McCann
INVESTIGATIONS
Information | Insight | Influence

Case Study: Enforcing a Non-Compete Agreement

McCann
INVESTIGATIONS
Information | Insight | Influence

Company Profile

McCann Investigations is a full service private investigation firm providing complete case solutions by employing cutting-edge computer forensics and traditional private investigative tools and techniques. For 25 years, McCann's investigators have worked in the public and private sector encompassing law enforcement, physical and electronic security and computer forensics.

McCann works with law firms, financial firms, private and public companies and individuals in cases including contentious divorce, child custody issues, fraud, embezzlement, spyware/malware detection, civil and criminal background investigations, and due diligence.

McCann Investigations tools include:

- Computer Forensics
- Mobile Device Forensics
- Spyware/Malware Detection
- Network Breach Detection
- Digital Debugging
- IT Network Vulnerability Assessments
- Background Investigations
- Under Cover Work
- Surveillance
- Corporate Intelligence
- E-Discovery

Business Situation

The United States oil and gas industry has a dominant presence in the Houston area. As a result, Houston has the highest number of Fortune 500 companies second only to New York. Because of the dense concentration of companies in the Houston area who are focused on the oil and gas industry, competition becomes fierce and protection of intellectual property rights are paramount to a company's success. Most companies have strict non-compete agreements in place with employees to ensure the protection of company assets, including intellectual property theft.

In this case, Energy Company X holds certain intellectual property rights, which includes, proprietary drilling equipment and client lists. Non-compete agreements exist in part to deter an employee from stealing intellectual property from an employer and benefiting by creating a competing entity using the former employer's technology, vendors and/or selling the employer's own technology to its existing customers.

In the current situation, Energy Company X learned that competitors knew of drilling equipment designs which were still in development and had not be used in the field to date. Competitors recognized the designs when presented by individuals who were pitching the designs for a newly formed company.

Energy Company X, upon learning of the formation of the competing company by its former employees, contacted McCann Investigations. Energy Company X believed that communications regarding the new venture had taken place on company laptops, desktops and smart phones, which the company provides to its employees. In addition to the use of company electronic devices, Energy Company X also provided company vehicles to employees. Energy Company X believed that meetings were taking place during the day and that the employees were using the company vehicles to drive to these meetings.

McCann Investigations has found that in most cases involving violations of non-compete agreements and theft of intellectual property, the former employees almost always use that company's laptops or smartphones to communicate with co-conspirators. An experienced computer forensics expert, in most cases, can recover data even it if has been deleted.

It is important to note, that in order for the data to be admissible as evidence in civil or even criminal litigation, the data must be extracted and stored in a forensically sound manner by a third party, licensed computer forensics examiner. Allowing the company's IT personnel to extract the data would deem the evidence contaminated and inadmissible in a court of law. It is extremely important that once the suspicion of wrongdoing arises, that the device is immediately powered down and delivered to a qualified computer forensics expert.

Technical Situation

Energy Company X required that the investigation remain covert in the beginning in order to learn the full extent of collusion within its ranks. Imaging and extracting the information from the employees' laptops were paramount in gathering information. In order for the devices to be imaged, computer forensics experts would have to have physical possession without arousing suspicions from the employees.

Energy Company X provides employees standard issue company iPhones. While iPhones are the best security options on the smartphone market, passwords are easily cracked and several years of past data can often be recovered. Android and Windows based phones provide even greater access than the iPhones for forensics investigations. Factory re-setting any of these

phones will wipe out all of the data. However, if the phone has been backed up to a laptop or a desktop, the data will be stored on that device and is recoverable.

The following are the types of devices that can typically be imaged for recoverable data:

- Smartphones - iPhones, Android, Blackberry, Microsoft Windows Mobile, Symbian
- Mobile phones - standard phones such as CDMA, TDMA, GSM
- SIM cards contained in mobile phones
- Removable flash storage contained in mobile devices
- Tablet devices - iPad, Android tablet, Microsoft tablet
- Other mobile devices - PDA devices, GPS devices, iPods, Palm Pilots, digital cameras, digital video recorders, digital audio recorders, MP3 players, flash storage devices, 2-way pagers

Mobile device operating systems are not as standard or stable as computer operating systems, so locating and reporting on data is more difficult and time consuming than on a Mac or PC.

While recovering deleted data from a smartphone is successful in most circumstances, there are problems that can arise in the imaging process:

- **Standard Imaging Protocols** - Mobile devices should follow standard forensic imaging protocols to avoid data being changed, written or updated on the devices.

    - An incoming phone call could cause an older call log entry to be overwritten potentially spoiling the state of the evidence.

    - The same can be true about allowing the mobile device to send or receive text messages, MMS, phone calls, emails, application updates, etc.

    - Methods to prevent this include cloning the SIM card for GSM devices to prevent network access and only powering on the device in a "stronghold box" or "Faraday Bag" which prevent any types of wireless, cellular, Bluetooth, Wi-Fi or phone carrier signals from reaching the phone.

