ALFA International
THE GLOBAL LEGAL NETWORK

2022 Labor & Employment Seminar

February 2-4, 2022

WHAT TO DO WHEN OSHA, THE DOL, ETC. COME KNOCKING ON YOUR DOOR

Courtney Nichols
Moderator
PLUNKETT COONEY
Bloomfield Hills, Michigan
cnichols@plunkettcooney.com

Kathy Terry
PHILLIPS MURRAH P.C.
Oklahoma City, Oklahoma
kdterry@phillipsmurrah.com

BEST PRACTICES – RESPONDING TO AN UNEXPECTED GOVERNMENT INVESTIGATION

Knock, knock – it's the Department of Labor! Are you ready for an unexpected government investigation? An investigation that is not likely to be linear, predictable, or patterned? This article provides basic guidance to assist in-house legal departments and outside counsel proactively prepare for unannounced government visits and protracted investigations.

A. Pre-Knock Preparation

Companies should work to establish: (1) policies; (2) response teams; and (3) an understanding of potential investigatory actions *before* the unexpected knock.

a. Policies

Companies should have a written protocol outlining the basic steps for each and every government investigation. The protocol should address: what contact needs to be made upon notice of an investigation and the method for such contact; the litigation hold/evidence preservation steps that must be taken in every case; confidentiality obligations of the individuals contacted; identify of external counsel who may be brought in to assist; and discussion of any internal audit(s) that may be relevant to government investigations (among other provisions that may be company or industry specific).

b. Response teams.

Companies should discuss, *before an investigation,* the members of a "Response Team". Generally the team is comprised of in-house legal and/or compliance professionals, along with outside counsel and/or trusted members of management within different regions/geographic locations. If an investigation will span multiple work sites, the team should include a trusted manager or official at each worksite.

In conjunction with identifying members of the "Response Team," companies should also establish specific contact chains. That could be a hotline, a distribution list, an internal database/chat function, etc.

c. Potential investigatory actions.

What agencies have jurisdiction and oversight with regard to the company's business? Some are easy to identify: the DOL, OSHA, EEOC, etc. But what about health and human services or the environmental protection agency? What state regulators or inspectors might stop by? What agencies have subpoena power and who cannot come barging in unannounced? Creating a checklist so that the Response Team has a basic understanding and does not invite an investigator in without authority and/or jurisdiction is critical.

The Response Team and/or in-house counsel should also work to prepare employees who will likely be targeted for government interviews. As a general matter, this would include: human resources employees; receptionists/those likely to answer calls and/or the door; compliance employees; and executives.

B. Post-Knock Actions.

Now they're here! If your company has completed the steps outlined above, the following should occur in a methodical fashion.

a. Contact and employee briefing.

After the investigation has begun, the Response Team/applicable team members should meet and debrief with counsel to determine: the nature/scope of the investigation; and what was already discussed. The company should then contact the government agency/authority and identify the primary contact moving forward, along with request that future requests for documents *and interviews* be directed to counsel.

Employees who are likely to be interviewed during the investigation should be identified and contacted as soon as practicable. Employees should know and understand their rights – including their choice to voluntarily submit to an interview. Be careful to not issue any directive that could be misconstrued as an attempt to obstruct justice. Telling the *truth* and preserving all evidence and information should be common themes prevalent throughout all employee communications.

b. Assess type and scope of investigation.

The method of contact is critical to assessing the scope and impact of an investigation.

For example, a Civil Investigative Demand ("CID") is a civil subpoena directed to the company. A CID does not pertain to criminal allegations and general commands the production of documents initially. Failure to comply can subject to the company to civil penalties or court sanctions. The government may serve a CID on any person or business in any jurisdiction in the U.S. and in foreign countries, provided such service complies with due process requirements. Typically a CID has a very short response time, which is often extended after communication between the investigator and counsel.

Conversely, a Grand Jury Subpoena indicates that a *criminal* investigation is underway. Unlike a civil subpoena, failure to comply or adequately comply with a grand jury subpoena can mean a criminal charge of obstruction of justice. It also indicates that there has been significant pre-service activities and the government's investigation has progressed significantly.

After determining the type and potential impacts of the investigation, you should assess whether the request can be narrowed. A CID usually begins as very, very broad. Government investigators and/or attorneys are often willing to narrow the scope if it means it will streamline the investigation and assist them with quickly locating relevant and meaningful information. It is not unusual for a CID to mirror a template document that necessarily requests irrelevant information. Do not feel as if you are stuck complying with each and every request, without modification.

c. Preserve and track location of all potentially relevant records and information.

