DIGITAL FORENSICS

Star Employee Left? How Preemptive Collections Reduce Risk and Improve Case Outcomes

 Lars Daniel, EnCE, CCO, CCPA, CIPTS, CWA, CTNS, CTA

12 September 2024

The following scenario is all too common.

A high-powered employee leaves a company. Months later, the company suspected that the employee stole sensitive data on the way out the door because the CFO noticed a meaningful revenue reduction from the accounts the employee was responsible for.

Unfortunately, that employee's laptop, desktop, and company phone have all been wiped and reissued to new employees. The evidence of potential wrongdoing is gone, as is the company's recourse against the former employee.

As a digital forensics expert with years of experience in high-stakes litigation, I've seen firsthand how the evidence landscape has shifted dramatically in our digital age.

Today, I want to discuss a critical strategy that can make or break a case: pre-emptive collections. This approach is not just about being prepared; it's about safeguarding your client's interests and ensuring the integrity of digital evidence from the outset.

Pre-Emptive Collections

When I say "Pre-emptive Collections," I refer to the proactive gathering and preservation of digital evidence before a specific incident or legal action occurs. Think of it as creating a time capsule of digital information - capturing a snapshot of data in its original, unaltered state.

Why are pre-emptive collections so important?

The answer lies in the nature of digital evidence itself. Unlike physical evidence, digital data can be altered, overwritten, or deleted with a single click, often without leaving a trace. Normal business operations, automatic system updates, or even intentional data destruction can compromise critical evidence before you even know you need it.

The benefits of the preemptive collection approach are manifold. First and foremost, it protects against spoliation - the destruction or alteration of evidence. Courts take a dim view of parties who fail to preserve relevant evidence, and the consequences can be severe. Negative inferences, adverse jury instructions, or even case-dispositive sanctions can result from spoliation.

Moreover, pre-emptive collections can save time and resources in the long run. By securing data early, you avoid the frantic scramble to gather evidence after a complaint is filed. This not only ensures a more comprehensive collection but also allows for a more strategic approach to case planning.

But perhaps the most compelling arguments for pre-emptive collections are made by recounting cases where this approach wasn't taken.

Case Example: The Non-Compliant Corporate Client

I was brought into a civil litigation case on the defense side, tasked with collecting electronic data. Unfortunately, we were engaged late in the process, not due to any fault of the attorney, but because the client - a Canadian company facing litigation in U.S. Federal court - had underestimated the need for forensic experts. They believed their IT department could handle all collections in-house.

This misconception coupled with the client's view that the discovery requests were overbroad, led to a cascade of complications. The company's executives, unfamiliar with U.S. discovery obligations and harboring privacy concerns common in Canadian business culture, were openly hostile to the process. I witnessed this resistance firsthand during conference calls, during which I attempted to explain, alongside the attorney, the importance of complying with court orders.

Initially, we aimed for a targeted collection of specific cloud and server data. However, the client's non-compliance escalated the situation dramatically. The judge, frustrated by the delays and resistance, ordered the most comprehensive data collection possible.

This expanded scope included full forensic acquisitions of all personal and work devices for the custodians, including the recovery of deleted data, as well as complete captures of server and cloud data.

What could have been a straightforward case with simple data collection taking a few days turned into a multi-month ordeal. The costs skyrocketed, the client's credibility with the court was damaged, and the case strategy had to be completely overhauled in light of the expansive data now available to the opposition.

All of this could have been avoided with a pre-emptive collection approach. You see, the attorneys for the company had consulted with us pre-litigation and understood the need to protect the relevant data in case of future litigation. They instructed the company's IT department to preserve important backup data.

However, the IT department failed to do so, and the backup data for the relevant time period "rolled over" and was deleted automatically by the backup system software. All because the IT department did nothing to preserve the data within a year, the amount of time backups were retained before automatic deletion.

Implementing a Pre-Emptive Collection Strategy

Implementing a pre-emptive collection strategy does require some upfront investment in terms of time and resources. However, the long-term benefits far outweigh these initial costs.

Not only does it protect against spoliation claims and negative inferences, but it can also significantly streamline the discovery

Not only does it protect against spoliation claims and negative inferences, but it can also significantly streamline the discovery process.

Rather than scrambling to gather relevant data after a lawsuit is filed, attorneys and their clients can focus on building their case strategy, knowing that critical evidence has already been secured.

Yes, pre-emptive collections work as a shield, but is also can be a sword. For example, collecting and protecting the data from a departing employee's devices gives you the opportunity and ammunition to go after potential wrongdoers with facts, as well as to combat unsubstantiated claims with actual evidence.

While the specifics on how to properly do pre-emptive collections depend on the case type and the electronic evidence items involved, the principles are the same. Here is an example of how it could be done for a departing employee.

Identify Data Sources

The first step is to identify all potential data sources relevant to the departing employee. Identifying these data points ensures that no critical information is overlooked in the preservation process. Every platform or device the employee uses could hold vital evidence, so comprehensive coverage is key.

- Work computers and external storage devices
- Company-issued mobile devices
- Email accounts, including archives
- Cloud storage accounts like Google Drive or OneDrive
- Collaboration platforms such as Slack or Microsoft Teams
- Network drives and shared folders
- Backup systems

Create Forensic Images

Once the data sources are identified, the electronic devices should be forensically imaged (copied). Creating forensic images preserves the data in its original form, preventing accidental overwrites or alterations during the examination phase.

Document the Preservation Process

The entire preservation process should be meticulously documented to ensure legal defensibility. Clear documentation is critical for later validating the authenticity and integrity of the preserved data in court. Ensure that you are:

- Maintaining detailed logs of all preservation actions.
- Recording the chain of custody for all data and devices.
- Noting any issues encountered during the preservation process.

Secure Storage of Preserved Data

Once the data is collected, it must be securely stored to ensure its integrity. Securing the data prevents unauthorized access or accidental loss, preserving its value as evidence. Since we ensured the custodian's data was preserved as forensic images, the evidence was tamper-proof due to the digital DNA the data received as part of the forensic image creation process.

While secure storage might not be needed to prove the data is reliable due to the digital DNA, it does allow you to show that no one accessed the data after the forensic images were created.

- Storing forensic images and data in a secure, access-controlled environment.
- Creating redundant backups of all preserved data.
- Implementing encryption for sensitive information.

Conclusion

The lesson here is clear: in today's digital landscape, waiting until litigation is imminent to consider data preservation is a risky gambit. Pre-emptive collections, guided by digital forensics experts, are not just a best practice—they're a necessary safeguard against the pitfalls of modern litigation.

Don't get caught with a surprise case only to learn the evidence you need is gone. Spending the time and money to create a preemptive collections plan can save an organization money in the long run on litigation, antacids, and aspirin.

ABOUT THE AUTHOR

Lars Daniel, EnCE, CCO, CCPA, CIPTS, CWA, CTNS, CTA

Practice Leader

Digital Forensics

Mr. Lars Daniel is the Practice Leader of the Digital Forensics Division. Mr. Daniel has qualified as an expert witness and testified in both state and federal courts, qualifying as a digital forensics expert, computer forensics expert, cell phone forensics expert, video forensics expert, and photo forensics expert. He has testified for both the defense and prosecution in criminal cases and the plaintiff and defense in civil cases.