# *IN THE BREAKOUT ROOM WHERE IT HAPPENED:* PRACTICAL TIPS FOR VIRTUAL INTERNAL INVESTIGATIONS

Jessica Magee
Michael Stockham
Sydne Collier

The days of a bubble-gum-and-baling-wire approach to the many issues flowing from COVID-19-induced telework are quickly fading. Companies must adapt to the realities of an extended period in which employees will operate remotely. For management teams, this means expanding focus to ensure new or changed risks are identified, addressed, and mitigated. Chief among them are compliance risks relating to internal controls over financial reporting, cyber controls, and safekeeping of confidential business and customer information. Whether resulting from systems-based surveillance, internal reporting, or whistleblowing, executive leadership and boards of directors face new hurdles and considerations when launching and overseeing an internal investigation. And these considerations are receiving greater attention as weeks turn into months, and months turn into quarter-and year-end financial reporting. Here, we offer some practical tips from our recent experiences investigating in an entirely remote and virtual environment.

## COMMUNICATE OFTEN AND MANAGE EXPECTATIONS

No one likes surprises, least of all a company's auditor or directors. When an issue surfaces, it is critical to inform key stakeholders to ensure those who "need to know" have the information necessary to move the operations of the company forward, while also fulfilling their obligations under accounting rules, corporate governance, and the law.

Problems do not go away; they fester. Companies with an issue to investigate should immediately deploy assets to run a proper process to weather the turbulence that allegations of impropriety and an internal investigation can bring. In-house counsel, compliance officers, and internal auditors must be especially vigilant in communicating allegations of executive misconduct or financial irregularities to the audit committee or others tasked with ensuring the integrity of financial reporting and internal controls. In this new virtual and remote environment, this means management should ensure its compliance hotline and other internal reporting and surveillance tools are not only

functional, but that they have adapted as warranted to address the needs and risks of a remote workforce, and are being actively monitored by authorized personnel and escalated in accordance with applicable policies, which themselves have been reviewed to ensure harmony with COVID-19-modified conditions.

Once made aware of alleged improprieties, the audit committee should communicate the scope of the concern to the audit partner from the accounting firm for their company and ensure the audit firm that the committee will conduct an investigation with integrity to fully understand and remediate any issues. The knee-jerk reaction is to worry the audit firm or others will "freak-out" when, for instance, alleged accounting irregularities or internal control busts surface. But the antidote is to communicate, early and often, to those who have a stake in uncovering any wrongdoing. Be intentional and consistent about the method, means, and records of such communications to ensure that, despite being dispersed across various locations and enticed by the ease of text-based communication, relevant stakeholders are participating in timely and robust process governance.

Once a remote investigation commences, providing feedback early and managing expectations often go a long way to ensuring that when the investigation concludes the stakeholders have sufficient information to do their jobs confidently and effectively. For example, the auditor's forensic "shadow team" will need sufficient information to judge whether the investigative process was reasonable. Poor or insufficient communication, intentional or otherwise, can impact that judgment and increases the risk of complications at the end of an investigation.

## ESTABLISH AND REINFORCE INVESTIGATIVE INTEGRITY

Investigative integrity is in the eye of the beholder—often the auditor's forensics team and, sometimes, regulators, law enforcement, and shareholders. Management, directors outside of the virtual investigation, and key investors must not influence the process, for instance, by requiring in-person interviews, limiting the time or scope allowed for interviews, or restricting access to tools generally used to facilitate virtual engagement (*e.g.*, screensharing of documents).

Investigators need to understand the company's policies and practices for conducting internal investigations and determine how to proceed virtually under

them. Similarly, investigators should counsel their client—often the board's audit committee—about the importance of understanding and adhering to company polices relating to trading restrictions, use of material nonpublic information, and preventing selective disclosure and other Regulation FD considerations during an ongoing (albeit virtual) investigation.

The remote nature of a virtual investigation increases the importance of working with a reliable member of management to coordinate access to relevant data and witnesses. Although this member of management is often integral to coordinating logistics in an investigation, it is important that they do not become *participants* in the investigation. Investigators should make clear to this management member at the outset that they cannot "listen in" on virtual interviews, even if they assist in scheduling and starting them. In addition to the standard practice of introducing the participants in an interview, investigators should consider stating that nobody else is permitted to participate in a phone- or video-based interview and ask any other individuals "in the room" to announce and excuse themselves by disconnecting.

