COMPUTER FRAUD AND ABUSE ACT:
A NEW TOOL FOR EMPLOYERS

By Frank Harty

Nyemaster, Goode, West, Hansell & O'Brien, P.C.
700 Walnut St., Suite 1600
Des Moines, IA 50309
Telephone: 515-283-3170
Facsimile: 515-283-8045
E-mail: fharty@nyemaster.com

In the information age, employers must be more vigilant than ever in protecting confidential information. Even with comprehensive policies and procedures safeguarding intellectual property, an employer can fall victim to unscrupulous workers. Employers now have another weapon to combat employee theft of intellectual property: the Computer Fraud and Abuse Act (CFAA).

INTRODUCTION

The CFAA, while originally enacted as a criminal statute, is increasingly being used in civil actions. Although a majority of cases brought under the CFAA have dealt with outside hackers, a growing number are based on former employees using their former employer's customer or business information that was obtained through unauthorized use of a company computer. See *Mintel Int'l Group, Ltd. v. Neergheen*, 2008 WL 2782818 at *2-3 (N.D. Ill. July 16, 2008); *Pac. Aerospace & Electronics, Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1197 (E.D. Wash. 2003). There is a growing trend towards using the CFAA in employer/employee disputes. *Pac. Aerospace & Electronics*, 295 F. Supp. 2d at 1197.

HISTORY OF THE CFAA

The first version of the CFAA was enacted in 1984 as the Counterfeit Access Device and Computer Fraud and Abuse Act. *Id.* at 1194. That version of the CFAA was meant to apply to electronic trespassers known as computer hackers. *Shamrock Foods Co. v. Gast*, 535 F.Supp. 2d 962, 965 (D. Ariz. 2008). Since its enactment, the CFAA has been revised many times. An important revision occurred in 1994, when Section 1030(g) added a civil cause of action for violation of the statute. *Pac. Aerospace & Electronics*, 295 F. Supp. 2d at 1195. The 1994 amendment was intended "to expand the statute's scope to include civil claims challenging the unauthorized removal of information or programs from a company's computer database." *Id.* at 1196 (citing *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc*., 119 F. Supp. 2d 1121 (W.D. Wash. 2000)).

The revisions of the CFAA have broadened its scope. In fact, the CFAA can be considered to be as ubiquitous as the internet itself. "The CFAA was intended to control interstate computer crime, and since the advent of the Internet, almost all computer use has become interstate in nature." *Shurgard*, 119 F. Supp. 2d at 1127.

The CFAA is filled with precise terminology that courts have struggled to interpret. This has resulted in differences among the district and circuit courts in the interpretation of the provisions of the CFAA.

CATEGORIES OF ACCESS

Various sections of the CFAA refer to "exceed[ing] authorized access" and accessing a computer "without authorization." E.g., 18 U.S.C. § 1030(a)(1); § 1030(a)(5)(A)(i). There is some question as to whether these terms are interchangeable. While some district courts view the terms as virtually the same, others have given them different applications and meanings. The

Seventh Circuit has said there is a "paper thin" difference between the two terms. *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006). The "legislative history . . . demonstrates the broad meaning and intended scope of the terms 'protected computer' and 'without authorization.'" *Shurgard*, 119 F. Supp. 2d at 1129.

Because Congress used both terms ("unauthorized access" and "exceeds authorized access") in the statute, some argue Congress expressed its intention to exclude culpability or liability for "exceeding authorized access" in the sections of the statute where it did not use that term. *In re Am. Online, Inc.*, 168 F. Supp. 2d 1359, 1370 (S.D. Fla. 2001). Specifically, one question that arises is whether an employer can bring a suit under the CFAA against an employee for emailing proprietary information to a competitor when the employee was generally authorized to access and use that information. Some argue that allowing claims against ex-employees for sending unauthorized information to new employers will inappropriately federalize what should properly be a state law claim. "[A] case of this kind sounds in state statutory and common law and is heard in state court." *Chas. S. Winner, Inc., v. Polistina*, 2007 WL 1652292 at *2, (D. N.J. June 4, 2007).

UNAUTHORIZED ACCESS

As discussed below, it appears that the better reasoned decisions hold that a private cause of action does exist under the CFAA when an employee exceeds authorization.

"Without authorization" is not defined by the statute. The term covers direct and obvious forms of unauthorized access, including the mimicking of IP addresses to obtain access to protected computer systems. *Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A.*, 267 F. Supp. 2d 1268, 1323 (S.D. Fla. 2003). Some courts have held the term covers other forms of access as well, such as when an agent-employee has breached his duty of loyalty. See, e.g.,

Citrin, 440 F.3d at 420; *ViChip Corp. v. Lee*, 438 F. Supp. 2d 1087, 1100 (N.D. Cal.2006); *Shurgard*, 119 F. Supp. 2d at 1125. The rationale supporting this approach is fairly straightforward: once a trusted employee stops acting on his employer's behalf, he is no longer an "authorized" system user.

