

NAVIGATING EDISCOVERY CONCERNS WHEN INVESTIGATING A FORMER EMPLOYEE'S DEVICES FOR POTENTIAL TRADE SECRET MISAPPROPRIATION OR OTHER MISCONDUCT



Joshua Hummel

Employee terminations can pose many challenges, but what should organizations do when investigating whether a recently terminated employee transferred or copied large amounts of proprietary information before turning over their devices? The recent case of *CaramelCrisp LLC v. Putnam*, 2022 WL 1228191 (N.D. Illinois Apr. 26, 2022), highlights several potential eDiscovery pitfalls that could arise when a company is not careful in how it searches, analyzes, and images a former employee's devices.

On March 7, 2019, CaramelCrisp, which sells gourmet popcorn under the name “Garrett Popcorn Shops,” terminated the defendant, its Director of Research and Development, for reasons not at issue in the case.

Following her termination, as per standard practice, the company's Senior IT Analyst began inspecting the defendant's laptop and allegedly discovered that two days before her termination, the defendant emailed herself vast amounts of confidential information and trade secrets, including the company's secret popcorn recipes, pricing and supplier information, production processes, development and distribution agreements, and market research. She allegedly copied more than 5,400 files onto a personal USB drive and deleted “substantially all of the data on her computer,” including the trash and recovery folders.

On March 22, 2019, the company's Vice President of Human Resources emailed the defendant accusing her of emailing herself confidential documents before her termination and claiming that she had violated her employment contract. On that same date, the company also began internal discussions concerning the possibility of implementing a litigation hold.

The defendant hired counsel and provided an affidavit representing that she deleted any copies of the company's information, but she declined to allow the company to forensically review her personal electronic devices, email, and cloud accounts. The parties later agreed that the defendant would make her personal devices available to a third-party forensic expert.

Although the third-party expert created a forensic image of the defendant's personal devices, he apparently did not conduct an analysis of the defendant's work laptop searched by the company's IT analyst, nor did the third-party expert offer any opinions concerning the defendant's activities on that computer.

On April 22, 2019, CaramelCrisp filed its complaint, alleging that the defendant misappropriated trade secrets and breached her employment agreement.

The defendant's forensic expert did analyze an image of her work laptop, however, and concluded that CaramelCrisp failed to use “best practices” when working with the computer

NAVIGATING EDISCOVERY CONCERNS WHEN INVESTIGATING A FORMER EMPLOYEE'S DEVICES FOR POTENTIAL TRADE SECRET MISAPPROPRIATION OR OTHER MISCONDUCT

PAGE 2



during the two weeks after her termination, “which irreparably altered the laptop so that it no longer reflected its original state.” Specifically, the defendant’s expert contended that CaramelCrisp: (1) failed to initially preserve the device and its contents at the time of the original collection; (2) accessed or changed approximately 39,000 files after her termination; (3) continued to log in under the defendant’s account when accessing the laptop; and (4) failed to take steps to mitigate a “garbage collection” process.

Concerning the last issue, the defendant’s expert described “garbage collection” as a “process unique to solid-state disks that sets all values of its unused areas to a specific value, resetting it to hold new contents in the future,” which “has the unfortunate effect of rendering previously deleted data unrecoverable.” In other words, according to the defendant’s expert, the “more [the] host device is used, the more likely garbage collection is to occur, or reoccur” because continuing to power a device on and off essentially flushes out or changes old data. Thus, by failing to first image the laptop and mitigate the “garbage collection” process, the defendant’s expert claimed, CaramelCrisp effectively deleted hundreds of files from the laptop after the defendant’s termination, rendering them and other evidence from the computer irretrievably lost.

Claiming that CaramelCrisp therefore spoliated evidence, the defendant moved for sanctions under FRCP 37(e), seeking various sanctions including dismissal of the case, the imposition of an adverse inference jury instruction at trial, a bar on the company’s introduction of testimony concerning the laptop, and/or an award of attorneys’ fees and costs.

In denying the defendant’s motion, the court held that the company’s duty to preserve evidence did not arise until March 22, 2019, when it contacted the defendant asserting its claims and began having internal discussions concerning a litigation hold. Because the evidence was lost before the duty to preserve arose, the court found that sanctions were not warranted.

The court did note, however, that the defendant had preserved her challenge to the reliability of the forensic image of her work laptop and that she could potentially still pursue a motion *in limine* before trial to preclude CaramelCrisp from relying on the image of the laptop because it was no longer a reliable copy and was therefore inadmissible. The court further observed that at trial, the defendant could present evidence regarding the company’s deletion of files and pursue her argument that the image of her work computer “‘carries no weight’ because CaramelCrisp altered electronic data by failing to follow best practices.”

Thus, although the company avoided sanctions for spoliation, it will likely still need to address admissibility, reliability, authenticity, and weight-of-the-evidence challenges regarding the information allegedly found on the defendant’s computer, undoubtedly making its claims more difficult to prove.

What can companies take away from this case?

1. **Determine whether there is a “reasonable anticipation of litigation” before investigating a recently terminated employee’s computers or other devices.** As noted by the court in *CaramelCrisp*, the mere

NAVIGATING EDISCOVERY CONCERNS WHEN INVESTIGATING A FORMER EMPLOYEE'S DEVICES FOR POTENTIAL TRADE SECRET MISAPPROPRIATION OR OTHER MISCONDUCT

PAGE 3



termination of an employee does not necessarily trigger an employer's duty to preserve ESI or implement a litigation hold. In some cases involving a terminated employee, however, there might already be a "reasonable anticipation of litigation" when the company starts to examine that person's computer, cell phone, or other device(s). Had those facts existed in *CaramelCrisp*, the court could have easily found that the employer breached its duty to preserve, warranting spoliation sanctions. Therefore, before examining an employee's devices, companies should consider whether a "reasonable likelihood of litigation" exists and whether a litigation hold and appropriate safeguards are in place to preserve relevant evidence.

2. **Be mindful of what happens to a device when it is inspected for suspicious activity, and proceed cautiously.** The defendant's forensic expert noted that frequent activity on a device, including simply turning it on or off, can reorganize and effectively delete old data, resulting in authentication issues or even the complete unavailability of critical information. If an employee is already suspected of misappropriating trade secrets information or other improper activity, consider forensically imaging their device(s) first to ensure that the evidence is preserved and nothing is changed or lost. Also, consider starting an investigation by first searching other sources of information that are backed up and not as susceptible to alteration or deletion (such as company email accounts) to determine if there are any indicators of suspicious activity, before turning to the employee's computer, USB drives, or other devices.
3. **It is important to have policies and processes in place to detect improper use of company trade secrets and other proprietary information.** CaramelCrisp had processes in place to check the emails and devices of terminated employees, allowing it to promptly detect potential trade secret misappropriation and take swift action. These measures can be very helpful in preserving evidence and in responding promptly to, or perhaps even avoiding, a potential loss of sensitive information.

For additional information on this topic, please contact **Joshua Hummel** at jhummel@@redgravellp.com.

The views expressed in this article are those of the authors and not necessarily those of Redgrave LLP or its clients.

Redgrave LLP is one of the largest legal practices focused exclusively on addressing the legal challenges that arise at the intersection of the law and technology, including eDiscovery, information governance, and data privacy. We employ some of the most experienced professionals in the field. We provide clients with practical, innovative, and cost-effective solutions and serve Global and Fortune 500 companies across a diverse array of industries. We also work collaboratively with Am Law 100 law firms in roles ranging from co-counsel to consulting and testifying expert witnesses and have appeared in state and federal courts throughout the United States.