Human Resources | Sample Cases

The following descriptions highlight a variety of matters for which Vestige has been retained. Each of these cases are real matters that we have worked, but for privacy and confidentiality purposes the identifiable information has been sanitized. These cases are not the entire population of cases matching such criteria, but instead represent a wide sample of the cases we have worked that are specific to HR. Should you need additional information, please contact us.

DIGITAL FORENSICS | Intellectual Property Theft:

Health Care Recruiter v Former Employee | **Client Data**

Vestige represented a health care recruiter (Plaintiff) in a case that involved a former employee (Defendant). The former employee was well known in the industry and took a mobile device containing contacts belonging to the Plaintiff upon leaving employment. The former employee was accused of contacting the contacts contained in the mobile device. The former employee admitted to taking the mobile device, but claimed that only a few of the contacts had been contacted. The former employee printed off a list of the contacts and gave it to our client claiming that was all she possessed. Mysteriously, the mobile device disappeared in a freak lake incident and the court considered it "lost". As relief for this "freak accident", Plaintiff won their motion to compel and Vestige imaged the former employee's home computer and cross referenced the contacts with the phone records of the former employee's cell, home and business line. Comparison of the acquired data with the original list revealed there was an excessive amount of contacts not originally provided to the health care recruiter by the former employee. More importantly, Vestige established a pattern of communication that the former employee was using to contact clients from the list. Needless to say, the health care recruiter was very happy with Vestige's work.

■ ■ ■

Mortgage Company v Individual | **IP Theft**

Vestige represented a mid-size mortgage company (Plaintiff) against an individual (Defendant) accused of IP theft. The individual was running a branch office in another state for the Plaintiff. During this time, the individual conspired to join a competing mortgage company. Armed with a plan, this individual began stealing client lists and proprietary information from the Plaintiff's company. After the material was taken, the individual would then delete the data off the Plaintiff's server. Most of the information was being taken through the exchange of e-mail between the individual's corporate account and a personal Yahoo! account. Vestige analyzed the branch office computers and the individual's home computer. Vestige discovered that the individual had installed an application called "Windows Washer." The individual claimed that the application was used to improve performance, which was in contrast to its obvious function of data wiping. Vestige provided expert testimony during both the preliminary injunction and motion for contempt hearing. Vestige was able to pinpoint when the individual had used the program and that the individual had changed the default settings in Windows Washer to achieve a deeper cleanse, such as selectively erasing certain files and activating the automatic cleaning setting. Despite the individual's attempt to erase data, Vestige still managed to find artifacts left behind by the application. Vestige's client, the Plaintiff, was granted a preliminary injunction. Testimony was so impressive that Vestige received subsequent referrals from the **opposing** expert and the **opposing** attorney.

■ ■ ■

Chemical Manufacturer v Employee | **Undercover Competitor**

A manufacturer of a patented chemical discovered that their Vice President of Sales was simultaneously working for a competitor. The manufacturer (Plaintiff) filed a temporary restraining order for violation of a non-compete agreement. The Defendant was pro se (representation without a lawyer) and his defense to the court order demanding a forensic examination was that he "routinely used information scrubbing software" to protect private and confidential information, including the manufacturer's own proprietary information. The Defendant claimed that he had in fact installed these processes years before the present litigation. Oddly enough, the Defendant simply failed to attend hearings or the trial and received default judgment in the home state of the manufacturer. In an attempt to circumvent the default judgment, the Defendant filed bankruptcy in his state of residency. Throughout a one year process, the manufacturer chased the Defendant in bankruptcy court and finally got an order to conduct a forensic examination on his computer. Vestige discovered that the Defendant had not only failed to stop the destruction process, but instead had installed the disk scrubbing software the afternoon that the judge ordered the turnover of the computer. This was contrary to his original claim that the software was being used routinely before any of the litigation matters became apparent. The end result was a $400,000 judgment non-dischargeable debt in bankruptcy court in favor of Vestige's client.

Biomedical Engineer Company | **Mass Deletion Cover-Up**

A biomedical engineer company terminated its Chief Science Officer due to an undisclosed reason. Upon return of the company's computer equipment used by the former CSO, the company discovered mass deletion and turned to Vestige for recovery of that information. Vestige was able to recover the deleted data and determined that a significant amount of relevant data had been deleted prior to its return. After reviewing and analyzing the recovered data, Vestige later discovered that the reason for mass deletion was to cover up a year long process whereby the former CSO had been establishing a competitive business for his own personal gain. Vestige was able to assemble an entire timeline and series of meetings that the CSO had with investors for this scheme. Vestige also uncovered patent infringement designs as well as direct inclusion of the company's intellectual property into the plans and product design of the CSO's competing venture.

DIGITAL FORENSICS | Fraud | Embezzlement:

Foreign Owned **U.S. Subsidiary**

This non-litigation matter involved a U.S. subsidiary wholly owned by a foreign company. The foreign company suspected that the subsidiary's General Manager and others were embezzling money. A group of officers from the foreign company flew to the United States. A team consisting of Vestige analysts and a forensic accounting firm met with them and began working immediately upon arrival to the U.S. subsidiary's location to investigate. Vestige preserved, collected and performed a fraud investigation on 25 computers. Vestige discovered that the GM was running a competing business while simultaneously employed by the foreign company. The GM was using several of the company employees, some of the management and the assets of the company for his own personal gain. Primarily high-dollar inventory, intended to be used for sales, was being rented out for side jobs. A 50,000 sq. ft. warehouse, separate from the parent company operation, was used to stage all the equipment that was going out and coming in from rentals. Total fraud amounted to approximately $6 million and was achieved through a variety of fraud schemes: check kiting, ponzi, inappropriate use of assets, false vendors, false contracts, revenue hiding and inappropriate expense recognition. As a result, management and involved individuals were removed, improved controls were put in place and guilty individuals were made to pay restitution.