Breach of a duty of loyalty terminates an agency relationship, and termination of that relationship can make the accessing of computer files that had previously been authorized change into unauthorized access under the CFAA. *Citrin*, 440 F.3d at 420-21. "The authority of the agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal." *Id.* at 421 (quoting *State v. DiGiulio*, 835 P.2d 488, 492 (Ariz. Ct. App. 1992)).

In *ViChip*, the defendant claimed his deletion of company-owned files from a company computer was authorized because he was an officer and director of the company at that time. *ViChip*, 438 F. Supp. 2d at 1100. However, the court held that as an employee and officer, the defendant had a duty of loyalty to ViChip and, along with that duty, an agency relationship. *Id.* The defendant breached that duty because he deleted the company's information after he found out he was being asked to resign. *Id.* When the defendant breached his duty of loyalty, "he also terminated his authorization to access the files." *Id.* Similarly, another court has held that former employees lost their authorized access to the company's computers when they became agents of a competing company. *Shurgard*, 119 F. Supp. 2d at 1125.

The Iowa Supreme Court has not expressly recognized a cause of action for a breach of the duty of loyalty. *Midwest Motorsports P'shp v. Hardcore Racing Engines*, 735 N.W.2d 202, 2007 WL 1201746 at *1 (Iowa Ct. App. April 25, 2007). Iowa does, however, recognize a fiduciary duty of loyalty owed by corporate officers and directors. *Midwest Janitorial Supply*

Corp. v. Greenwood, 629 N.W.2d 371, 375 (Iowa 2001). "A fiduciary relationship exists between two persons when one of them is under a duty to act for or to give advice for the benefit of another upon matters within the scope of the relation." *Cagin v. McFarland Clinic, P.C.*, 317 F. Supp. 2d 964, 968 (S.D. Iowa 2004) (citing *Kurth v. Van Horn*, 380 N.W.2d 693, 695 (Iowa 1986)).

NARROW VIEW

There is a second line of cases that interpret the meaning of "without authorization" in a different way than the cases concerned with a breach of a duty of loyalty. *See, e.g., Shamrock*, 535 F. Supp. 2d 962, 964-95. The second line of cases holds that "without authorization" only applies to outsiders; persons whom have never had authorization to access the computer. *Id.* That line of cases holds that "the CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information." *Id.* at 966. The courts espousing this narrow interpretation reason "the statute was not meant to cover the disloyal employee who walks off with confidential information. Rather, the statutory purpose is to punish trespassers and hackers." *Am. Family Mut. Ins. Co. v. Rickman*, 554 F. Supp. 2d 766, 771 (N.D. Ohio 2008).

As one example, in *Brett Senior & Associates, P.C. v. Fitzgerald*, the employer claimed the employee had violated Section 1030(a)(4) under the "exceeds authorized access" provision, but the court found that the employee "did not obtain any information that he was not entitled to obtain or alter any information that he was not entitled to alter." 2007 WL 2043377 at *3 (E.D. Pa. July 13, 2007). The employer was actually objecting to the *use* of the proprietary information that the court held was not covered by the CFAA. *Id.* at *3-4. Similarly, other courts have rejected the argument that a breach of the duty of loyalty terminates "authorized"

access. *Chas. A. Winner*, 2007 WL 1652292 at *3-4 (focusing on the statutory language of "exceeds authorized access" as opposed to "exceeds authorized use.")

According to the CFAA, "exceeds authorized access" is "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." 18 U.S.C. § 1030(e)(6). "Exceed[ing] authorized access" includes the creation of a computer program that gathers information from a public website when the effectiveness of the program depended on the former employee's knowledge of confidential information belonging to his ex-employer. *Pac. Aerospace& Electronics*, 295 F. Supp. 2d at 1196-97 (citing *EF Cultural Travel BV v. Explorica, Inc*., 274 F.3d 577 (1st Cir. 2001)). If information was covered by a confidentiality agreement that the ex-employee had signed, the use of the computer program constituted "unauthorized access." *Id.* In *Explorica*, manual collection of the same data as the computer program was "theoretically" possible, but use of the computer program went beyond any reasonable or expected authorized use of the website. *Explorica*, 274 F.3d at 583.

Other courts have declined to enter in the debate over the meaning of "unauthorized" and "exceeds authorized access" by dismissing claims under other parts of the statute. See, e.g. *Rickman*, 554 F. Supp. 2d at 772 (holding that the employer had not adequately shown a "loss" under the statute); *Cohen v. Gulfstream Training Acad.*, 2008 WL 961472 at*4 (S.D. Fla. April 9, 2008) (holding employer did not show damage or loss resulting from the interruption of service.)

