Digital Forensics | Intellectual Property Theft

The following descriptions highlight a variety of matters for which Vestige has been retained that involve alleged IP Theft. Each of these cases are real matters that we have worked, but for privacy and confidentiality purposes the relevant 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 in this specific area. Should you need additional information, please contact us.

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.

Small Business v Individual | **IP E-mails**

Vestige represented a small roofing business (Plaintiff) against an individual (Defendant) involving an IP theft matter. The individual wanted to create a competing roofing business. Vestige found some e-mails in regards to the data that was being taken. The individual subsequently crafted excuses that such e-mails discontinued on a certain date and further claimed that these e-mails containing IP were never opened for viewing. Vestige uncovered that the individual did in fact examine and open the e-mails containing IP.

Small Company v Smaller Company | **Protective Order for Client Data**

Vestige represented a small company (Plaintiff) against a smaller company (Defendant). The Plaintiff had hired the Defendant, who was technologically savvy, to create a database. In order to create the database, the Defendant had to have access to all of the Plaintiff's client information to populate the database. Coincidently, one of the Defendant's ex-employees was also an ex-employee of the Plaintiff. This two-fold ex-employee pair informed the Plaintiff that the Defendant was bragging that he was going to steal the data. The Plaintiff subsequently got a temporary restraining order and an order from the judge allowing Vestige to image all the Defendant's computers the next morning. Vestige was able to move fast and craft a protective order that allowed for the requesting party's expert to review data from the producing party's computers while simultaneously protecting privilege.

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.

Small-Mid Company | **IP Theft**

A small-mid size company (Plaintiff) had accused an individual (Defendant) of IP theft. A temporary restraining order was issued against the individual for the potentially stolen information and the accusation that a defragmenting application was being run to possibly overwrite the hard drive. Vestige represented the individual. Vestige imaged the individual's Macintosh home computer and was able to prove no malfeasance had occurred. Vestige then reviewed the individual's work computer and the opposing expert testimony. Many of the conclusions that the opposing expert documented were in contrast to what Vestige concluded. Vestige was able expose many holes in the opposing expert's testimony. Vestige showed that the opposing expert was just plain wrong in some cases and had stretched the truth in other areas.

Large Financial Institution v Small Financial Services Company | **Large IP Theft**

An IP theft case was brought before a civil court. Vestige represented a large financial institution (Plaintiff) against a small financial services company (Defendants) accused of stealing proprietary information. The Defendants were comprised of a group of former employees that used to work for the Plaintiff, but had decided one day to quit and start up a new competing business. The former employees claimed they only took things that they were allowed to take. Vestige was given the task of imaging a large amount of data—imaging all the work computers used by the Plaintiffs, all the work computers used by the Defendants and all the home computers of the Defendant's main players. Complicating matters was the fact that the Plaintiff's computers (approximately 30-40) were encrypted. Despite this hurdle, Vestige was able to handle an enormous amount of data in a timely matter (several days) and discovered enough evidence for Vestige's client. In the face of the Vestige's thorough and damaging analysis, the Defendants decided to settle.

Large Company v Small Company | **Former Employee - USB Drive**

Vestige represented a large company (Plaintiff) against a small company (Defendant) in an IP theft matter. The Defendants were comprised of former employees who were previously employed by the Plaintiff but decided to leave. One employee, who originally wished to remain employed by the Plaintiff, later decided to leave. Vestige's client, the Plaintiff, discovered that this individual had taken some information on a USB drive. Vestige received the individual's work computer and USB drive at about 10:00 a.m. A conference call was made by 4:00 p.m. the same day to discuss the findings. Vestige discovered that the USB drive given to the Plaintiff was not the drive used to take the data. It was determined that there were other drives used to take data. Vestige exhibited an ability to do analysis quickly and expose multiple sources of the stolen data. The outcome was that the client got the data back and diffused a potential deal-breaking situation.

Manufacturer v Competitor | **Two-Faced Employee**

Our client, a U.S. based manufacturer discovered through a local newspaper that a tax abatement was granted to one of its international competitors in an abutting community. Upon researching this development further, the manufacturer learned that the person heading up the foreign company's U.S. entry was our client's own Vice President of Sales and Marketing. Following the termination of the VP of Sales, Vestige was immediately brought in to investigate the extent of competitive information that was funneled to the foreign company. An investigation by Vestige revealed that significant amounts of proprietary and intellectual property were given to the foreign company. Some of the competitive information that was removed included: U.S. and European pricing, supplier contacts and preferential pricing, client lists, marketing plans and operational manuals. In addition to this, the VP of Sales was steering existing business away from the U.S. company to the foreign competitor. The matter resulted in the foreign company having to pay restitution for the VP's past year's salary. The foreign company was also required to return all intellectual property; it was permanently banned from competing in the U.S., and the former VP was permanently banned from working in the industry.

Dental Practice v Former Owner | **Non-Compete**

Vestige represented a dental practice (Plaintiffs) against its former owners, husband and wife (Defendants). The husband was a dentist who sold his practice to the current Plaintiffs. He continued working under the new ownership for awhile, but later decided to leave. His wife remained for a period of time after he left. The Plaintiff subsequently noticed that many of their patients stopped coming and found out the Defendant (the husband) went to work for another dental practice. Non-compete provisions were included as part of the sales agreement between the Plaintiff and Defendant. The Plaintiff requested that Vestige image the Defendant's computer at his new office where the patients' database was contained. Despite the fact that the database was unique and uncommon, Vestige was able to successfully pair up all patient data between both dental practices of those that received treatment and paid. The client was able to use this info along with the assistance of a Forensic Accountant Firm in the arbitration hearing to calculate a damage value for each customer lost. The Plaintiff won as a result of Vestige's unparalleled services.