CASE STUDY

ARCHERHALL

Digital Forensics Investigation for Plaintiff's Attorney in Wrongful Termination

The Situation

The Plaintiff was a cashier who was terminated after she reported to HR that she had been the target of extremely inappropriate behavior from her Supervisor. She reported that he made lewd comments and that twice he had pressured her into sexual intercourse. Plaintiff's Attorney filed a complaint on her behalf alleging that the defendant employer had failed to prevent sexual harassment and had retaliated against and wrongfully terminated Plaintiff.

ARCHERHALL
AIM HIGH

We are a leading provider of computer forensics and e-discovery services for businesses and law firms nationwide. We don't take chances with your data when litigation is a possibility,and proper handling is critical.

The Challenge

The wrangling over discovery began almost immediately. At issue was the Supervisor's personal computer. Plaintiff's Attorney wanted to have an ArcherHall digital forensics expert examine the computer data for communications between Plaintiff and Supervisor. Defense Counsel had produced some responsive data, but Plaintiff's Attorney knew that certain communications would be harder to get. These included deleted photos, videos, and messages, and app-based communications, such as Facebook Messenger and Viber.

The Solution

ArcherHall had forensically collected the data from Plaintiff's phone as well as from an iPod Touch, which Plaintiff said she had used to communicate with her Supervisor. Out of frustration or embarrassment, Plaintiff had deleted most of these messages. ArcherHall was able to recover enough messages to show that relevant communications had occurred between Plaintiff and her Supervisor on Supervisor's personal accounts. This increased the strength of the Plaintiff Attorney's argument that the Supervisor's personal computer should be made available for a full forensic examination to capture a more complete record of those communications, including metadata.

The Outcome

To address Defense Counsel's objections, ArcherHall used a Triangle Agreement. This document provided a clear protocol for the examination of the computer that balanced the need for relevant data against the Supervisor's privacy. ArcherHall forensically examined the computer and captured all data which met certain criteria agreed to by the Parties. ArcherHall then provided this data to Defense Counsel to review for privilege. ArcherHall then provided the non-privileged data and a privilege log to Plaintiff's Attorney.

Key Success

The result of ArcherHall's work was relevant messages, photos, and videos—many deleted—which otherwise Plaintiff's Attorney may not have had access to. The case settled shortly thereafter.