

## Regulatory Investigations

*Proper Steps Must Be Taken to Preserve Discoverable Data*

**BY PAUL J. NEALE  
AND JOHNATHAN BRIDBORD**

As anyone who has been involved in the recent rash of regulatory investigations can attest, many critical decisions are made amidst chaos and panic in a very short period of time. One line of decision-making relates to the steps that will be taken to preserve information. It is an unavoidable fact that, in most instances, a civil class-action litigation will inevitably follow the regulatory matters.

Therefore, the steps taken to preserve information must take into account the long-term discoverability of any relevant information, whether it is ultimately managed and produced in the context of responding to a subpoena issued by the U.S. Securities and Exchange Commission or some other agency.

This is an important fact often overlooked during the initial stages of an internal investigation. However, the ruling in *Coleman Holdings v. Morgan Stanley* (Fla. Cir. Ct. 2005) and other decisions granting sanctions and/or adverse inferences underscore the importance of seeing the forest through the trees.

**Paul J. Neale** is executive vice president and **Johnathan Bridbord** is a senior forensics examiner at DOAR Litigation Consulting.

The first critical step in maintaining control of information is to prepare and distribute a document preservation



memo to the affected employees—if not the entire company. But this can also trigger impulsive document destruction by certain employees who can easily see how central figures in similar regulatory investigations have been fired and in some instance indicted.

If an employee is going to take this risk when the investigation becomes known, there is little that can be done to prevent it up to a certain point.

Along the long line of decision-making often comes a bridge that many executives and legal officers dread crossing—the forensic acquisition of employees' desktop and laptop computers. An even more onerous bridge is the prospect of accessing and acquiring images of employees' home computers.

A forensic acquisition (also referred to as an image) of a hard drive entails using a forensically sound process and system to capture a complete, bit-by-bit copy of the target hard drive. This includes all active files along with unallocated and slack space in which deleted files or fragments of them reside.

Captured by the appropriate person using proper procedures, this image is an evidentiary sound copy of the hard drive because the image maintains all of the files' properties, or meta-data, as it existed on the day of the acquisition.

The forensic acquisition of the computer drives of at least the critical if not all of the custodians of relevant information should be required. Of course, the main concern for any general counsel and executive is the psychological impact that such an "invasive procedure" might have on the employees whose hard drives—almost certainly containing private and confidential information unrelated to the subject matter at hand—will be forensically imaged.

But employees should be told directly what is being done, and when and how it will occur. Furthermore, the message can clearly state that hard drive imaging is being done primarily for document preservation purposes and not with intent to surf through personal information. In fact, a large majority of drives acquired as part of an internal

investigation in response to regulatory actions are usually stowed away for access if and when the need arises.

Circumstances within one such investigation, however, underscore the importance of forensically imaging hard drives. In this case, during questioning of an employee by counsel in the early stages of an internal investigation, the employee admitting deleting pertinent files once he became aware of the New York attorney general's subpoenas. The company had sent out preservation memos making it clear that such information needed to be retained.

The employee stated that he deleted folders of files relating to specific company clients. Having forensically imaged the employee's hard drive, it could be determined specifically when the files were deleted. It could also be concluded that the files had originated in his company e-mail account, which was backed up in accordance with the company's document retention policy.

Therefore, it was possible to restore copies of the deleted folders and files, and provide the regulators with documented procedures to show that the proper steps had been taken and that the company was in compliance.

Attempts to perform covert or "black bag" drive acquisitions to avoid employee awareness almost always backfire. First, the proliferation of laptop computers makes just about any employee, particularly executives and those in business development roles, mobile. Therefore, it becomes a logistical nightmare to obtain access to those computers.

Second, someone inevitably gets wind of the process and word quickly spreads throughout the organization regardless

of the size of the company. The perception that the company is trying to discreetly obtain employees' information puts workers in a defensive position that could promote document destruction as opposed to preventing it.

The approach to obtaining images of employee computer hard drives should

---

*Captured by the appropriate person using proper procedures, a forensic acquisition is an evidentiary sound copy of the hard drive because the image maintains all of the files' properties, or meta-data, as it existed on the day of the acquisition.*

---

be to set up a convenient location within the company for employees to drop off their computers. The imaging process can typically be accomplished within one to two hours.

This may provide the investigative team with the perfect opportunity to interview the employee as part of their investigation. If a large number of computers need to be processed, it may warrant telling employees to drop their computers off at the end of a day and have multiple drives imaged overnight so the computers are available the next business morning. In the end, implement a process that causes the least anxiety and prevents significant disruption to the business.

While forensically imaging hard drives may in most instances be strictly a preventive measure, there are other tangible benefits. The obvious one is

that to the extent relevant data is likely to be stored on local workstations, it has been preserved and can be accessed at some later point. Also, you will be in a position to quickly show regulators, and later plaintiffs' counsel, that you have taken every reasonable step to avoid the accidental or purposeful spoliation of information that may have been relevant.

Although backup tapes have garnered the most attention in the relevant court rulings, data residing on local workstations that are not backed up by the company's central archive systems is equally susceptible to the same pitfalls of spoliation. The opportunity to preserve this information presents itself early and every day that passes increases the risk that data will be destroyed.

As the law evolves, companies and their counsel are being held to a higher standard to properly manage and preserve electronic information. The failure to do so can have—and has had—severe and costly consequences.

This article is reprinted with permission from the April 26, 2005 edition of the NEW YORK LAW JOURNAL. © 2005 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information, contact American Lawyer Media, Reprint Department at 800-888-8300 x6111. #070-04-05-0036