

PUBLICATION

Four Tips for Responding to a Civil Investigative Demand: A Report from the Trenches

November 22, 2013

Simply being served with a Civil Investigative Demand (CID) means enormous financial strain and reputational risk for some companies. On top of that, in this heightened regulatory environment, federal agencies seem to be trying to prove that each is the toughest enforcer on the block. Based on recent experience, this tough-on-enforcement attitude manifests as:

1. At the start of the investigation, little to no negotiating with the government on the scope of a broad CID.
2. During the course of the investigation, little to no feedback from the government as to any issues/violations it is finding.
3. At the conclusion of the investigation, little to no information as to the number of any issues/violations identified and no specific examples of any issues/violations identified.
4. At each stage, no guidance from the government about what practices should be adopted, ceased or modified in order to satisfy the government.

Despite this unfortunate reality, at least forewarned is forearmed. If your company knows that it likely cannot alter the scope of the CID, then your company can concentrate on complying with the CID as efficiently and cost-effectively as possible. To that end, here are some practical tips learned from recent experience.

5. Retain outside counsel as soon as possible, and *involve* outside counsel early on for two reasons. First, to ensure the attorney client privilege protects communications pertaining to the investigation. Second, so that the privilege protects communications pertaining to issues/challenges of which your company is already aware and already trying to address.
6. Notify and involve your IT person early on. The CID will likely require your company to produce huge volumes of data and to produce it in a format that the government can review with its software. Your IT person may have to communicate with various third party vendors to access certain data if the data is stored in a proprietary system. Also, your IT person may need to undertake "trial runs" of producing samples of data in order to be able to provide reliable estimates to the government as to how long it will take your company to produce certain categories of documents in the necessary format.
7. Decide early on whether to disclose the fact of the CID beyond the immediately relevant employees who will be responsible for complying with it. If the fact of a CID is disclosed too widely, it could result in loss of business and negatively affect employee morale. On the other hand, disclosing the existence of a CID to targeted individuals can prevent problematic email communications about issues/challenges that the company is trying to address. Also disclosing the CID to certain former employees may be necessary if there is sufficient reason to believe that the government will attempt to contact them.
8. In selecting the "team" within the company that will be responsible for complying with a CID, it is important to consider seniority alongside personal characteristics like being responsive, thorough, protective, and willing and able to delegate. While the government will likely extend certain

production deadlines based on a legitimate reason for the delay, given the vast scope of a CID, one delay in production can easily result in a domino effect of other deliverables falling behind.

In this new heightened regulatory environment, simply responding to a Civil Investigative Demand is more difficult. However, if a company knows what to expect going into the process, the company can at least focus its energies on complying with the CID as efficiently and cost-effectively as possible.