New York Law Journal
Technology Today
TUESDAY, JULY 28, 2009
An incisivemedia publication

STATE E-DISCOVERY ISSUES

State Courts and the Federal Computer Fraud and Abuse Act

By **Mark A. Berman**

When a former employee leaves a company and there are issues as to whether he has wrongfully accessed the company's computers, servers and/or e-mail accounts, in addition to traditional common law claims of breach of fiduciary duty, unfair competition, conversion and trespass, a litigator has in her arsenal a cause of action alleging civil violation of the federal Computer Fraud and Abuse Act.[1] For instance, fraudulently obtaining information from a company's e-mail server or visiting a Web site and accessing unauthorized information from it with intent to defraud may constitute a violation of the act.

The Computer Fraud and Abuse Act (CFAA) was enacted in 1984 "to provide a clear statement of proscribed activity concerning computers to the law enforcement community, those who own and operate computers, and those tempted to commit crimes by unauthorized access to computers."[2]

Discussing amendments enacted in 1996, the Senate remarked on Congress' effort to keep up with technology, to protect both the government and private citizens, and to "remain vigilant to ensure that the [CFAA] is up-to-date and [provide] law enforcement with the necessary legal framework to fight computer crime."

An individual violates the CFAA and is subject to civil penalties when he "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, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period."[3]

ISTOCK

The act applies to computers "used in interstate or foreign commerce or communication."[4] Other grounds for violation include "knowingly [causing] transmission of a program, information, code or command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer," "intentionally [accessing] a protected computer without authorization, and as a result, recklessly [causing] damage" or "intentionally [accessing] a protected computer without authorization, and as a result of such conduct, [causing] damage and loss.[5]

Four state Commercial Division cases[6] have discussed the application of this statute, which, in each case, was narrowly construed. It is worth reviewing the CFAA when drafting a pleading as it provides grounds for "compensatory damages and injunctive relief or other equitable relief," with a two-year statute of limitations from the date of the act complained of or the date of discovery of the damage.[7]

In *Hecht v. Components International Inc.*,[8] the court granted summary judgment dismissing a counterclaim alleging violation of the CFAA, where a former CEO and shareholder of a company purportedly improperly deleted over 1,500 company e-mails using Web access to the company's e-mail server following severance of his relationship with the corporation.

The court noted that the requirement of demonstrating lack of authorization to use a company computer could be met either implicitly, if, for instance, access was protected by a password or, explicitly, where notice limiting access had been given.

Plaintiff submitted an affidavit claiming his post-resignation access to the computer system was limited to his personal files maintained on Outlook Express. While noting that the company's shutting down its server each time following plaintiff's remote access to the system implicitly established that such access was not "authorized," the court found no intent to defraud on the grounds that plaintiff only sought to obtain his personal files.

The court held that defendants failed to come forward with evidence of fraudulent intent where their computer report only revealed that plaintiff's access to the company's e-mail server was "standard," suggesting that "sensitive information was not reached."

In *Zeno Group Inc. v. Wray*,[9] a former employee allegedly deleted from the company's server documents relating to a

MARK A. BERMAN, *a partner at commercial litigation firm Ganfer & Shore, is secretary of the e-discovery committee of the Commercial and Federal Litigation Section of the New York State Bar Association.*

firm client "as well as activity reports and new business files."

The court granted summary judgment to defendant finding "there is no allegation that the server [defendant] accessed was beyond her authorization…[and that] "it strains reason that someone could delete files on a server beyond their authorization level," noting that the alleged wrongful actions did not occur after any alleged loss of "authorization."

As far as the allegations that plaintiff deleted computer files and e-mails from her laptop that had been provided to her by the company for business use prior to her departure, the court found these allegations to be "at best redundant" of plaintiff's cause of action for conversion.

Statutory 'Damage' or 'Loss'

In *Scory LLC d/b/a The Intelligent Office v. Maroney*,[10] after defendant left plaintiff's employ, he allegedly "remotely accessed [plaintiff's] computer ["to obtain [plaintiff's confidential information"] and telephone system,[11] and redirected two of [plaintiff's] toll free numbers to telephones unrelated to [plaintiff's] business."

The court noted that, while plaintiff alleged that defendant "attempted" to access the computers without "authority," it failed to allege that defendant actually obtained such access. The court noted that plaintiff further failed to provide proof that defendant obtained "anything of value" and that it sustained any "loss"[12] or "damage"[13] under the CFAA.[14]

In *Matter of Doubleclick Inc. Privacy Litigation*,[15] the court noted that "Congress intended the term 'loss' to target remedial expenses borne by victims that could not properly be considered direct damage caused by a computer hacker."

