Employment

Andrews Litigation Reporter

VOLUME 24 ★ ISSUE 14 ★ FEBRUARY 9, 2010

Expert Analysis

The Computer Fraud and Abuse Act: An Essential Tool for Employers

By William J. Ryan, Esq. and René Hertsberg, Esq.

Traditionally, dissatisfied or malevolent employees who wanted to steal data from employers needed to spend considerable time and energy to copy or transmit paper documents.

However, with the proliferation of USB storage devices ("thumb drives"), CDs, external hard drives, personal e-mail accounts and other forms of mobile electronic file storage, businesses are finding themselves at greater risk of this type of injury.

Employees with regular access to company data in the performance of their job duties can now quickly and effortlessly copy valuable information minutes before quitting or being fired, and pass it along to competitors long before the theft is uncovered.

CFAA claims can be easier to prove than trade-secret claims because they focus on the act of computer access rather than on the content of the data taken.

Although preventative measures like cyber-vaults and password-protected access layers are valuable tools to secure data from outside intruders, strictly technological solutions are rarely 100 percent effective. The Computer Fraud and Abuse Act can be used to protect against insider theft, and employers should be aware of how to maximize their rights as created by the law.

An Overview

First enacted in 1984, the CFAA was designed to protect computers owned by the federal government and large financial institutions. Over the years the law has undergone multiple revisions to broaden its applicability, and in its current form it can be an effective tool for everyday businesses.

WEST®

A principal benefit of the CFAA is that it provides a faster, and often cheaper, venue for enforcing an employer's rights over traditional state law remedies. For example, the CFAA provides jurisdiction for the employer to file suit in federal court, which many lawyers believe adds gravity to a lawsuit and often in allows the case to proceed more quickly than it would in state court.

CFAA claims can also be easier to prove than trade-secret or breach-of-contract claims because they focus on the act of computer access instead of the content of the data taken by the employee.

Nevertheless, the benefits of CFAA claims are enhanced if the employer implements effective computer-authorization policies and evidence-preservation strategies before a theft occurs. Some of these strategies are discussed later in this article. Additionally, business owners should consider implementing procedures designed to preserve their CFAA rights because many of these measures will also help protect rights under trade-secret and other state laws.

The Computer Fraud and Abuse Act

The current version of the CFAA[1] covers a variety of situations, ranging from illegally using government computers to using computers for extortion. This article will focus on key provisions that employers can use against employees who steal company data.

The essential elements of a civil claim by an employer against an ex-employee accused of stealing confidential company data include:

- An employee accessing a "protected computer";
- Without authority or exceeding authority;[2] and
- Damages.

Any information may be protected by the CFAA; it does not distinguish between types of data.

Federal Jurisdiction

The requirement of an employee's accessing a "protected computer" is what establishes federal jurisdiction over a CFAA claim. The law defines a protected computer as one that "is used in or affecting interstate or foreign commerce or communication."[3] This is a relatively low bar; computers used in businesses that operate across state lines or any computers with an Internet connection qualify.[4]

Authorization Requirement

The primary focus when evaluating a potential CFAA claim is whether the employee was authorized to access the employer's computers and/or servers. To prevail, an employer must prove that the employee's access of company computers was "without authorization" at the time of misappropriation.

On this important issue, however, federal courts have taken two essentially different approaches. Under one approach, courts analogize "without authorization" to a trespass; an employee will be found to have accessed computers without authorization only where the company has in place express policies prohibiting the employee's access to the computers or data in question.

In this scenario, an employee who improperly takes or uses company data from computers she regularly uses in her job may escape the CFAA's reach. A more sensible, employer-friendly line of cases takes a different approach.

One approach holds that an employee is without authorization to use information any time she takes company data for an improper purpose.

This second approach holds that an employee is without authorization any time she takes company data for an improper purpose, even if the company granted her job-related access to that computer or data. The result of this "split of authority" is that the scope of protection afforded a business may depend on where that business is located.