## PLAN FOR REMOTE DOCUMENT AND DEVICE COLLECTION

The realities of texting and other communication apps means investigators often need to collect data from employees' and executives' phones. And factors, like whether a company issues devices to employees or allows them to "BYODevice" and related company policies, impact investigators' access to certain device-held data. Even once an investigator understands applicable access rights and restrictions, the nature of a virtual investigation can complicate the logistics of collecting device-held data. During COVID-19, many vendors are not allowing technicians to go onsite to a company's office. Thus, investigators are often responsible for remotely coordinating the pickup and return of a witness's device with the vendor's technician—while also garnering witness trust that access to the device will not be abused or expose unrelated personal information. Hence, in this era of virtual investigations, special attention should be paid to forming an achievable plan for timely and responsibly collecting, imaging, and returning witness devices and securing the understanding and agreement of the witness to do so when required.

Remote investigations have little impact on the process for gathering electronic data from a client. IT departments now regularly transfer emails and other data electronically through file-transfer sites. However, the process for identifying, securing, obtaining, and reviewing hard-copy materials and external storage devices from a witness (*e.g.*, journals, calendars, notes, thumb drives, etc.) has

been significantly impacted. In every interview, investigators should ask the witness to describe the type and location of such materials in her possession, custody, or control, and whether any such materials have been intentionally or inadvertently deleted, destroyed, or lost. Investigators should also devise chain-of-custody protocols to ensure that gathering such materials occurs in a timely and reasonable manner, thereby demonstrating process integrity.

Once the investigators collect hard-copy materials, they must devise a strategy for using them remotely during witness interviews. Current videoconference platforms have tools that allow investigators (and witnesses when warranted) to share documents during conference. However, the process can be tedious, especially when documents are lengthy and the witness (rightly so) wants to be familiar with the entire document before answering any questions. One alternative is to provide materials before the interview—by overnight mail or secured file share site, for instance. Investigators need to consider whether to advise a witness that she should or may review the documents prior to an interview or, alternatively, should *not* access them until instructed to do so during the interview and then only on-camera to ensure integrity of that process. Similarly, investigators can email the witness a password-protected zip file with a read receipt requested, and instruct the witness not to open until the interview begins. Compared to screen-sharing, this technique provides more freedom to the witness to review documents at their own pace before or during the interview as the case may be, and also provides investigators added control about when to make witnesses aware of certain documents in a remote, virtual setting. Regardless of the process, investigators should document the steps and rationale behind the approach to prepare to defend it as a reasonable to the audit firm and other potential third party stakeholders, including regulators and law enforcement.

## GIVE APPROPRIATE AND EFFECTIVE *UPJOHN* WARNINGS

Attorneys investigating on behalf of a company must provide effective *Upjohn* warnings and take steps to protect privilege during their work. This is especially important during virtual investigations, where there are new and different risks to ensuring confidentiality and maintaining privilege. Investigators should keep three major points top of mind when planning and conducting an investigation.

*First*, establish who enjoys the privilege. Investigators should communicate: (1) who they represent (the audit committee, for example), (2) that they are hired to gather information and provide legal advice to that client, (3) that they do not

represent and cannot advise the employee, (4) that the company may decide to waive its privilege and share the employee's communications with others, and (5) that employees should treat the interviews as confidential.

*Second*, protect the privilege. Consider the particular circumstances of interviewing employees (and sometimes company outsiders) remotely, and fashion appropriate restrictions and agreements tailored to the circumstances. For instance, investigators should consider using a single platform to conduct online interviews. If possible, use the platform already used by the company so that employees can easily access and navigate virtual interviews. When coordinating interviews, remind the employee that the discussion will be confidential and that he or she should make arrangements to be set up in a private location, with good internet connectivity. Once connected to the virtual interview and while providing the *Upjohn* warning, consider asking the employee to describe where they are located and whether others are present. Additionally, obtain verbal or written confirmation from the employee that he or she:

- agrees to keep the interview confidential;
- is alone in the room with a door shut;
- is not permitting anyone to "listen in" by any means, and took reasonable steps to ensure he or she is not overheard or interrupted;
- is not recording the interview;
- will not take notes during the interview or make notes about the interview afterward; and

*Third*, reinforce the privilege. Investigators must make the same preparations to ensure confidentiality by conducting the interview in a secure location, making proper attorney-client privilege and attorney-work product disclaimers in interview notes, and memorializing that the *Upjohn* warning was given and that the employee understood the warning, agreed with the terms, and had no additional questions.

