Workplace Law Bulletin
Society for Human Resource Management, www.SHRM.org

Recent Developments in Trade Secret Law: the Computer Fraud and Abuse Act

6/10/2011
By Jason C. Schwartz and Michael Murray

The Computer Fraud and Abuse Act increasingly plays a prominent role in trade secret litigation, bringing these disputes into the federal courts. It has been invoked in wide-ranging circumstances, from the criminal prosecution of a Social Security Administration employee who misused personal data about women he encountered to a civil suit between an employer and a former employee who stole the employer's client list to start a new firm.

As explained below, two key elements of the Computer Fraud and Abuse Act, the need to show that the violator's access was "without authorization," and the requirement to show "loss" of at least $5,000, have divided the courts. This article offers an explanation of these two important issues, as well as practical guidance in light of this still-developing law.

Without Authorization
Under the Computer Fraud and Abuse Act, a plaintiff generally must show that the defendant accessed a computer "without authorization" or in a way that "exceeds authorized access." 18 U.S.C. § 1030(a)-(b). The act defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." The courts are divided over the interpretation of these terms.

On one side of the split stand two circuit courts of appeal that have held that an employee acts "without authorization" or in a way that "exceeds authorized access" when he or she accesses files for an illegitimate purpose. *Int'l Airport Ctrs. LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F. 3d 577 (1st Cir. 2001); see *NCMIC Finance Corp. v. Artino*, 638 F. Supp. 2d 1042, 1056 (S.D. Iowa 2009); see also *United States v. John*, 597 F.3d 263 (5th Cir. 2010) (implying that criminal act may be "without authorization" per se).

In *Int'l Airport Ctrs. LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), for example, the 7th U.S. Circuit Court of Appeals held that an employer states a CFAA claim when an employee uses a work computer in violation of his duty of loyalty. In that case, a real estate company relied on employees to discover properties worth acquiring. An employee decided that he wanted to start his own real estate business and began using the computer to take the employer's opportunities for himself, in breach of his employment contract. Soon thereafter, he irretrievably deleted the research he performed and other data that would have demonstrated his illegitimate conduct.

The 7th Circuit held that the employee had acted "without authorization" because "his authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit [the company] in violation of his employment contract, he resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee." Notably, the 7th Circuit did not inquire as to whether the employee violated a formal usage policy.

On the other side of the split stand three circuits that have held that an employee acts "without authorization" or in a way that "exceeds authorized access" when he or she accesses files in violation of a usage limitation. *United States v. Nosal*, No. 10-10038, 2011 WL 1585600 (9th Cir. 2011); *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *United States v. John*, 597 F.3d 263, 271 (5th Cir. 2010). In *United States v. Rodriguez*, for example, the 11th Circuit upheld the conviction of an employee who had access to particular files but used that access for

personal purposes in violation of his employer's policy. Rodriguez, a Social Security Administration (SSA) employee, had access to the SSA database of individuals' sensitive Social Security information because of his position as a liaison to beneficiaries. SSA had a policy that prohibited employees from accessing the database without a "business reason" for doing so. Rodriguez, in violation of this policy, accessed the database to locate personal information of women he encountered. He used that information to ascertain their birthdays, addresses and marital statuses, sometimes sending unsolicited gifts to mere acquaintances. Rejecting Rodriguez's claim that he was a whistle-blower testing SSA's security, a jury convicted Rodriguez.

On appeal, Rodriguez argued that he did not access a computer "without authorization" or in a way that "exceeds authorized access" because SSA gave him access to the database. The 11th Circuit rejected that argument, holding that "the plain language of the act forecloses any argument that Rodriguez did not exceed his authorized access." The court observed that "[t]he policy of the [SSA] is that use of databases to obtain personal information is authorized only when done for business reasons" and that "Rodriguez conceded at trial that his access of the victims' personal information was not in furtherance of his duties as a TeleService representative and that 'he did access things that were unauthorized.'"

The 9th Circuit's decision in *United States v. Nosal* is illustrative as to the conflict between this line of cases and *Citrin*. In *Nosal*, a high-level search firm executive conspired with his assistant to steal a confidential database of executives and companies in order to found his own search firm. The district court, however, dismissed CFAA charges, reasoning that the employee had not acted "without authorization" because the employer had given him some access to the computer, even though the employee's action violated the usage policy of the employer. The district court relied on language in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), stating that "[n]o language in the CFAA supports [the] argument that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest."

The 9th Circuit reversed, holding that an "employee 'exceeds authorized access' under [CFAA] when he or she violates the employer's computer access restrictions—*including use restrictions*." (emphasis added). The court interpreted *Brekka* as standing for the proposition that the employer gets to determine the authorization of an employee through either access to the computer or limited access to the computer.

Given this developing case law, in order to protect your trade secrets and other confidential information, and to put your company in the best position to enforce its rights under the Computer Fraud and Abuse Act if necessary, it would be advisable to adopt a formal computer usage policy. This policy should, among other things, inform employees with respect to the data and systems to which they have access, the purpose for which they may access them, and the extent, times and manner in which they may do so. Employers should have a system for employees to acknowledge the policy (either manually or with click-through screens, for example) and have periodic training sessions.
Ideally, the policy should be part of a comprehensive data security system limiting access to sensitive data on a need-to-know basis and classifying information by various levels of security. Such a system should accurately label data at the appropriate level of secrecy (e.g., public, confidential, secret) and provide different treatment for data classified at different levels (e.g., freely disseminate, do not disseminate, do not copy, lock up at all times).

Loss
Another key element is the requirement to show "loss to one or more persons during any one-year period ... aggregating at least $5,000 in value." The act 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 interruption of service." Courts have divided over whether actual damage to a computer or system is required to establish "loss."