The following hypothetical illustrates this distinction: A company with no computer or privacy policy has an employee who decides to quit for a more lucrative position at a competitor but remains on staff for a time in order to surreptitiously copy data from company computers to use at the new employer. Three federal appellate courts have addressed this situation, with varying results.

The leading appellate case is *International Airport Centers LLC v. Citrin*,[5] in which the 7th U.S. Circuit Court of Appeals found that an employee's authorization to use a company computer is predicated

on the employer-employee agency relationship. Therefore, when the employee in the hypothetical scenario violates his duty of loyalty by deciding to misappropriate company data for personal gain, he voids the agency relationship with his employer and thereby lacks authorization to copy those files.

This employer-friendly opinion suggests that even in the absence of computer or privacy policies, a company may be able to successfully assert a CFAA claim against a former employee in the states covered by the 7th Circuit (Illinois, Indiana and Wisconsin).

The next appellate court to address the situation was the 11th Circuit, in *United States v. Salum*,[6] a case that involved the criminal prosecution under the CFAA of a police lieutenant who accessed the National Crime Information Center, an FBI database that tracks crime-related information, to obtain information he later gave to a private investigator. Although the defendant had authority to access the NCIC by virtue of his position as a lieutenant, the 11th Circuit upheld his conviction, holding that the lieutenant exceeded his authority when he accessed the database for an "improper purpose."

This language is in line with *Citrin* and is therefore another employer-friendly opinion that would seem to allow a CFAA claim for the employer in the states covered by the 11th Circuit (Alabama, Florida and Georgia).[7]

However, the most recent appellate court case, *LVRC Holdings v. Brekka*,[8] held that an employee only exceeds authority when the offender has no permission to use the computer for any purpose or when an employer rescinds the employee's right to access the computer. The 9th Circuit rejected *Citrin* by holding that an employee's authorization does not turn on any breach of duty and by adopting the simpler view that if an employee is given authorization to access company computers, that authority is valid until revoked by the employer.

This employee-friendly opinion suggests that, in terms of the hypothetical situation, in the absence of any computer or privacy policy, the employer's CFAA claim is not likely to be successful in the jurisdictions covered by the 9th Circuit (Alaska, Arizona, California, Guam, Hawaii, Idaho, Montana, Nevada, Northern Mariana Islands, Oregon and Washington).

For businesses that operate in a different state, the outcome of the hypothetical scenario is genuinely uncertain. In 2009–10 alone, district courts in Connecticut, Kansas, Missouri, New York, Pennsylvania, Tennessee and Texas indicated an adoption of the narrower view espoused by *Brekka*,[9] while district courts in Iowa, Massachusetts, Nebraska and Virginia indicated an adoption of the broad view espoused in *Citrin* and *Salum*.[10]

Companies that are successful in misappropriation lawsuits have confidentiality agreements and privacy policies in place.

Ultimately, this issue will likely remain unresolved absent U.S. Supreme Court or congressional intervention.

However, as discussed below, implementing confidentiality agreements and privacy policies allows an employer to potentially avoid this debate, secure its rights under the CFAA and reduce litigation costs.

Damages

To maintain a CFAA claim, the employer must plead damage or loss as a result of the alleged CFAA violation. The law defines "damage" as "any impairment to the integrity or availability of data, a system or information," and defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the offense, and any revenue lost, cost incurred or other consequential damages incurred because of a interruption of service."[11]

There is a proviso applicable to most CFAA claims that any alleged loss must total at least $5,000 in any one-year period in order to maintain the claim, unless the claim involves some type of personal injury or threat to public safety.[12]

Confidentiality Agreements and Privacy Policies

Most companies that are successful in lawsuits against ex-employees who misappropriate company information have confidentiality agreements and

privacy policies in place. This is true because, as discussed above, CFAA claims are predicated on a person's accessing a computer without authorization.

Confidentiality agreements and privacy policies set the boundaries of employees' access and can serve in court as easy proof of lack of authority. Similarly, trade-secret laws can only protect information that is designated as "secret." Such agreements and policies bolster a lawsuit against the ex-employee who steals data by allowing potential claims for violation of trade-secret laws and for breach of contract.

