Gregory S. Johnson
PAINE HAMBLEN, LLP
717 West Sprague Avenue, Suite 1200
Spokane, WA 99201
509-455-5395
greg.johnson@painehamblen.com

PROTECTING INTELLECTUAL PROPERTY AND THE COMPUTER FRAUD AND ABUSE ACT

For many companies, their intellectual property is their raison d'être.

Organizations spend thousands of dollars protecting themselves from computer hackers, external intrusions, computer viruses and so forth. Ironically, as often as not, the persons who are able to do the most harm to a company are its employees and departing employees.

Several years ago, the Ponemon Institute, a privacy management research firm, and Symantec, a computer security applications company, announced the results of a co-sponsored survey of 945 adults who were laid off, fired or lost jobs in the past 12 months. Of these 945 individuals, 37% said they were asked to leave; 38% said they had found a new job; and, 21% moved on because they anticipated lay-offs. All of them had access to proprietary information such as customer data, contact lists, employee records, financial reports, confidential business documents, software tools or other intellectual property that belonged to their employer. **According to the survey, 59% took company data with them when they left their jobs**. Of the 59% percent:

- 65% took e-mail lists;
- 45% took non-financial business information;
- 39% took customer information, including contact lists;
- 35% took employee records; and,
- 16% took financial information.

About 61% of the surveyed persons took the information as paper documents or hard files; 53% burned the information onto a CD or DVD; 42% downloaded the information onto a USB "thumb drive," and 38% sent the data to themselves as an e-mail attachment. The surveyed

persons indicated that the stolen information was used to get a new job, start their own business, or simply for revenge.

Notably, the survey revealed that part of the problem rests with companies themselves and their relaxed attitude towards internal security. The survey found that only 15% of respondents' companies reviewed or audited the paper documents or e-files that employees were taking. The report further revealed that if businesses did conduct a review, it was very poor with 45% of the reviews not being completed and 29% of them being fairly superficial. As troubling is that 24% of the ex-employees indicated that they still had access to their former employer's computer system after they had left the company, with over 50% citing access remained available between one day to a week, and 20% citing that access remained available for more than a week.

How should companies protect themselves from these unsavory realities? Generally, with foresight and planning and by considering and addressing the issues set forth below.

The Computer Fraud and Abuse Act.

The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, was originally promulgated to protect computers from hackers and outside intrusions. The CFAA has also been used against employees who steal information from their employers, however the success of this tactic has varied because the Federal Circuits have provided split opinions which has made to applicable law, jurisdiction dependent.

The interplay between the CFAA and employment matters can be seen in *Condux International, Inc. v. Haugum*, 2008 WL 5244818, 2008 U.S. Dist. LEXIS 100949, (D. Minn.) (decided December 15, 2008). Condux alleged that when Haugum decided to leave Condux, he misappropriated company confidential information and then attempted to erase evidence of his theft. Condux sued Haugum under the CFAA, claiming unauthorized access. In response, Haugum asserted that "his position as vice president of the company 'authorized' him to access of Condux's computer system and specifically to access the confidential business information at issue." Thus, Condux could not establish that he acted without authorization or in excess of authorized access. *Id*. at *4. The Condux Court addressed a line of cases that holds a person civilly liable under the CFAA "when he accesses confidential or proprietary business

information from his employer's computers that he has permission to access but then uses that information in a manner that is inconsistent with the employer's interests or in violation of contractual obligations or fiduciary duties." *Id.* The Court also addressed a contrary line of cases which hold that "the CFAA is implicated only by the unauthorized access, obtainment, or alteration of information, not the misuse or misappropriation of information obtained with permission." *Id*. The *Condux* court adopted the latter view, stating:

> [T]he conduct at the heart of the dispute is not the access of the confidential business information but rather the alleged subsequent misuse or misappropriation of that information. Such allegations, however, are not sufficient to state a claim for violations of [the CFAA].

Id. at *6. Hence, in instances where an employee is authorized to access certain company electronically stored information ("ESI"), there is not unauthorized access within the meaning of the CFAA when the information is accessed and then misappropriated and misused.

Query: what if, as a part of its employment agreement, a company makes clear that such access and misuse is "unauthorized?" More specifically, in addition to the standard non-compete, confidentiality, trade secret, work for hire, and intellectual property assignment clauses, what if the employment agreement included a clause that states something such as:

> As part of your employment with Our Company, you will become privy to certain information that is company Confidential, Proprietary, and constitutes Trade Secrets. This information is solely owned by and belongs to Our Company and shall only be used to further the business of Our Company. You shall not, may not, nor are you authorized to use this information for any other purpose. Further, using this information for purposes other than forwarding the business of Our Company exceeds whatever authorization you believe you may have. Such unauthorized use of company information shall constitute default of this Agreement and a violation of the CFAA.