In *Alarmex Holdings, LLC v. Pianin*,[16] defendant, the former president and current owner of an equitable interest in plaintiff company, allegedly wrongfully used his company laptop to access the company's e-mail system for purposes of unfair competition and tortious interference with [plaintiff's] business relations.

Plaintiff alleged that, after defendant left the company, he used the laptop issued to him to access an e-mail account in order to obtain proprietary information, including product pricing and production in an attempt to persuade a key customer of plaintiff to place orders with him, rather than with plaintiff.

The court held that, while the proposed pleading alleged lost profits from such key account as a result of defendant's alleged wrongful access to e-mail accounts, and that he had deleted certain e-mails, this did not violate the CFAA. The court indicated that in order to maintain a cause of action under the CFAA, the complaint must allege "damage" to the company's computer system and losses related to remedying the computer or losses incurred due to an interruption in service.

Because such alleged damages did not fall within the act and because the computer utilized was only a company-issued computer that belonged to defendant, there was no violation of the CFAA.

Conclusion

Taking into account the foregoing decisions, the Computer Fraud and Abuse Act should not be overlooked when drafting a complaint alleging improper conduct by a former employee, where there is a concern that she improperly accessed the firm's computer network.

However, the statute is exacting and, as noted above, state courts narrowly construe its provisions.

The Computer Fraud and Abuse Act should not be overlooked when drafting a complaint alleging improper conduct by a former employee. However, the statute is exacting and state courts have narrowly construed its provisions.

Nevertheless, the CFAA remains a powerful tool with a built-in provision providing for injunctive and equitable relief that may be useful when a business is threatened by loss of critical data and information.[17] As such, the act should be reviewed in any application for injunctive relief, and a CFAA cause of action should be considered in addition to pleading more typical common law causes of action.

1. 18 U.S.C. §1030(a). The Computer Fraud and Abuse Act (CFAA) also provides for criminal penalties, which are not addressed herein. See 18 U.S.C. §1030(c). The CFAA does preempt state law claims. See *Hecht v. Components International Inc.*, Index No. 3371/08 at 12 (Sup. Ct. Nassau Co. Nov. 10, 2008) (citing *Pacific Aerospace & Electronics v. Taylor*, 295 F. Supp. 2d 1188, 1194 (E.D. Wash. 2003)).
2. S. REP. NO. 104-357, at *3 (1996).
3. 18 U.S.C. §1030(a)(4). See 18 U.S.C. §1130(g).
4. 18 U.S.C. §1030(e)(2)(B).
5. 18 U.S.C. §1030(a)(5)(A)-(C).
6. As this article only addresses state court decisions and given the few decisions construing the CFAA, a litigator should review relevant precedent from the federal courts to ensure that all the elements of such a cause of action are properly pleaded.
7. 18 U.S.C. §1030(g).
8. Index No. 3371/08 at 12 (Sup. Ct. Nassau Co. Nov. 10, 2008)
9. 2008 WL 4532826, Index No. 602632/06 (Sup. Ct. N.Y. Co. Sept. 26, 2008).
10. Index No. 13251/06 (Sup. Ct. Nassau Co. May 25, 2007).
11. As the CFAA does not apply to telephones, the allegation that defendant "hacked into [plaintiff's] password protected telephone system and rerouted telephone numbers does not constitute a violation of the CFAA." A computer is defined as "data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator or other similar device." 18 U.S.C. §1030(e)(1).
12. "Loss" is defined 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."18 U.S.C. §1030(e)(11).
13. "Damage" is as "impairment to the integrity or availability of data, a program, a system or information." 18 U.S.C. §1030(e)(8).
14. The CFAA provides that only a plaintiff who "suffers damage or loss by reason of a violation of this section may maintain a civil action." 18 U.S.C. §1030(g).
15. 154 F.Supp. 2d 497, 521 (S.D.N.Y. 2001) (any loss actionable under the CFAA is subject to the Act's damages minimum).
16. 2006 WL 5110875, Index No. 601987/05, at 1 (Sup. Ct. N.Y. Co. March 23, 2006).
17. S. REP. NO. 104-357, at *12.

Ganfer & Shore, LLP
360 Lexington Avenue
New York, New York 10017
212.922.9250
mberman@ganfershore.com