT AN INTERNAL INVESTIGATION. NOW WHAT?

Regardless of who conducts the investigation, there are certain steps that should be taken and certain pitfalls that should be avoided whenever a company conducts an internal investigation:

DO NOT HOLD GROUP MEETINGS WITH POTENTIAL WITNESSES.

Although more time-consuming, counsel should separately interview each individual with potentially relevant knowledge. In any other situation, the most efficient means of gathering information would be through a collaborative meeting of all the relevant individuals. However, in the context of a government investigation such a meeting tends to be viewed through a dubious lens. Not only might the government perceive this meeting as a "get your story straight" session, but it might also "taint" possible witnesses by compromising their first-hand knowledge of relevant facts and information. This is a particularly serious concern where the company is investigating the potential misconduct of a group of employees as such group meetings can give *those* employees the opportunity to get their story "straight" in an arguably privileged context.

DO PROVIDE *UPJOHN* OR CORPORATE *MIRANDA* WARNINGS TO WITNESSES.

At the beginning of each employee-witness interview, counsel should clearly explain the attorney-client relationship and how the privilege applies. Specifically, counsel needs to explain that he or she represents the company, not the individual employee, and therefore the privilege belongs to the company and only the company can raise or waive privilege protections. Counsel should also make a record of giving this warning; indeed some counsel require witnesses to sign an acknowledgement of receipt of the warning. Generally, a written record by counsel will suffice as there is usually no need to record these types of meetings.

While this warning is an awkward and stilted way to start any interview, it is absolutely essential. Under the Supreme Court's holding in *Upjohn*, this explanation is a necessary step in rebutting potential claims by the employee that an attorney-client relationship existed between the employee and the company's lawyer.[4] If the employee is able to demonstrate a reasonable belief that the lawyer was representing the employee individually, then the employee may be able to suppress statements the employee made to counsel during the interview on the basis of a putative attorney-client privilege.

DO CONSIDER ANY MANDATORY REPORTING DEADLINES IMPLICATED BY THE TYPE OF ALLEGED MISCONDUCT.

As discussed below, it can be a good idea in certain circumstances for a company to self-disclose or self-report the findings of an internal investigation. However, for some conduct, such reporting is *mandatory* with severe penalties for those companies that fail to comply. In recent years, this mandatory reporting has most often occurred in the data security field where both federal and state laws require prompt reporting to affected individuals and appropriate government agencies. It is important to quickly understand the appropriate statutes and their required deadlines as that can affect the type and intensity of any investigation. For instance, HIPAA generally requires a company to notify affected individuals of any breach of their protected health information or personally identifiable information within thirty (30) days of learning of a breach.

DO CONSIDER POTENTIAL VOLUNTARILY SELF-REPORTING POTENTIAL MISCONDUCT OR ADVERSE FINDINGS.

If during the course of the investigation the company uncovers misconduct, the company may consider making a voluntary disclosure to the government, or "self-reporting." If misconduct has occurred, self-reporting and voluntary cooperation may help persuade the government that indictment is unnecessary. Voluntary cooperate cooperation has become particularly important in light of two new Department of Justice ("DOJ") initiatives: (i) the Yates Memo and (ii) the DOJ's Foreign Corrupt Practices Act (the "FCPA") Pilot Program (the "Pilot Program").

Prior to September 2015, corporations could receive "cooperation credit" simply by demonstrating their willingness to cooperate in the government's investigation. However, since the publication of the Yates Memo, DOJ has now taken the position that companies *will not* receive cooperation credit unless and until they provide information on all individuals responsible for the conduct. The Yates Memo goes on to emphasize that individuals must be the focus of investigation from the start, not just at the end as the case winds down, and that individuals are not to be released in settlement agreements just because the company itself settles the case. As a practical matter, there does not appear to have been a sustained increase in individual prosecutions yet, but that could change moving forward.

Similarly, in April 2016, the DOJ announced its new Pilot Program focused on possible violations of the FCPA.[5] The Pilot Program is restricted only to cases brought by the DOJ's Criminal Fraud Section through April 2017. Under its provisions, the Pilot Program provides *additional* credit to companies that voluntary disclose FCPA violations while simultaneously *withholding* full cooperation credit from those companies that only disclose violations after the government launches its investigation. As a practical matter, the Pilot Program allows a cooperating company to receive up to a fifty (50) percent reduction under the low end of the applicable sentencing guideline *and* avoid the imposition of a corporate monitor.

DO NOT WITHHOLD NON-PRIVILEGED MATERIALS SIMPLY BECAUSE THEY APPEAR UNFAVORABLE.

Bad documents are a fact of life—every company has them but they do not automatically implicate liability. When the investigation uncovers unfavorable documents responsive to the government's request, the worst thing to do is anything that could be viewed as covering them up. In November 2008, the Department of Justice indicted an in-house lawyer for allegedly making false statements, concealing documents, and obstructing an investigation by the United States Food and Drug Administration.

The lawyer was not alleged to have been involved in the conduct under investigation. Instead, the charges arose out of alleged misrepresentations the lawyer made to the FDA regarding the completeness of the company's production.[6] Although the charges were ultimately dismissed, the case demonstrates the seriousness with which counsel must proceed in responding to governmental inquiries.

DO DISCUSS PRIVILEGE EARLY AND OFTEN.

Government inquiries inevitably implicate privilege issues. The company should consider at the outset whether, and to what extent, its potential voluntary disclosure to, and cooperation with the government will encompass a waiver of the protections otherwise afforded by the attorney-client and/or attorney work-product privileges. Whatever facts, information, or evidence a company may consider voluntarily disclosing to the government will most likely have been collected by the attorneys conducting the internal investigation.

Counsel should therefore consider memorializing only the purely factual aspects of the investigation's findings separate and apart from any non-factual attorney work product (i.e. mental impressions and potential legal conclusions) and core attorney-client privileged communications. To the extent the company decides to make a voluntary disclosure, the segregation of non-privileged facts will provide a privilege-free means of communicating with the government.

DO PREPARE FOR THE UNEXPECTED.

The number of government investigations is at an all-time high and is expected to continue increasing. All in-house lawyers should therefore be prepared for the unexpected. Your company should develop policies and procedures on how to respond to investigations and train employees on document retention, as well as protocols for talking to government investigators. Employees should know whether, and under what circumstances, the company will provide them with legal counsel. These policies and procedures should be reviewed with employees during their initial orientation, integrated into annual company training programs, and copies of these policies and procedures should be maintained in areas that are readily accessible.

Knowing how to properly respond to a government subpoena protects the company and minimizes potential risk exposure.

ENDNOTES

[1] 15 U.S.C. 78u-6, et seq.

[2] *SEC: Casino-Gaming Company Retaliated Against Whistleblower*, available at: https://www.sec.gov/news/pressrelease/2016-204.html.

[3] *Sally Yates, United States Deputy Attorney General, Individual Accountability for Corporate Wrongdoing, available at: https://www.justice.gov/dag/file/769036/download.*

4 Upjohn Co. v. United States, 449 U.S. 383 (1981).

5 U.S. Department of Justice, Criminal Fraud Section, Foreign Corrupt Practices Act Enforcement Plan and Guidance, available at: https://www.justice.gov/opa/file/838386/download.

6 United States v. Stevens, No. 10-CR-0694 (D. Md. Nov. 8, 2010).

Barrett Howell is a Partner in the White Collar Section of Bracewell LLP's Dallas office.

Ryan Meyer is an Associate in the White Collar Section of Bracewell LLP's Dallas office.

Kit Addleman is a Partner in the White Collar Section of Haynes and Boone's Dallas office.