Several recent cases illustrate the importance of these agreements in asserting CFAA claims. In *Continental Group v. KW Property Management,*[13] a district court held that an employer had a reasonable likelihood of success in proving that a former employee accessed a computer and did so without authorization, in violation of the CFAA, when she misappropriated thousands of the employer's computer files. This holding relied on the fact that the employer had written computer-access policies stating that its computer equipment was only to be used for company purposes.

In *EF Cultural Travel BV v. Exploria Inc.*,[14] a former employee and vice president of EF Cultural Travel started a competing travel-service Web site and used his understanding of EF's Web site and trip codes to help create a program designed to pull pricing information from EF's Web site, which he later used to set his own prices.

The employer convinced the court it had a reasonable likelihood of proving that the former employee violated the CFAA because he exceeded his authorized access to EF's Web site when he used information labeled as "confidential" and "proprietary" in a confidentiality agreement he signed while working at EF. By labeling company data confidential and proprietary, EF preserved its CFAA claim because there was a limitation placed on the public authorized use of EF's public Web site.

These cases illustrate how an employer may be able to circumvent the legal battle between broad and narrow "authorization" definitions by maintaining written policies and agreements explicitly detailing employee computer authorizations and strictly limiting the use of company computers and information to company purposes only.

If such policies are already in place, employers should review and alter them to maximize their rights under the CFAA. By using this strategy, savvy employers can protect their rights under the CFAA regardless of which state they do business in.

The Importance of Evidence Preservation

A business owner's point of view is much different from that of a lawyer's. The business owner is forward-thinking: How do I grow my business, and what do my employees need to be successful? The litigation attorney is trained in terms of proof: What happened, and how do we prove what happened?

The difference often results in frustration when wrongful conduct is discovered months or even years later and proof of the wrongdoing necessary to bring successful litigation is missing. This happens often because evidence is routinely discarded long before somebody realizes its necessity.

Preserve evidence by storing old, outdated or nonfunctioning computers in a secure area.

Legal jurisprudence is riddled with CFAA cases involving forensic investigation of computer equipment, and maintaining possession of the physical equipment may prove fertile ground for gathering evidence against ex-employees.

This is why evidence preservation is such an important issue, especially in CFAA cases. When computer equipment, thumb drives, CDs and other physical evidence belonging to an ex-employee are missing, the costs of discovering wrongful conduct are greatly increased. CFAA claims must be filed within two years of the wrongful conduct or when the wrongful conduct is discovered,[15] but evidence may be long gone by that time.

A simple resolution is *not to throw away computer equipment* as soon as it is no longer needed. Instead, a company should treat old, outdated or nonfunctioning units in the same way it treats documents under a document-retention policy. Or, if there is no such retention policy, old, outdated or nonfunctioning computers and related materials should be labeled and stored in a secure area.

Information technology professionals are able to extract key information from an ex-employee's computer, even if it has not been used for a long time or has had other users in the interim. In *Citrin*[16] the employer was able to prosecute its CFAA claims against its ex-employee precisely because it kept the ex-employee's company laptop and had it forensically examined. This information can prove crucial to enforcing one's rights under the CFAA and other state laws.

Conclusion

While it may be difficult to prevent every employee from misappropriating data, employers can easily implement certain measures designed to protect their rights under the CFAA and other laws.

Notes

1 18 U.S.C. § 1030.

2 For simplicity's sake, this article refers to this requirement as "without authorization."

3 18 U.S.C. § 1030(e)(2)(B).

4 *See, e.g., Dedalus Found. v. Banach,* No. 09 Civ. 2842(LAP), 2009 WL 3398595 *2-3 (S.D.N.Y. 2009) (collecting citations).

5 440 F.3d 418 (7th Cir. 2006).

6 257 Fed.Appx. 225 (11th Cir. 2007).

