RISK MANAGEMENT

5 Tips for Responding to Civil Investigative Demands

Christine Kirchner

September 17, 2020

LEGAL RISK

Civil investigative demands or letters, also referred to as CIDs, are powerful tools for the Attorney General and other government agencies to collect and acquire information necessary for an investigation that could result in the prosecution of individuals or entities. CIDs target individuals or entities believed to have defrauded the U.S. government or abused governmental programs. Common recipients of CIDs include medical providers and health care companies being investigated for fraud or submitting false claims to government health care programs, as well as federal government contractors that allegedly inflated pricing for labor or materials or otherwise engaged in improper billing, or "false claim" practices.

Frequently, the U.S. Department of Justice (DOJ) issues CIDs related to *qui tam* (or whistleblower) lawsuits, in which the government seeks information from the target to determine the validity of the whistleblower's allegations and to evaluate whether it will intervene in the civil proceedings. Until a CID is issued, the target may have no knowledge of the lawsuit filed against it because it is under seal and not readily accessible in the public record.

Any company who receives a CID should recognize the seriousness of the request and thoughtfully prepare its response. It is important to understand that when a CID is issued, it is considered an instrument aiding a civil investigation that can produce a criminal prosecution. Additionally, even in the civil context, the impact can include significant damages and civil penalties, reputational harm, and potential

In general, CIDs request documents and other material believed to be either in the possession, custody or control of a target to be either inspected or produced. Not only are physical business records frequently requested, but also electronically stored information (ESI), including emails, text messages and even voicemail messages stored on a company's server. CIDs can also include questions relating to the requested documents and materials and can further require the provision of recorded statements.

Upon receiving a CID, the company should first consider which individuals or departments will have to produce information and start a preservation program to ensure that they do not destroy or delete relevant documentation through any sort of corporate document retention policy. It is vital to avoid inadvertent ESI destruction. For example, companies should avoid disposing of employer-issued devices, and disable the automatic deletion of ESI that may no longer be stored on an individual user's cell phone or laptop but still stored on the entity's servers. It may be necessary to implement a bring your own device (BYOD) policy or issue directives to employees who use personal devices to not alter or replace their devices.

Secondly, the company needs to immediately determine the scope of the CID and whether it can respond and comply given resident expertise. Generally, retaining outside counsel is advised, with the rare exception of larger companies with sophisticated in-house legal resources. It is important to make an initial determination as to whether the issuing agency or DOJ has complied with basic procedural requirements such as specifying the conduct being investigated, the laws violated, or the type of information being requested and how it must be produced. If the request is overly broad, burdensome or invasive, the company should consider negotiating with the issuing agency and possibly filing a motion to set aside or modify the CID. Keeping open lines of communication with the issuing authority is key. Early communication and a willingness to cooperate can change the course of the investigation—ideally keeping it civil. A prompt acknowledgment and conversation about the requests and their scope, with an early intervention or clarification request can cause the agency to be cooperative.

Thirdly, if possible, determine whether the recipient of the CID is a target of a fraud investigation or merely a witness who is deemed likely to have or control relevant information or witnesses relating to another person or entity under investigation. Such information concerning what laws may be violated or the conduct being investigated may not be apparent from the CID. Again, prompt consideration of the CID and early planning can save precious time if a dialogue needs to be opened or a legal motion needs to be filed with regard to its validity.

Fourth, ensure that the information provided is complete and accurate, as answers to written questions or any testimony provided will be under oath and written certification that all documents requested have been produced will be required. CIDs are powerful instruments because they allow the issuing agency to request information and testimony far broader than through typical discovery devices. In fact, challenging CIDs or successfully narrowing the scope is extremely difficult as most courts will give great deference to the requests and allow very few objections or claims of privilege to the documents. This is why CIDs are a more frequently used tool—once the government decides to intervene in a whistleblower action, or initiate its own suit, it will be limited to traditional discovery instruments.

Maintaining credibility with the government is critical to avoiding increased scrutiny for a claim with the DOJ. It may be tough to strike the right balance between being forthcoming and complying with the CID in a comprehensive way and instinctively protecting the company's interests. This is a primary reason to retain counsel with the necessary expertise. Being untruthful or misleading in your communications with the entity issuing the CID or producing incomplete information will likely draw additional scrutiny and possibly turn a civil investigation into a criminal matter.

Finally, negotiate away the inevitable, with counsel if possible. If your internal investigatory process indicates that documents and/or the witness testimony show improper billing practice or fraud, attempt settlement with the DOJ or other governmental agency. While turning over documents may be mandated, this also poses a threat to the entity because there is no Fifth Amendment privilege related to the production of documents as exists with regard to an individual's testimony. If you are going to negotiate a settlement, ideally you will want to do so before any sealed complaints become public record after a limited period of time. However, DOJ may request and file motions with the court to keep the records under seal, particularly if the investigation is cooperative and fruitful.

Responding to a CID requires prompt and skilled attention during the typical 20-day response period. Quick planning can lead to either a cooperative and successful provision of information or, in the worst case, an open dialogue with the DOJ or other governmental agency that could mitigate the investigation's impact, and ideally, prevent reputational harm and keep the process civil.