FORENSICALLY PRESERVING ELECTRONIC EVIDENCE DURING A LOCKDOWN

During the COVID-19 lockdowns, how did fraud examiners manage evidence collection? Learn from forensic technology industry experts about collecting custodian information and remote data preservation.

During the height of the COVID-19 pandemic, with extensive travel restrictions in place, a U.S. regulator subpoenaed Prospect Worldwide — a large global manufacturing company with offices in the U.S. and Latin America — to preserve company data related to an investigation. The scope of this data included company-owned computer hard drives, mobile phones, and corporate email and file-server data for more than two dozen company employees (aka "data custodians") who possessed potentially relevant information. (The company name and case details have been changed for this column.)

A local, experienced forensic technology collection team typically would conduct this type of preservation work on-site. However, because of pandemic travel restrictions and social distancing orders, forensic investigators had to perform most of the required preservation activities remotely — often from their home offices. They worked with Prospect Worldwide's IT department and retained outside counsel to apply creative and alternative methods, in cooperation with the data custodians, to facilitate remote connectivity to target data sources.

The forensic investigators needed to preserve and collect data in a legally defensible manner so Prospect Worldwide could potentially present it as evidence in a court of law. So, they had to obtain complete forensic images of the computer hard drives, mobile devices and other

data sources, and maintain full tracking of chain of custody. How did they do it when they couldn't travel, didn't have any on-site IT corporate resources and couldn't work together in person as a team? Read on!

The forensic investigators reviewed and tested multiple solutions from software companies that claimed to perform remote collections, but they concluded that many products are still limited by internet bandwidth speeds and reliability of connections. So, they decided instead to employ a multi-phased approach. Interestingly, the most reliable remote collection method was a time-tested approach that didn't involve new technologies or fancy new tools in the Latin America collection. (However, the investigators used newer technologies in the U.S. remote collections.)

Phase No. 1: planning and identification of data sources

During phase No. 1, the forensic investigators conducted telephone and email

interviews with relevant company stakeholders — those who had business knowledge or a stake in the outcome, such as the legal department, department heads, compliance officers and others — and their outside counsel. The investigators focused on identifying and documenting all potentially relevant data sources from the data custodians' devices plus additional systems and storage locations that required preservation and analysis.

They began by interviewing Prospect Worldwide's IT personnel to understand the inventory of company-issued or otherwise identifiable data assets each data custodian maintained; company authorized-use policies; email and document management systems supported by each location; any data loss prevention solutions or activity logs maintained during the investigation period; on-premises and cloud-based storage platforms supported by each location; and any other communications applications permitted by the company.

The forensic investigators also interviewed data custodians to document the broadest range of computers, mobile devices, personal email accounts, and all other systems and applications that might contain information relevant to the case. The forensic investigators used the information they obtained from the interviews to draft a data preservation plan and collection timeline. They also prepared "remote-collection kits" to send to the data custodians that contained necessary hardware (including encrypted hard drives), software and documentation to collect sound forensic images. The forensic investigators then began to schedule individual remote-collection sessions with the data custodians.

In parallel with the interviews, the investigators worked with Prospect Worldwide's IT personnel to instruct and oversee the self-preservation activities of data within the network infrastructure, including network data and live-server email.

COLUMNIST
VINCENT M. WALDEN, CFE, CPA
MANAGING DIRECTOR, ALVAREZ & MARSAL'S DISPUTES AND INVESTIGATIONS

Phase No. 2: remote data preservation

The investigators shipped one or more forensic remote-collection kits to each data custodian from whom they needed data preservation. Investigators scheduled dates and appointment times for online meetings to perform remote collections. During the appointments, the investigators used collaboration tools (like WebEx, GoToMeeting, Microsoft Teams or TeamViewer) to take control of the data custodians' local devices. Then they used preloaded forensic imaging software on the hard drives in the remote-collection kits to create and verify bitstream forensic images, which would capture mirror images containing exact replicas (bit by bit) of the data stored on each device. Once forensic investigators remotely verified forensic images and the backups of those images, they completed the chain-of-custody documentation associated with the preservations.

Finally, the data custodians shipped the images back to the investigators on the provided encrypted hard drives to ensure the confidentiality of the data during transit.

The investigators made special arrangements with the forensic lab to ensure that it'd be able to receive shipments during the lockdown. The backup image copies remained with the data custodians until the investigators confirmed receipt and readability of the shipped encrypted images. Only then could the data custodians ship the remaining encrypted backup images to the investigators' forensic lab.

