PUBLICATION

The Evolving Risk of Fraud in the Wake of COVID-19

September 25, 2020

Earlier this summer, the Department of Justice (DOJ) updated its *Evaluation of Corporate Compliance Programs* guidance. As the recent updates make clear, one of the hallmarks of an effective corporate compliance program is the ability to conduct well-scoped, appropriately funded, independent, objective, and well-documented investigations. The current workplace realities created by the COVID-19 pandemic (remote workers, social distancing, limited travel, new technologies, etc.) have changed how internal investigations are conducted. Despite some of the current difficulties associated with internal investigations, the DOJ compliance program guidance makes it clear that internal investigations remain a critical element of any well-functioning compliance program. Performing internal investigations under current circumstances requires flexibility and the use of appropriate (and in some cases new) technology.

Current economic and workplace conditions underscore the importance of internal investigations as a key element of an effective compliance program. Increased competitive pressures on companies and financial stress on individual workers coupled with remote work environments (including management and compliance professionals) create a petri dish of opportunities for fraud and other misconduct. In September 2020, the Association of Certified Fraud Examiners published the results of a survey of certified fraud examiners. The survey notes that certified fraud examiners overwhelmingly (74 percent of respondents) confirm that preventing, detecting, and investigating fraud in the COVID-19 environment is more difficult than it was pre-COVID. To compound matters, the survey finds that fraud and other misconduct has been on the rise since COVID began:

- 77 percent of respondents observed an increase in the overall level of fraud.
- 92 percent of respondents expect to see a further increase in the overall level of fraud during the next year.
- 83 percent of respondents observed an increase in cyber fraud schemes and 90 percent anticipate a further increase over the next year.
- 69 percent of respondents have observed an increase in fraud by vendors and 83 percent anticipate a further increase over the next year.
- 57 percent of respondents have observed an increase in loan and bank fraud and 76 percent anticipate a further increase over the next year.
- 42 percent of respondents have observed an increase in employee embezzlement and 73 percent anticipate a further increase over the next year.
- 49 percent of respondents have observed an increase in bribery and corruption and 70 percent anticipate a further increase over the next year.

Although the technologies and methods may need to change, the basic elements of conducting an effective internal investigation remain constant. Relevant documents and data need to be reviewed. Employees, subcontractors, and vendors need to be interviewed. The information discovered needs to be analyzed and a report needs to be delivered to management and/or the Board in a timely manner. As always, this process needs to be done in a manner to ensure accurate and candid treatment of those involved and the protection of confidential and privileged information.

The first step in any investigation is finding what relevant information exists in an internal resource like the Internal Audit Department or Human Resources or an external resource such as an investigator, accountant, or legal counsel. As most relevant information is already in an electronic format, it should be provided to the investigator in an easily accessible and cybersecure manner. Because the information is often highly sensitive or privileged, the importance of cyber security in conducting internal investigations cannot be overemphasized. The release of business sensitive information and/or privileged information is never a desired unintended consequence. For international sources of information, especially in the EU, various restrictions under GDPR may also apply. In the remaining circumstances where the relevant information is only available in a hard copy format, health precautions (masks, gloves, social distancing, etc.) for both the investigator and records custodians should be devised so that the investigator can obtain the relevant information in a timely, secure, and safe manner.

Another essential aspect of any competent investigation is conducting and documenting interviews of those involved. Although current working conditions may limit the ability to travel and conduct in-person interviews (which are preferable as they allow the investigator to form better opinions about the credibility of witnesses and observe body language), alternate methods such as Zoom, WebEx, or even phone calls should be used (and recorded). Although remote virtual interviews may seem more informal than traditional in-person interviews, investigators need to ensure that video interviews are conducted with similar dignity and formality as in-person interviews. This includes ensuring that attorneys conducting virtual interviews provide witnesses appropriate *Upjohn* warnings to ensure the witness understands that the attorney represents the company, not the witness, and therefore, the company controls any waiver of attorney client privilege or confidentiality.

As part of any remote witness interview process, the investigators need to ensure that the IT tools and connections work for both the investigator and the witness and no interruptions occur. If an online platform is utilized, the investigator needs to ensure that it is a secure, password protected, method. Again, confidential information and any applicable privileges should be protected from inadvertent release or waiver. Getting documents beforehand to witnesses may expedite the interview but also give witnesses more time to explain troublesome ones. The ability to confer with fellow investigators during interviews via private chat rooms should be set up. Reporting up to the proper chain — orally or in writing — is next.

Conversely, companies may take some solace in knowing even the government faces COVID-related challenges in conducting its investigations. For instance, the Securities and Exchange Commission has been using initial interviewing capabilities to conduct its investigations via a Zoom-like proprietary program. Government investigations may shorten what in normal times might be a longer session. Investigations will object to obvious texting by witnesses on their devices. Postponements and attorney proffers have now become more frequent. Likewise, various United States Attorneys' offices have now reinstituted in-person grand juries to take evidence, including dividing the panel into groups seated in separate rooms, with Zoom connections, while the prosecutors, witnesses, and court reporters conduct the examination and receive and mark exhibits in another room.

All of these complications point to one obvious result: more planning and likely delays in getting information is for the time being what investigators have to endure. Delays in self reporting, cooperation with the government, and remediation, as well as enhancements to compliance programs from lessons learned, may follow.

If you have any questions, please contact one of the authors or any member of Baker Donelson's Government Enforcement and Investigations Team.