Conducting Internal Investigations During the COVID-19 Pandemic

In times of crisis, criminal activity — particularly crimes involving theft and fraud — tend to spike. There is no reason to believe that the Covid-19 pandemic and the unrest in the financial markets will be any different. An important difference for company counsel, however, will be in how the malfeasance, negligence or wrongdoing can be investigated.

By Jacqueline C. Wolff, Scott T. Lashway and Matthew M.K. Stein
Law Journal Newsletters' Business Crimes Bulletin
March 25, 2020

In times of crisis, criminal activity — particularly crimes involving theft and fraud — tend to spike. There is no reason to believe that the COVID-19 pandemic and the unrest in the financial markets will be any different. An important difference for company counsel, however, will be in how the malfeasance, negligence or wrongdoing can be investigated.

The usual methods for conducting a meaningful and thorough investigation need to change quickly. In-person document collection and review as well as face-to-face interviews are out, and questions and challenges have arisen for counsel. For example, without in-person witness interviews, how can defense counsel truly assess the merits of any whistleblower report or a witness's credibility? How can documents be shown to a witness sitting in a different country if borders are closed and flights are cancelled? Even if the law firm has a local office in the country in question, what if that country is in lockdown? How can documents be transmitted across international borders to U.S. counsel needing to defend the company before the DOJ or the SEC without violating local privacy laws? How can a company ensure enforcement of a document hold during an internal investigation and parallel government inquiry when its employees are all working from home? And with counsel accessing a company's data remotely and increases in Internet crimes, such as phishing, how can the security of that data be maximized?

Preservation of Documents and Legal Holds

COVID-19 and extended remote-work arrangements present new issues around implementing legal holds and preserving documents subject to government inquiries. More employees work from home, bring documents home, print documents at home, and electronically store documents at home or on non-business computers, devices or systems. Those home-based documents will be outside of any automatic document hold that can be applied by a company's IT department, and manual holds, especially of physical documents, require individual employees' cooperation. Accordingly, companies should:

1. Remind employees that company information created or stored off-premises belong to the company and remain subject to a legal hold if one is in place; copies of electronic documents should not be stored on employees' home/personal computers or in personal cloud storage accounts.
2. Consider extending time periods under existing document retention policies.
3. Remind employees that communications should be made using only company-approved channels and not through text messages, and that they should not delete voice messages on their personal phone on matters covered by a document hold or message retention policy.

Document Collection

Travel restrictions challenge the typical collection process. Sophisticated companies may be able to handle collecting electronic documents in-house with direct transmission to a vendor to process and load into a review platform. With technology personnel working from home, companies will need to consider the following:

1. For inaccessible physical documents and locally-stored electronic documents, are they critical to the investigation? Do electronic documents or records stored on centralized or cloud-based servers exist that can serve as useful proxies?
2. For electronic documents stored on centralized servers, if remote work restrictions prohibit technology personnel from forensically capturing metadata and file structures, do personnel exist who have access to most documents? They may be permitted to make them available to counsel for review using alternative means. Of course, that could increase a company's cybersecurity risk. These measures should not be undertaken without a thoughtful and informed balancing of the risk and criticality of each category of documents.

Issues Particular to Global Investigations

COVID-19 travel restrictions raise important considerations for counsel around digitizing physical documents, the wisdom and availability of cross-border document transfer, and the mechanism used for cross-border transfers — from both legal permissibility and cybersecurity risk perspectives.

The documents may be a type that cannot be transferred out of the country for jurisdictional reasons or because local laws require them to be stored in that country. In certain countries, bank privacy laws may prohibit transfer of such information outside of the country. In other countries, blocking statutes may prohibit providing information to individuals in the United States for a non-government investigation or for any purpose without approval of the host government. In both instances, violators could risk criminal penalties.

The documents could also contain personal data subject to a privacy law imposing restrictions on cross-border transfers to the United States or on new uses (briefly, international privacy laws broadly define personal data as information relating to an identified or identifiable individual, generally including business contact information; exceptions exist, however). Those types of restrictions are becoming common, requiring consideration of whether transfers and viewing by counsel are consistent with privacy notices and permissions relevant to the personal data contained in the documents, what cross-border mechanisms are permissible and what documentation is required. Today, Argentina, the Cayman Islands, the European Union, Israel, Japan, Switzerland and the UK all have rules limiting cross-border transfer to the United States. If India enacts a pending privacy bill, it may join them. And under Hong Kong law, the individual's consent is required for a use that is not consistent with the terms of the initial privacy notice.