- **Advanced Security Settings -** Some newer devices prevent any type of access to information without the passcode.

- **Self-Destruct Mode -** Some devices have the capability to securely erase themselves if the wrong password is entered too many times.

- **SIM Card Passwords** - Most SIM cards have hardware based password control that can lock out the card after too many wrong passwords. (Locked SIM cards can sometimes be unlocked with help from mobile provider by providing a SIM carrier specific PUK code.)

- **Remote Self-Destruct** - Allows self-destruct commands to be sent remotely by Blackberry or Exchange server administrators. (This is another reason to be sure specially trained forensic experts with the proper equipment handle the mobile devices.)

While permanently wiping data from a smart phone is possible, the average user typically is not tech savvy enough to accomplish this. In most cases, a computer forensics examiner will be able to recover deleted data.

Solutions

Because of the complexity of the case encompassing multiple components of non-compete violations, McCann investigators deployed a full investigation incorporating multiple tools. The tools included:

- Computer Forensics
- Mobile Device Forensics
- Background Investigations
- Surveillance (GPS tracking of vehicles)
- Undercover (including video and audio recordings of meetings)

Computer Forensics Utilizing Undercover Methods

To maintain a covert investigation, McCann computer forensics examiners posed as a contract IT services company. The examiners presented business cards from an IT services company which was a legitimate sister company. The examiners were able to do complete computer forensics imaging on-site, creating forensically sound copies of the hard drives of each laptop and desktop. The copies could then be transported to the computer forensics lab for further analysis and extraction of data that was requested by the client. The data that was extracted included emails, documents and drawings. Specifically, the client wanted to determine with whom the employees were communicating, and more importantly, was proprietary information in the form of drawings and designs, as well as customer lists, downloaded or exported from the company network. In depth analysis on the devices revealed email communications related to creating a new business entity as well as the download of proprietary files. It should be

noted that the employee had deleted all of the email communications. However, the computer forensics examiners easily recovered the deleted emails and documents. An examination of metadata revealed the user, and exact dates and times that designs and client lists were downloaded and exported to USB flash drives.

Mobile Device Forensics

McCann Investigations received the smart phone of the former employee. Through forensics imaging of the device, McCann investigators were able to recover deleted emails, text messages, call history, and images. Upon investigation of the text messages, emails and call history, it was determined that the employee was in communication with another former employee and using intellectual property of Energy Company X. In fact, they had started a competing company, utilizing the intellectual property and client list of Energy Company X, and had already begun communicating with those clients regarding their new company.

With this data, extracted in a forensically sound manner, Energy Company X was able to provide information to their attorney and begin proceedings to file civil litigations and injunctions against the former employee and any accomplices.

Background Investigations

McCann investigators performed an in depth background investigation on each of the suspected employees. The investigations included a basic background check, relationship diagram, digital footprint search, and social media mapping.

Surveillance

McCann investigators were able to deploy GPS devices on the company's vehicles driven by the employee, which allowed them to track the employee's movements in real time and gain detailed surveillance information. The GPS tracking further facilitated the investigators by providing the public location of the subject, which in turn allowed the investigators to capture covert audio and video recordings of meetings employee had with accomplices. Investigators then were able to provide invaluable information regarding the depth of the non-compete violations to Energy Company X.

Undercover Work

Because of the covert nature of the investigation, and the client's desire to gather as much evidence as possible, McCann investigators worked undercover to gather information regarding the gravity of the non-compete violations.

McCann's lead investigator made contact with the subject at an industry relation conference posing as a venture capitalist looking for opportunities in the oil and gas arena. Several meetings involving undercover investigators took place over the coming months which not only revealed current and former employees

colluding to start a competing company; it also revealed that drilling equipment designs taken from the client were already in the development stage. Covert cameras and recording devices were placed throughout the meeting space, which effectively documented all involved, as well as, visually displayed the drilling equipment that had been built using the client's proprietary designs.

Products and Services Used:

- Computer Forensics Technician – Licensed Private Investigator in the State of Texas with certification in computer forensics.
- EnCase, a Guidance Software – Leading software application to forensically image computers.
- Oxygen Forensic Suite – Leading software application to forensically image Smartphones.
- Spark Nano GPS with extended battery pack, weatherproof pelican case and real time tracking.
- Licensed Private Investigators to perform undercover work and document all interaction with subjects.

Conclusion:

With the pervasiveness of technology in the workplace, computer forensics is a key component of investigations that most effectively gathers evidence. However, because of the complexity of some investigations, it is required to utilize tools and techniques that are more traditional to private investigations such as, backgrounds checks, surveillance, and under-cover work. In a dynamic case, involving intellectual property theft and non-compete violations, a more intense focus on gathering evidence from every angle, both digital and traditional, will ensure that the client has incontestable evidence and documentation to present in a civil or criminal case.