7 Note that some district courts have argued that the 1st and 5th Circuits adopted the broad view, although some later district court cases within those circuits adopt the narrower view. *See, e.g., Guest-Tek Interactive Entm't v. Pullen,* No. 09-11164-NMG, 2009 WL 3403129, *2-3 (D. Mass. 2009) (arguing the 1st Circuit adopted the broad view in *EF Cultural Travel BV v. Exploria,* 274 F.3d 577 [1st Cir. 2001[); *NCMIC Fin. Corp. v. Artino,* 638 F. Supp. 2d 1042, 1055-1059 (S.D. Iowa 2009) (arguing the 5th Circuit adopted the broad view in *United States v. Phillips,* 477 F.3d 215, 220-21 [5th Cir. 2007]).

8 581 F.3d 1127 (9th Cir. 2009).

9 *See Bro-Tech Corp. v. Thermax,* 651 F. Supp. 2d 378, 406-407 (E.D. Pa. 2009); *Jet One Group v. Halcyon Jet Holdings,* No. 08 CV 3980 (JS)(ETB), 2009 WL 2524864, *5-6 (E.D.N.Y. 2009); *Cenveo Inc. v. Rao,* No. 3:08 CV 1831 (JBA), 2009 WL 3166699 (D. Conn. 2009); *Joe N. Pratt Ins. v. Doane,* No. V-07-07, 2009 WL 3157337, *2-4 (S.D. Tex. 2009); *US Bioservices Corp. v. Lugo,* 595 F. Supp. 2d 1189, 1191-1195 (D. Kan. 2009); *Lasco Foods v. Hall & Shaw Sales, Mktg. & Consulting* 600 F. Supp. 2d 1045, 1053 (E.D. Mo. 2009); *ReMedPar v. AllParts Med.,* No. 3:09 CV 00807, 2010 WL 55303, *6-9 (M.D. Tenn. 2010).

10 *See NCMIC,* 638 F. Supp. 2d at 1055-1059; *State Analysis. v. Am. Fin. Servs. Ass'n,* 621 F. Supp. 2d 309, 315-316 (E.D. Va. 2009); *Ervin & Smith Adver. & Pub. Relations v. Ervin,* No. 8:08 CV 459, 2009 WL 249998, *7-8 (D. Neb. 2009); *Guest-Tek,* 2009 WL 3403129, *2-3.

11 18 U.S.C. § 1030(g); *see also Cenveo,* 2009 WL 3166699, *3; *U.S. Gypsum Co. v. Lafarge N. Am. Inc.,* No. 03 C 6027, 2009 WL 3598329, *5 (N.D. Ill. 2009). However, some district courts have held that for certain types of CFAA claims, a plaintiff must plead both damage and loss despite the plain language of the statute that reads "[a] ny person who suffers *damage or loss*" (emphasis added). Therefore, it is important to be aware of the law's pleading requirements when making CFAA claims. *See, e.g., Fink v. Time Warner Cable,* No. 08 CV 9628(LTS)(KNF), 2009 WL 2207920, *4 (S.D.N.Y. 2009); *Gerelli Wong & Assocs. v. Nichols,* 551 F. Supp. 2d 704, 708-709 (N.D. Ill. 2008).

12 18 U.S.C. § 1030(c)(4)(A)(i).

13 622 F. Supp. 2d 1357 (S.D. Fla. 2009).

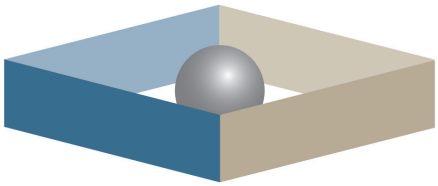
14 274 F.3d 577 (1st Cir. 2001).

15 18 U.S.C. § 1030(g).

16 440 F.3d 418.

William J. Ryan is a partner at **Scandaglia & Ryan** in Chicago, representing major companies in a variety of complex commercial litigation and intellectual property settings. **René Hertsberg** is an associate at the firm, focusing his practice on commercial, employment and intellectual property litigation.

For additional information, please contact William Ryan at 312.580.2036, wryan@scandagliaryan.com or René Hertsberg at 312.580.2060, rhertsberg@scandagliaryan.com.



SCANDAGLIA & RYAN