Prospect Worldwide's IT personnel preserved and directly transferred corporate data, such as network shares and live-server email, to the forensic investigators' main office via regional secure file transfer protocol (SFTP) maintained in each jurisdiction, or they shipped it to a forensic investigator in their region. Investigators separately and remotely preserved information from personal email and cloud-based storage tools such as Google Drive, Box.com and Dropbox with credentials provided by the data custodians.

The investigators forensically preserved data from multiple countries and fully tracked the chain of custody from each device. They included keyword search and statistical analysis techniques in the information to help them in their review of documents. Prospect Worldwide, after sifting through the data, submitted all relevant documents to the U.S. regulator in time to meet the subpoena deadline. Success!

Phase No. 3: Additional in-house approach

During the planning stages of the engagement, forensic investigators also considered additional approaches that wouldn't require transfer of data outside Prospect Worldwide's IT environment. One such approach was leveraged in the U.S. where the client already had a large cloud-hosted environment.

As the COVID-19 digital transformation and work-from-home initiatives drove organizations to provide access to employees remotely, forensic practitioners were also using remotely accessible environments *within* organizations'

firewalls to conduct defensible preservation of information and rapidly set up virtual investigation and analysis servers.

Rather than take data off company premises, emergent technologies provided all parties (including outside counsel, forensic accountants and other third parties) a comfort level in managing security and privacy risks and obligations. These technologies permitted rapid deployment of virtualized data-analysis servers that share hardware and software resources with other servers performing different business functions. This approach allowed for the remotely imaged data sources to be accessed for analysis within a 24-hour window instead of the traditional five- to seven-day lag associated with shipping the data to a forensic lab.

Is remote data preservation and analysis the new norm?

The above case study demonstrates the practical application of a remote data preservation exercise. John T. Hays, an associate with Eversheds Sutherland (US) LLP, who specializes in complex business litigation, says, "Depending on the requirements of the investigation, remote preservation can capture data from a variety of sources while still maintaining the forensic integrity and chain of custody of the data collected."

As technologies, bandwidth and processes improve, perhaps remote collections or analysis will become the new norm given the social impacts and behavioral changes we'll see from the COVID-19 pandemic. Employees probably will be traveling less, which will save companies money and time. However, with any data preservation, fundamental principles of data integrity and chain of custody are always required. Therefore, organizations typically engage experts in data preservation, rather than traditional IT professionals, for data collection. Whether forensic investigators are physically present with devices or are remotely accessing them, they must obtain complete verified bitstream images, "MD5 hash validations" (which can help ensure that files aren't modified or corrupted during the transfer process), and chain-of-custody documentation to qualify the data for admission as collected evidence into courts.

Questions fraud examiners should be asking

Separate from the obvious travel restrictions that were in place during the COVID-19 pandemic, here are some internal questions that legal, investigative and other anti-fraud professionals should ask when evaluating whether remote preservation can replace physical on-site preservation:

- What are the key data sources forensic investigators need to preserve? Can they target these sources to reduce the scope of the data preservation while still meeting all investigative, evidentiary admissibility and preservation requirements?
- Where are the data custodians located? (An investigation firm might have local forensic practitioners, or it might require extensive travel to physically reach data custodians, which could result in increased costs.)
- If forensic investigators can't access data, are custodians willing to ship their devices even if it means they won't have them for 48 to 72 hours?
- Can an organization's IT department set up a segregated virtual environment online with its firewall (IT environment) for forensic investigators to access remotely?
- Will an organization conduct remote collections with the help of actual data custodians or other representatives, such as family members? Will the organization authorize the procedure?
- Do remote locations have enough internet bandwidth? Are connections stable enough to support screen-sharing and efficient and reliable file transfers?

The answers to these questions, coupled with the urgency of an investigation and the technical wherewithal of data custodians, can determine decisions about the preservation of key data sources. When in doubt, consult a trusted forensic preservation professional to ensure evidence validity during investigation discovery or litigation. ■ FM

Vincent M. Walden, CFE, CPA, is a managing director with Alvarez & Marsal's Disputes and Investigations Practice and assists companies with their anti-fraud, investigation and compliance monitoring programs. He welcomes your feedback. Contact him at vwalden@alvarezandmarsal.com.

The author thanks Andy Antunez and Robert Johnson, senior directors with Alvarez & Marsal's Disputes & Investigations practice, for contributing to this column. Contact them at aantunez@alvarezandmarsal.com and rjohnson@alvarezandmarsal.com. – ed.