Large Corporation | **Internal Audit**

Vestige assisted a large corporation in performing an internal audit. The corporation wanted to go public, but suspected upper management might be inflating the value of the company for its own personal benefit. Vestige was hired to examine the system and run searches in which the data results would be turned over to a forensic accounting firm. Vestige was able to gather information and process it quickly. This resulted in the exposure of foul play and saved the company from a botched IPO.

Individual | **Fictitious Vendors and Invoices**

Vestige was hired by a forensic accounting firm to assist in the investigation of an individual that allegedly embezzled close to $3 million. A subsequent investigation confirmed that approximately $3.2 million was embezzled through the use of both fictitious vendors and invoices to these vendors. Vestige was hired to examine the financial systems, the accounting department's operations and the correspondence amongst other individuals within the company to determine the extent of collusion. Vestige helped show that it was a single individual placed in a position of power with a lack of internal controls that resulted in the $3.2 million loss. The client was made whole through the proceeds of its insurance policy.

DIGITAL FORENSICS | Document Alteration:

Individual v Large Manufacturer | **Wrongful Termination**

Vestige was involved in this employment dispute (alleged wrongful termination) as a computer forensic expert to assist counsel and their client in determining whether disciplinary documentation had been altered ex-poste facto of the incident. Considerable testing and validation of the particular document was undertaken by Vestige to validate that while the document had been altered after the termination date, that the information that had specifically been altered was consistent with the employer's sworn testimony.

DIGITAL FORENSICS | Opposing Expert Validation | Critique:

Individual v Mid-size Company | **Wrongful Termination**

Vestige represented an individual (Plaintiff) against a mid-size company (Defendant) involving a wrongful employment termination matter. Vestige was hired to prove or disprove that the Defendant was thorough in its response to discovery requests from the Plaintiff. Vestige found that the Defendant was not thorough enough in its discovery as information was deleted, new computers were purchased, data was disguised and other storage devices were withheld. Vestige successfully defended its process in multiple hearings and won its client a $250,000 sanction and the Defendant's pleadings were stricken as punishment. Vestige's client was provided a favorable outcome that set up a court hearing for multimillion dollar damages.

CYBERSECURITY | Data Breach | Incident Response:

Financial Services Firm | **Data Privacy Breach**

Vestige was engaged by a new client when they were notified by one of their customers that some of the customer's Personally Identifiable Information (PII) was discovered during a routine Google search. The Financial Services firm verified that proprietary, private data appearing to originate from itself was in fact being indexed by Google and still available by following the Google search link. The initial assessment by the Financial Services firm was that 3.5 million records were likely breached, but they did not know how. Vestige's Rapid Response Team swung into motion, forensically preserving the affected infrastructure, forensically analyzing the memory and storage of the organization and successfully identifying the attack vector. Vestige worked with the company's InfoSec individuals to ensure that the attack vector was removed, identified and cleared any additional back-door entry points and then worked hand-in-hand with the Financial Services legal team to turn attention to other major aspects of a Breach Response. At the forefront of this was identifying which records had been (or were likely) compromised to coordinate notification efforts. Through our forensic analysis we were able to prove that a large fraction of the records (all but 60,000 records out of 3,500,000+) were actually compromised and further to show that of the 60,000 records, only 11,000 contained PII necessitating notification. A matter that could have resulted in significant impact – including putting the Financial Services firm out-of-business, while still costly for the organization, ended up being a fraction of the cost because Vestige was able to Forensically prove what data had and had not been compromised.

Mid-size Corporation | **Internal Investigation**

The original owner of the corporation had been reduced to a minority shareholder and was no longer on the Board of Directors; however, the owner continued to have knowledge of what occurred at subsequent Board meetings and would send e-mails with questions related to information exchanged at these meetings. The corporation initiated an internal investigation and hired Vestige after it grew suspicious that information was being leaked out to the original owner by someone on the inside. The corporation suspected that the information was somehow connected to their IT staff member. Vestige performed covert forensic analysis after-hours without IT's knowledge. Vestige not only uncovered that the IT staff member was leaking information, but that this particular IT staff member had a felony record surrounding identity theft. During our investigation, Vestige discovered that this individual's Outlook database had a contact record for everyone in the corporation along with their social security number and other information that would aide in identity theft. Vestige gave a suggestion on how to remove the individual and minimize the IT's access. Vestige used its resources and expertise to stop a small problem from unknowingly becoming a big problem.

Former Employee | **"Time Bomb" Threat or False Fear**

In this matter an employee was terminated by his employer. This individual worked as a network engineer and had a troubled past. After being terminated, the individual began shopping for a job and used a recruiter to aid in the process. The recruiter successfully landed him a new job. While working for his new employer, the same individual began bragging to some of his fellow co-workers of his mastery of computer hacking. The individual further claimed he had placed multiple "time bombs" on his former employer's computer systems. Word began to spread of these claims in his current department. Upper management decided they no longer wanted the individual and talked to the original recruiter. Upper management also requested that the recruiter notify the former employer of these claims. Ironically, the former employer was having system problems and became suspicious that the "time bomb" claims by the individual were legitimate. Vestige investigated the issues and found out the former employer had not implemented any "time bombs" on their system. The problems experienced by the former employer were actually due to the deterioration of their system infrastructure. Vestige was able to extinguish the former employer's fears and suggested a redesign of their infrastructure, advised on the importance of separation of duties and referred the former employer to a competent networking company to solve their systemic issues.