Companies must immediately engage in a good-faith effort to preserve all documents and information related to the investigation. This includes: electronically stored information; documents; witness statements; photographs; surveillance video; text messages/chat messages; social media messages; and all other forms of arguably relevant tangible information. A list of custodians who may have relevant documents should be created within 24-48 hours of notice of the investigation and those custodians should be put on alert to not destroy their communications and/or evidence. Any automatic deletion of documents/email policy should be immediately suspended as to all relevant custodians.

Companies should receive a signed acknowledgment from each custodian confirming: (1) they have received the hold notice; (2) they will not delete or destroy any relevant (err on the side of over-inclusion) records; and (3) they understand that their failure to comply could have serious ramifications and may result in disciplinary action.

Simultaneously, IT should be contacted to make sure that automatic deletion cycles are suspended, that email

accounts are preserved (in their entirety), that phone records/video surveillance is preserved, and that the preservation efforts are being documented. As a general matter, the company should have a spreadsheet or list of relevant and/or potentially relevant information and identify: (1) the location of such information; (2) the preservation efforts taken with regard to that information; and (3) the individuals with access to that information.

d. Determine whether a parallel internal investigation is warranted.

Depending on the subject matter of the investigation and circumstances involved, there may be a need to conduct an internal investigation at the same time as the ongoing government investigation. Such reasons could include:

- Addressing and stopping any ongoing wrongdoing.
- Providing interim/remedial measures to affected employees.
- Remediating potential fines by showing the government you're taking action yourself – however, this could be construed as an "admission of liability" in cases where you intend to contest such liability.
- Protecting executives and members of the board of directors from claims they have breached any fiduciary duties owed to the company.

When a parallel investigation is occurring, it is critical to ensure that: (1) there is no conflict of interest as it relates to the chosen investigator; (2) information is not being corrupted in the internal investigation that could affect the government investigation; (3) the company is not admitting liability and/or creating a record by which liability may be found at a later date; and (4) the Board/executives are aware of the internal investigation and potential ramifications of same.

It is also to note in internal investigations that employees must be given the *Upjohn* warning before starting each interview. This is akin to a *Miranda* warning, which warns the employee that counsel represents the employer and not the employee, that any privilege attaching to statements made during the interview belongs solely to the company, and that the company may waive the privilege and disclose the contents of the interview to third parties, including the government.

e. Review and maintain.

This one is likely common sense: no document should be turned over to the government without: (1) reviewing and identifing the document; (2) making note of the production of the document (generally every provided should be copied and maintained independently by the company); and (3) red-flagging documents that will likely result in future requests or interviews. Any document that is privileged (i.e. HIPAA protected, GDPR protected, or attorney-client privileged) should not be turned over but should be cataloged as responsive and withheld. With turnover of staff and the length of time many investigations last, a log or other record of communications to identify requests already made, responses issued, conversations with investigator(s) regarding documents and requests, will likely be a significant time and resource saver in the future.

A best practice is creating a chronology, along with reference to associated documents. For example:

March 1, 2022: DOL initiated wage and hour investigation. CID received.

March 18, 2022: Documents provided – found at Bates 00001-00208 in Binder 1, Tab A. Also located at (add internal hyperlink)

March 25, 2022: Witness AB questioned. Spoke mostly regarding Bates 00100-00103. No issues.

April 18, 2022: Phone call with investigator; sending requests for additional information. Wants to narrow scope of investigation. May have three more witness interviews.

April 20, 2022: Additional requests received. Response due by May 2, 2022.

May 2, 2022: Provided responses – found at Bates 00209-00352 – Binder 1, Tab A. Also located at (add internal hyperlink).

C. Concluding the Investigation.

At the conclusion of a government investigation, the investigator will generally schedule a time for a final conference (note: this is the practice in DOL investigations). The final conference should be attended by counsel and at least one other individual who takes very thorough notes. The notes are critical for when the final assessment letter is received to confirm that there are no "surprises" in the ultimate assessment/conclusions of the investigator that the company was not given an opportunity to address.

If the company disputes a violation, they should not wait to present the evidence at a hearing or in subsequent litigation. The company is best served by being transparent and identifying the particular reasons why they think the investigator/agency is misplaced, along with the evidence they have in support of that belief.

Depending on the agency and type of investigation, settlement or negotiation may be possible. Companies should work with their Response Team and trusted colleagues to gather information regarding the investigator/agency's *recent actions* relative to settlement or compromise *before* signing off on investigation results or issuing payment in full for any alleged penalties or fines.