LOSS AND DAMAGE

It is imperative to show the requisite damages under the CFAA. To successfully state a claim under the CFAA, the party must have suffered a loss of more than $5000 within a one year

period (18 U.S.C. § 1030(a)(5)(B)(i), or must fall under 18 U.S.C. § 1030(a)(5)(B)(ii-v)). The statutory definition of "loss" was narrowed in 2001, so cases decided before that year do not reflect the current definition. *Cohen*, 2008 WL 961472 at *4.

As defined in the CFAA, "loss" means "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). It is particularly significant that recoverable damages include the costs of responding to the transgression, such as the cost of performing a computer system damage assessment. See *Explorica*, 274 F.3d. at 584-85. Allowable damages also include the cost of making the database more difficult for hackers to access. *Id.* at 585. "Customer information has previously been held to constitute a property interest sufficient to satisfy the damage requirement of the CFAA." *Four Seasons Hotels & Resorts B.V.*, 267 F. Supp. 2d 1268, 1324 (citing *In re Am. Online, Inc*., 168 F. Supp. 2d 1359, 1380).

One district court has held that loss includes "a loss of business, goodwill, and the cost of diagnostic measures." *Explorica*, 274 F.3d at 584. "Loss" is "a cost of investigating or remedying damage to a computer, or a cost incurred because the computer's service was interrupted." *Nexans Wires S.A. v. Sark-USA, Inc*., 319 F. Supp. 2d 468, 477-78 (S.D.N.Y. 2004). Another court has held that loss of business due to the improper use of confidential or proprietary information is not covered under the CFAA, because § 1030(e)(11) limits its scope to "damages incurred because of interruption of service." *Nexans*, 319 F. Supp. 2d at 477-78. "[R]evenue lost because the information was used by the defendant to unfairly compete after

extraction from a computer does not appear to be the type of 'loss' contemplated by the statute." *Id.* at 478.

As defined by the CFAA, "'damage' means any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). "Damage" includes the loss of information. *Shurgard*, 119 F. Supp. 2d at 1127. The term is defined in a way to focus on the harm the CFAA seeks to prevent, and does not define specific acts which would constitute "damage." *Id.* at 1126.

CFAA damages in the typical rogue employee case may also include incidental costs caused by the transgression. For example, if an employee emails confidential client information from a company system to an unsecure address such as a home e-mail address, an employer may be required to notify customers of the security breach. Numerous state laws require notification. See, e.g. 815 ILCS 5301et seq.; Michigan Code 445.72, § 12; Minnesota Code § 325E.61.

FRAUD

The CFAA requires the presence of a modified form of fraudulent intent. This term is important under Section 1030(a)(4), which provides that whoever "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 . . ." will be punished according to another provision of the CFAA. 18 U.S.C. § 1030(a)(4). It is much easier to prove fraud under the CFAA than Iowa common law. As one court has explained, fraud, in this context, means only "wrongdoing" and not proof of the common law elements of fraud. *Shurgard*, 119 F. Supp. 2d at 1126.

MISCELLANEOUS ISSUES ARISING UNDER THE CFAA: RELIEF

"Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief . . . [d]amages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages." 18 U.S.C. § 1030(g). Damages may be limited to those that result from the interruption of service. *Cenveo Corp. v. CelumSolutions Software*, 504 F. Supp. 2d 574, 581 (D. Minn. 2007). This reading of the statute indicates that lost revenues due to stolen clients are not recoverable. *Cohen*, 2008 WL 961472 at *4. "Indirect damages are recoverable, but there must be an underlying intrusion into the computer system or computer data and that 'loss' was intended to 'target remedial expenses borne by victims that could not properly be considered direct damage cause by a computer hacker." *Rickman*, 554 F. Supp. 2d at 772 (citing *In re DoubleClick Inc. Privacy Litig*., 154 F. Supp. 2d 497, 521 (S.D.N.Y. 2001)).

ADDITIONAL ISSUES: PROTECTED COMPUTER

The CFAA does not apply to all computers, but rather only to "protected" computers. However, the definition of "protected" is very broad. A protected computer is a computer that is: 1) exclusively used by a financial institution or the government, or 2) a computer used in interstate or foreign commerce. 18 U.S.C. § 1030(e)(2).

PROCEDURAL ISSUES: CIVIL ACTIONS

Although the CFAA primarily provides criminal penalties, civil remedies are also available.

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages

> and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware."

18 U.S.C. § 1030(g).

To bring a civil action, the action "must involve one of the five factors in (a)(5)(B), [but] it need not be one of the three offenses in (a)(5)(A)." *Shamrock*, 535 F. Supp. 2d at 964 (quoting *Theofel v. Farey-Jones*, 359 F.3d 1066, 1078 (9th Cir. 2004)). Therefore, civil actions can be brought for other violations of the CFAA, including 18 U.S.C. § 1030(a)(4).

CONCLUSION

The CFAA, once a rather obscure federal criminal statute, is now a powerful weapon to combat industrial espionage. Counsel representing employers would be well advised to become familiar with the CFAA.