TIMOTHY M. BLISS

The Computer Fraud and Abuse Act: A New Use for an Old Tool

As technology continues to evolve and become increasingly entrenched in our society, the manner in which businesses operate continues to be redefined. This technological renaissance can be both a blessing and a curse for employers, who have seen their processes streamlined to a degree that was unimaginable even a decade ago but have also faced problems unheard of in the not-so-distant past. As businesses become more automated, employers have become increasingly vulnerable to theft of proprietary or other confidential information, which is often stored electronically in a central location and protected by limited security measures. A departing employee with access to such files can download them to an external hard drive or other storage medium in a matter of minutes, conceal the device in his or her pocket or briefcase, and then leave the business without arousing any suspicion. Only after the individual begins to use the information to start up a competing business, hijack his or her former employer's clients, or encroach on sales leads does the theft become known.

State statutes prohibiting misappropriation of trade secrets and common law causes of action based on agency principles have provided the primary remedies for employers seeking injunctive relief or damages for the theft of their proprietary information. These causes of action, many of which developed long before computers, often contain narrow definitions or require employers to prove elements that limit their applicability to the modern electronic workplace. Moreover, employers often have no choice but to litigate such claims in frequently overburdened state courts that lack the resources and the docket space to address the lawsuit as expeditiously as is necessary to stem the damage to the employer.

In addition to "traditional" statutory or common law claims, however, employers harmed by theft of trade secrets or other tortuous activity involving their computer systems should consider possible remedies afforded by the federal Computer Fraud and Abuse Act (CFAA). 18 U.S.C. § 1030. The CFAA was originally enacted in 1984 to criminalize computer hacking. *See, e.g., International Ass'n of Machinists & Aero. Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 495 (D. Md. 2005). Since the CFAA was passed, it has been amended to authorize a civil action by any person "who suffers damage or loss" of more than $5,000 as a result of certain prohibited conduct. The act broadly defines "loss" to include "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." 18 U.S.C. § 1030(e)(11). *See Airframe Sys. v. Raytheon Co.*, 520 F. Supp. 2d 258, 262 (D. Mass. 2007).

Several courts have commented that the CFAA's provisions are not a model of clarity and are poorly organized. *See, e.g., Czech v. Wall St. on Demand Inc.*, 2009 U.S. Dist. LEXIS 114125 (D. Minn. 2009). Claims brought by an employer under the CFAA, however, usually involve an alleged violation of one of three provisions.

Section 1030(a)(2)(C)

A person violates § 1030(a)(2)(C) of the CFAA if he or she "intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains information … from any protected computer." The act defines a "protected computer" as a computer used by a financial institution or the federal government or any computer "used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2). In order to establish a § 1030(a)(2)(C) violation, therefore, an employer must establish (1) intentional access to a computer, (2) without or in excess of authorization, (3) whereby the defendant obtains information from the protected computer.

Frequently, former employees sued under the CFAA argue that the conduct at issue was not unauthorized because the conduct occurred while the individual was still employed and the access was within the individual's job duties. In fact, several courts have accepted this argument, holding that an individual exceeds his or her authorization to information only when either the initial access to the computer or database is prohibited or when the initial access is permitted, but the employee accesses information that is unauthorized at the time the access occurs. *See U.S.*

Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189 (D. Kan. 2009); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965–67 (D. Ariz. 2008).

Numerous other courts that have considered the issue, however, have rejected a strict interpretation of the term "exceeds authorization." *See EF Cultural Travel BV v. Explorica Inc.*, 274 F.3d 577, 583 (1st Cir. 2001); *Lasco Foods Inc. v. Hall & Shaw Sales, Mktg., & Consulting LLC*, 2009 U.S. Dist. LEXIS 99535, *13–*14 (E.D. Mo. 2009); *Calyon v. Mizuho Secs. USA Inc.*, 2007 U.S. Dist. LEXIS 66051 (S.D.N.Y. 2007); *Shurgard Storage Ctrs. v. Safeguard Self Storage Inc.*, 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000). Those courts generally follow the approach employed by the Seventh Circuit Court of Appeals, which applied agency principles in a case in which the defendant accessed his employer's protected information after the employee had decided (unbeknownst to his employer) to terminate employment voluntarily and start a competing business. *See International Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). Although the employee contended that the access at issue did not exceed his authority, the Seventh Circuit held that the employee's breach of his duty of loyalty to his employer terminated his authorization to access the information at issue and rendered all subsequent access unauthorized. The Seventh Circuit reached this conclusion notwithstanding the fact that the employer was unaware of the employee's intentions and, therefore, had not actually prohibited the employee from accessing the files at issue.

Section 1030(a)(4)

A person violates § 1030(a)(4) of the CFAA if he or she "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value. …" In addition to the previously discussed issue of whether the access at issue was authorized, defendants faced with a § 1030(a)(4) claim frequently seek to have the claim dismissed by arguing that the employer's complaint fails to meet the particularity requirement imposed by Fed. R. Civ. P. 9(b). The majority position, however, is that the "intent to defraud" required under the provision of the act is not necessarily equivalent to fraud per se. Therefore, the heightened pleading requirement of Rule 9(b) does not apply to a § 1030(a)(4) claim. *See Motorola Inc. v. Lemko Corp.*, 2009 WL 383444 (N.D. Ill. 2009); *P.C. of Yonkers Inc. v. Celebrations! the Party & Seasonal Superstore LLC*, 2007 U.S. Dist. LEXIS 15216 (D.N.J. 2007).

Section 1030(a)(5)

A person violates § 1030(a)(5) of the CFAA if he or she "causes damage" to a protected computer by gaining unauthorized access or transmission of a program, information, code, or command. The act defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). As such, claims under this section frequently involve employees who download or install secure erasure programs or "file wiping" software to remove incriminating evidence of their illicit activities from employers' laptop computers and other devices before they are returned upon termination. Since most employers' computer use policies state that all e-mails or other files created using company hardware or software systems are the property of the employer, the deletion of such files constitutes a violation of this section. *See International Airport Ctrs.*, 421 F.3d at 420; *Arience Builders Inc. v. Baltes*, 563 F. Supp. 2d 883, 884–885 (N.D. Ill. 2008).

In addition to these three provisions, the Computer Fraud and Abuse Act prohibits a range of other computer-related offenses that may occur in the employment context. Moreover, the act has been—and is likely to continue to be—amended regularly in order to keep pace with evolving technologies. As such, it is important for practitioners to become familiar with the CFAA and to employ it whenever possible to combat misuse or abuse of the electronic tools that have become an integral part of business in the electronic age. **TFL**

Timothy M. Bliss is an attorney with Vetter & White in Providence, R.I. He handles all types of civil litigation and employment litigation and represents both corporations and individuals in disputes before state and federal courts, before administrative agencies, and at arbitration hearings.

SIDEBAR *continued from page 5*

in that regard, I am as guilty as anyone of perpetuating the selection of that uninformed jury—all in the name of objectivity and fairness.

I am not sure that the process results in selecting a jury that represents a fair cross-section of the community. I am more certain that it does not result in the selection of a jury of one's peers. What I am certain of, however, is that, with regard to the entire jury selection process, I am properly accused of being somewhat of an anarchist (or maybe just disingenuous) because, as much as I may complain about the process, I offer no suggestions for improvement. **TFL**

Bruce McKenna is admitted to practice in Oklahoma and New York and is a member of The Federal Lawyer*'s editorial board. His practice consists primarily of professional negligence defense.*