Obviously, it cannot be stated with certainty what a court such as *Condux, supra*¸ would hold, when confronted with such a clause and the attendant argument, but as a factual matter, given the express contractual terms, it would be more difficult for a court to find that improper use of company information was "authorized."

Unfortunately, while some courts have agreed with this view, in *United States v. Nosal* (a.k.a. *Nosal I*) 676 F.3d 854 (9th Cir. 2012) (*en banc*, April, 2012), our Ninth Circuit did not agree and held that that defendant employees did not "exceed[] authorized access" by

transmitting confidential information in violation of company policy, stating, among other things: "the government's proposed interpretation of the CFAA allows private parties to manipulate their computer use and personnel policies so as to turn these relationships into ones policed by criminal law. Significant notice problems arise if we allow criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read."[1]

However, in *United States v. Nosal II* (October 20, 2016), a Ninth Circuit panel held that Nosal, whose computer access credentials had been revoked, acted "without authorization" in violation of the CFAA when he or his former employee co-conspirators used the login credentials of a current employee to gain access to computer data owned by the former employer and to circumvent the revocation of access. While password sharing was prohibited by the company agreement, the *Nosal II* holding did not address the policy, rather the Court noted that under the facts of *Nosal I*, the defendants had accessed the company computer via their own logins/passwords, from within the company (not an unauthorized CFAA violation) whereas under the facts of *Nosal II*, the defendants logins/passwords had been revoked, and they used another employee's login/password to access company computers from outside the company, which is exceeding authorized access within the meaning of the CFAA. A copy of the Nosal II opinion can be seen here: http://cdn.ca9.uscourts.gov/datastore/opinions/2016/07/05/14-10037.pdf.

Despite the Ninth Circuit CFAA holdings, there are still steps companies can take to secure their ESI from internal instrusion.

Data Management.

Many organizations do not properly manage their ESI. For the most part, their ESI exists as a "hodgepodge" that is easily available to employees who have no business reason or need to access it. Every organization should have a document retention and destruction policy (another complete topic). Pursuant to this policy, ESI should be categorized and organizations should choose the most appropriate set of controls for each data class and access should be restricted and available only to those who need it.

[1] *But see, United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), which construe the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty.

File Monitoring.

Companies spend large sums of money monitoring files that come to their systems from the outside. Few companies spend the time and money that is necessary to monitor files that move around their network or exit their systems. By using system, network, and gateway logs, it is possible to monitor network traffic. It is also possible to monitor inordinate use. Thus, for example, if a user began copying many files (a process which uses more system resources) the file copying can be known. In addition, many vendors sell applications that inspect e-mail, peer-to-peer file-sharing systems, Web postings and FTP sites, for ESI that may be exiting the company's system. These particular tools generally lie near network gateways and issue alerts when they "see" suspicious data packets. Many of these applications can also identify, trap, block, or encrypt data as it leaves the network. Thus, if a departing employee began manipulating more files than usual or began sending files outside of the organization, such would be known.

Identify and Address Endpoints.

"Endpoints" are generally recognized as any point on a system where ESI can enter or exit.

Portable devices, such as laptops, PDAs, iPods, digital cameras and removable media, such as "thumb drives" or USB drives, make it easier than ever for employees to connect to an endpoint and "walk" ESI out of an organization. Companies must control and monitor devices that can be temporarily connected to its computer system and monitor the ESI that can be downloaded to these devices.

From a software perspective, there are applications that can monitor a company's system and know when devices are being connected to it and depending on the settings, can stop file transfers and/or track what is taking place.

From a hardware perspective, many PCs come with a DVD "burner" and/or multiple USB ports. If an employee does not need these devices to perform the business of the company, these ports or devices should be disconnected or removed all together. Users who claim to need access to such devices can be directed to use a centrally located computer that is controlled by information services and contains the necessary tracking software.

Conclusion.

An organization's intellectual property is often its rasion d'etre. The Ponemon Institute/Symantec survey establishes that more than half of the employees who leave an organization will leave with company data. The survey further establishes that companies do not do enough to keep internal data theft from occurring. Organizations must implement and enforce well written employee agreements and policies that address these issues. Given the Ninth Circuit CFAA holding, companies must proactively manage their data, monitor files that are in motion, and ensure that their systems are secure from both internal and external attacks.

697047.DOC