Published on *The National Law Review* https://natlawreview.com

Federal Authorities Increasing Prosecution of Computer-Based Fraud Charges

Article By:

Dr. Nick Oberheiden

Over the past several decades, almost every industry has undergone significant changes to how business is conducted due to the widespread use of computers and other technologies. While technological developments certainly make business more efficient, they also open the door to the abuse of client and customer information.

When an individual or business uses computers to obtain and use sensitive information, they may face a variety of federal charges, including computer fraud offenses. In some cases, the use of a computer to commit a crime is seen as an "enhancement," making the underlying charge more serious. In other cases, using a computer to commit fraud will result in separate criminal charges. In either case, allegations of computer fraud are extremely serious and present a variety of challenges, both to the prosecution and the defense.

Recently, the federal government has begun cracking down on computer fraud charges under 18 U.S. Code § 1030 (the Computer Fraud and Abuse Act). The Computer Fraud and Abuse Act focuses on fraud committed against government entities as well as private individuals and organizations. In terms of the latter, the Act prohibits individuals and organizations from using a computer without authorization to access another's "protected computer."

Most often, these cases involve an individual attempting to derive an economic benefit; however, any use that could be seen as benefiting the accessing party may still constitute computer fraud. These charges can carry significant criminal consequences, even for those without any prior record, including federal imprisonment, forfeiture, or restitution, as well as civil liability.

Employee's Use (and Abuse) of Access

One type of case that federal law enforcement is especially on the lookout for are those involving employees who use access granted by virtue of their position to commit crimes. Employees are often in the position of possessing customer's sensitive information, whether it be passwords, healthcare information, or trade secrets. Typically, employees must agree that they will not use customer information to derive a personal benefit or commit an illegal act.

For example, in a recent case out of the Northern District of Texas, a security analyst with the popular

home-security company ADT now faces 52 months in federal prison after he pleaded guilty to several charges involving hacking into customers' video feeds.

The U.S. Attorney claimed that the man added his own email address to several customers' accounts, giving him real-time access to the video surveillance in their homes. He would accomplish this by either telling customers that he needed to add his email to their account to perform necessary maintenance or adding his own email without the customers' knowledge.

Once he had access to the video feeds, the man would allegedly watch videos of naked women and couples having sex for his own sexual gratification. According to the plea agreement, he accessed more than 200 customers' accounts, viewing the videos more than 9,500 times.

The man was charged with several counts of computer fraud. He faced up to five years in prison. However, rather than take the case to trial, the man entered an open guilty plea in which he acknowledged responsibility for the offenses and asked the judge to fashion an appropriate sentence. Ultimately, he received a slightly mitigated sentence of 52 months incarceration.

Theft of Trade Secrets

Federal law enforcement is also pursuing criminal action against individuals and companies who use computers to steal important business information from clients or the companies that contract for their services.

In a recent announcement by the U.S. Attorney's Office for the Western District of Oklahoma, a man pleaded guilty to conspiracy to steal trade secrets from an oil and gas company. In that case, the man was a controller for the valve division of an oil and gas company that serves customers engaged in drilling and production. Evidently, the man registered for a new business that directly competed with one of his company's customers. He then recruited employees from the customer company to join his new business.

While this alone presents legal problems, the man then "downloaded the technical drawings, material specifications, and manufacturing instructions for the victim company's valves" as well as the company's financial information. For example, he was able to obtain not only the design of the valves but also the cost of manufacture and customer information. The evidence also suggests that he replaced the victim company's logo with his own company's logo.

Having taken the company's design, the man then manufactured the valves and sold them in direct competition with the victim company. Making matters worse, he then told his employees to delete all potentially inculpatory text messages and files.

Most recently, the man entered a guilty plea to conspiracy to steal trade secrets. He faces five years in prison, a $250,000 fine, restitution to the victim company, and up to three years of supervised release.

While it is hard to say that the defendant in either of these two examples did not know that their actions were in violation of the law, that will not always be the case. Certainly, in some situations, a party can inadvertently violate computer fraud laws. Regardless of intention or the extent of the evidence against an individual, obtaining the assistance of an experienced computer fraud attorney is crucial in this type of case.

Computer fraud cases are exceptionally challenging, both for the prosecution and the defense. To properly defend against these allegations, a defendant must have knowledge of both the complex legal principles and the underlying technology.

The Government's Burden to Prove a Fraud Case

Any fraud case requires the prosecution to show a defendant made an intentionally false statement or misrepresentation with the intended result of furthering their own interests or the interests of a third party. Thus, "guilty" knowledge is a prerequisite to any fraud conviction.

While, in some cases, prosecutors may have direct evidence of an individual's intent to commit fraud, more often, this comes in the form of circumstantial evidence.

For example, in the trade secrets case mentioned above, the defendant's act of telling employees to delete certain emails could be seen as evidence that he intended to cover up his past actions because he knew they were illegal. Computer fraud lawyer Nick Oberheiden explains:

Any time the prosecution relies on circumstantial evidence, it opens the door for a defendant to challenge the prosecution's interpretation of the evidence. Circumstantial evidence, by its nature, requires the fact finder to make an inference before reaching the ultimate conclusion. In most situations, the inference the prosecutor asks the judge or jury to make is not the only reasonable inference based on the facts.

That said, by the time an individual learns that charges are pending, the federal government will already have a significant head-start. Federal prosecutors diligently investigate claims of computer fraud before notifying the subject of their investigation. Thus, those facing computer fraud charges, or those who fear that they are under investigation for any computer-based offense, may consider reaching out to an experienced computer fraud defense lawyer as early as possible.

National Law Review, Volume XI, Number 217