Depending upon the facts, workable solutions may balance the need for review with the risk of making the documents available to counsel in the United States, such as placing documents on the company's or a vendor's cloud storage or using thin clients. (A thin client is a computer or software program that connects to a remote server and displays applications and data run on the server.) These solutions need to be carefully considered in light of applicable privacy laws:

1. Cloud-based storage. The documents could be stored in the company's cloud server or in a cloud storage account owned by the company. Even though U.S. counsel is downloading the data, the company could take the position that no non-privileged copies of the documents exist in the United States. However, the transfer itself could raise concerns under privacy laws, and storage in the cloud could be contrary to information security protocols. Cloud storage is not fully within the company's control, and if misconfigured, it could expose the documents to third parties. Finally, the company would need to contract with the proper cloud storage or service provider to provide that storage: g., if a contract is signed with a U.S. company, it is more difficult to argue that the documents were not transmitted to the United States or to a company within the United States' subpoena power.
2. Thin client access. A thin client, if configured to prevent counsel from downloading or printing documents viewed on the thin client, could permit a company to take the position that it has not

transferred the documents viewed through it to the United States. Counsel should ensure that the company's position is internally consistent on the issue. If this approach is used, technology personnel should be consulted to ensure that counsel receives the minimum access necessary to view the documents and that information security protocols are not otherwise violated.

3. Remote server access. A company could reconfigure its offshore servers to give access to U.S. counsel. Again, technology personnel should be consulted to ensure that this configuration does not violate information security protocols or increase the company's cybersecurity risks. It also presents the same risks around potential transfers to the United States when U.S. counsel accesses the documents on those servers.

Those considerations are magnified when handling physical documents containing delicate or sensitive content, or electronic information stored in an air-gapped system. (Air gapping is the practice of creating computer networks that have no connection to the global Internet. Systems accessible through a VPN are not air-gapped.) Some documents may contain particularly sensitive content preventing transfer to another country, including the United States. Counsel will need to consider the risk of converting physical information to electronic form as well as what on-the-ground options are available for examining the material. For example, could counsel employ 'agents' in the country without waiving privilege or the investigation's confidentiality? This depends in part on the country: different countries apply the attorney-client privilege and attorney work product protection differently. If local 'agents' in a country keep copies of their contributions to an investigation, they could be seized by that country's government — even if those documents are privileged under U.S. law — because the local government does not have comparable privilege laws.

Witness Interviews

Unless company counsel is in the same geographical area as the witness and that area is not subject to travel restrictions, it may be impossible to perform in-person interviews. The challenges to telephone interviews have not changed: e.g., no credibility evaluations, and no certainty as to the number of listeners on the telephone call.

Using a video bridge helps solve that. Counsel can see the witness. It reduces the risk that unannounced participants are on the line; most video calls cannot be conferenced without the host's knowledge. And video calls provide some ability to assess credibility, albeit imperfectly.

But concerns remain about conducting interviews by videoconference. Local law could impact it — or the witness could record it. For example, at least one U.S. court acknowledged Italian law's apparent granting to employees a broad right to take, for employment litigation purposes, documents and information concerning the employer; an Italian employee might decide under that legal protection to record the interview. Under Article 24 of the Italian Constitution, the right to defense is "inviolable at every stage." See also, AlixPartners, LLP v. Mori, C.A. No. 2019-0392-KSJM, 2019 WL 6327325, at 14 & n.147 (Del. Ch. Nov. 29, 2019). While the General Data Protection Regulation (GDPR) would likely require notice of recording, an employee intending to record the interview for litigation purposes may not be aware of, or inclined to follow, applicable legal restrictions. Moreover, in many U.S. states and foreign countries, e.g., New York and India, a conversation may be recorded if one party to it consents.

Remote video interviews where counsel does not have in-person representation introduces other challenges: exhibits, documents, and the witness's own counsel. While under normal circumstances, the witness and their own counsel will be in the same location for a video interview, with everyone self-isolating that may not be possible. A protocol, therefore, has to be set up to allow the witness to confer with counsel during the course of the interview without company counsel "present."

Another significant challenge to remote video interviews relates to document handling:

1. For documents shown to the witness, counsel will need to decide whether to provide them in advance or show them on screen. It is better to show them on screen: it avoids the risk that documents sent by courier will be delayed in transit — a higher likelihood with cross-border quarantines — and could avoid introducing documents into a country that counsel might prefer not to. Regardless, counsel should test their videoconferencing approach in advance, as not all platforms allow efficient on-screen sharing.
2. For documents stored in a country with restrictions on cross-border transfers to the United States, U.S. counsel may be tempted to ask the witness to put them on screen for discussion. Keep in mind that transmission by video bridge is no different than using a thin client and subject to the same caveats.

* * *

The current climate presents new hurdles for company and counsel handling internal investigations. Those hurdles can be overcome, and for urgent internal investigations, at speed — but only with thoughtful and advanced planning.

*****

Jacqueline C. Wolff, a member of the Board of Editors of Business Crimes Bulletin, and **Scott T. Lashway** are partners at the law firm of Manatt, Phelps & Phillips, LLP, in the Investigations and White Collar Defense and Privacy and Data Security practices. **Matthew M.K. Stein** is a Special Counsel in Manatt's Privacy and Data Security practice. They can be reached at jwolff@manatt.com, slashway@manatt.com, and mstein@manatt.com. *Any opinions expressed in this article are those of the authors, and not necessarily those of Manatt or any one or more of its clients.*