Some courts have held that the costs of investigating an offense do not constitute "loss" if there is no computer damage. In *Civic Ctr. Motors Ltd. v. Mason Street Import Cars Ltd*., 387 F. Supp. 2d 378 (S.D.N.Y. 2005), for example, the U.S. District Court for the Southern District of New York rejected the argument that costs that are not

"the result of computer impairment or computer damage" constituted "loss." In that case, a car dealership sued former employees and a competitor for theft of client lists. The car dealership alleged that its competitor conspired with its former employees to hack into a website used by customers to obtain price quotes in order to steal those customers. The car dealership claimed lost profits from the loss of clients.

The district court dismissed the car dealership's CFAA claim. The court ruled that the car dealership did not satisfy the first prong of the "loss" definition because "[c]ases in this jurisdiction have found that 'losses' under the CFAA are compensable only when they result from damage to, or the inoperability of, the accessed computer system" not when they are incurred investigating business losses unrelated to actual computers or computer services. Several other courts have ruled similarly. *Andritz Inc. v. S. Maintenance Contractor LLC*, 626 F. Supp. 2d 1264, 1266-67 (M.D. Ga. 2009); *Nexans Wires S.A. v. Sark-USA Inc*., 319 F. Supp. 2d 468, 474 (S.D.N.Y. 2004), *aff'd on other grounds*, 166 F. App'x 559 (2d Cir. 2006); *accord Register.com, Inc. v. Verio Inc*., 126 F. Supp. 2d 238, 252 n. 12 (S.D.N.Y. 2000) (interpreting statute prior to Patriot Act amendments defining "loss").

Other courts, however, have held that "loss" arises under the first prong even when there is no computer damage. In *A.V. v. iParadigms LLC*, 562 F.3d 630 (4th Cir. 2009), for example, the 4th Circuit held that a company established loss by pointing to the costs it incurred in investigating whether its system suffered flaws, even though no damage had occurred. In that case, a plagiarism detection service company, iParadigms, became embroiled in a lawsuit brought by four high school students. The high school required students to submit their papers through iParadigms, which archived the papers. The students sued iParadigms for allegedly infringing their copyright interests in the papers. The court awarded summary judgment on the copyright claims to iParadigms.

iParadigms then filed a counterclaim against one of the students for allegedly obtaining unauthorized access to iParadigms' service. The student had done so by way of the password of a college student that had been posted online. iParadigms sought damages for the considerable money and manpower it spent in determining how the student had accessed its service without authorization, not knowing that the password had been posted online. The district court awarded summary judgment to the student on this counterclaim, on the grounds that iParadigms did not suffer actual or economic damage.
The 4th Circuit reversed. The court observed that CFAA's definition of "loss" is a "broadly worded provision." Relying on the clear text of that provision, it concluded that CFAA "plainly contemplates consequential damages of the type sought by iParadigms—costs incurred as part of the response to a CFAA violation, including the investigation of an offense."

In so holding, the 4th Circuit joined significant authority holding that the costs of an investigation constitute "loss" under the act even when there is no associated computer damage. *AssociationVoice Inc. v. Athomenet Inc*., No. 10-cv-00109-CMA-MEH, 2011 WL 63508, at 6-7, 15 (D. Colo. 2011) ("[T]he act proscribes actions that do not result in any damage or interruption of service."); *Multiven, Inc. v. Cisco Systems Inc*., 725 F. Supp. 2d 887, 894 (N.D. Cal. 2010); *NCMIC Finance Corp. v. Artino*, 638 F. Supp. 2d 1042, 1064 (S.D. 2009); *SuccessFactors Inc. v. Softscape Inc*., 544 F. Supp. 2d 975, 980-81 (N.D. Cal. 2008); *Patrick Patterson Custom Homes Inc. v. Bach*, 586 F. Supp. 2d 1026, 1036 (N.D. Ill. 2008); see also *Resdev, LLC v. Lot Builders Ass'n*, No. 04-Civ-1374, 2005 WL 1924743 (M.D. Fla. 2005) (unpublished); *accord EF Cultural Travel BV v. Explorica Inc.*, 274 F. 3d 577 (1st Cir. 2001) (decided before the Patriot Act added definition of term "loss," Pub. L. No. 107-56, § 814(d)(5)). This view is consistent with the legislative history of the 1996 CFAA amendments. S. Rep. No. 104-357, at 11 (1996) ("[When] the system administrator [must] devote resources to re-secur[e] the system ... although there is arguably no 'damage,' the victim does suffer 'loss.' If the loss to the victim meets the required monetary threshold, the conduct should be criminal, and the victim should be entitled to relief.").

This case law suggests several practical pointers. Immediately upon learning of a data breach, employers should consider conducting a forensic investigation into the breach, hiring an outside consultant if necessary, carefully tracking time, resources and money expended on the effort. Employers should also work with law enforcement if and when appropriate.

The forensic investigation should focus on determining the scope of the breach and any resulting damage or interruption in service and on re-securing computer systems. The evidence uncovered by such forensic examinations is often invaluable when pursuing the company's rights in court, and the expenses associated with such investigations may help establish the $5,000 loss threshold for federal jurisdiction under the Computer Fraud and Abuse Act.

Further Development Expected

Given the increasing role of the federal courts in this important area of the law, we expect to see further development of these key issues in the years ahead. In addition to monitoring these developments and adjusting your policies and practices as appropriate, HR professionals would be well-advised to ensure that their companies' secrets are securely protected by appropriate systems, policies, agreements, training, audits and other best practices.

Jason C. Schwartz is a partner in the Washington, D.C., office of Gibson, Dunn & Crutcher LLP, an international law firm, where his practice includes the litigation of high-stakes trade secrets and noncompete matters. Michael Murray is an associate in Gibson Dunn's Washington, D.C., office.