## ENCOURAGE GOOD GOVERNANCE PRACTICES

The world's quick adaptation to virtual life should not draw an audit committee, the company, or investigators away from solid good governance practices. Indeed, the new-for-now-normal of extended telework is precisely the time when all stakeholders should redouble their efforts to ensure that the investigative process and oversight governance amplify a company's commitment to reasonable and reliable practices.

Once an investigation kicks off, the auditor and possibly other third-parties will be grading the audit committee and the company's conduct. Properly documenting and executing an investigation includes meaningful, real-time engagement by the audit committee. This can be achieved by providing the committee chair with frequent updates, debriefing the full committee at key junctions, and documenting the full extent of the committee's deliberations and engagement in committee minutes. Overall, the goal is to run a reasonable process with clearly demonstrated integrity that the committee and company can stand behind. Good and thoughtful governance are the keys to achieving that result.

## PRESERVE WORK PRODUCT AND PRIVILEGE WHEN MEMORIALIZING AND REPORTING FACTS AND FINDINGS

Investigators should consider enlisting one or two team members to attend and take notes in all virtual interviews. This can help ensure uniformity of process, which makes investigative teams more efficient and agile, while also mitigating the risk of information silos that are especially likely to arise when teams are geographically dispersed and each team member takes and stores their notes differently.

Interview notes should reflect not only who was present during the interview and that the *Upjohn* warning was provided, but also that the witness stated he or she understood it, had no questions, and agreed to tailored terms—discussed above—designed to protect confidentiality. In addition, interview notes should be watermarked or otherwise annotated to disclaim all protections claimed by the investigative team including work product and privilege protections. As ever, notetakers should be thoughtful about whether and when to include verbatim quotes or otherwise attributed statements because these can become fodder for later discovery requests.

Investigators should be particularly thoughtful about how and to whom they provide reports, and the discoverability of memoranda, Powerpoint

presentations, and other documentary materials. Of course, in any internal investigation, investigators must balance the need to zealously protect privilege and work product while ensuring adequate and complete information is shared with a company's auditor and, in some instances, regulators and law enforcement. Special attention should be paid to the issues raised in *U.S. Securities and Exchange Commission v. RPM International Inc.,* in which the U.S. District Court for the District of Columbia granted a motion to compel by the SEC requiring RPM International to produce interview memoranda prepared by outside counsel investigating on behalf of the company's audit committee. Order on Motion to Compel, *SEC v. RPM Int'l, Inc.*, No. 16-1803 (D.D.C. Feb. 12, 2020); Order at 3-4, *SEC v. RPM Int'l, Inc.*, No. 16-1803 (D.D.C. July 8, 2020), ECF No. 99 (providing the analysis behind the court's order on February 12, 2020, granting the SEC's motion to compel interview memoranda). After investigators reported insights from 19 interviews with Ernst & Young, the company's independent accounting firm, EY in turn provided the SEC its own detailed summaries of those reports. This, the district court concluded, resulted in a broad subject matter waiver of privilege and work product protections. Much is being written on the *RPM International* decision, and it is too soon to tell whether it will be considered an outlier or become prevailing law. Nevertheless, it is a clear reminder that investigators must be intentional about what records and reports they make and provide and with whom they are shared.

Jessica Magee and Michael Stockham are partners, and Sydne Collier an associate, in Thompson & Knight LLP's trial practice, where they focus on securities and white collar investigative and enforcement matters. To learn more about the topics in this article or about their practices, contact them at Jessica.Magee@tklaw.com, Michael.Stockham@tklaw.com, and Sydne.Collier@tklaw.com.