

New York Law Journal

Select 'Print' in your browser menu to print this document.

Copyright 2010. ALM Media Properties, LLC. All rights reserved. New York Law Journal Online

Page printed from: <http://www.nylj.com>

[Back to Article](#)

Trade Secrets and the Computer Fraud and Abuse Act

Laurie Berke-Weiss

06-15-2010

The Computer Fraud and Abuse Act (CFAA), [18 USC §1030](#), has emerged as a vehicle for trade secret misappropriation claims where a computer transmission is involved in the transfer or destruction of corporate data from a computer whose use in some way affects interstate commerce. When enacted in 1986, the CFAA was solely a criminal statute, aimed at preventing the illegal accessing of national security information through computer use and the electronic transmission of information which could harm the United States or benefit foreign nations. Amendments to the act expanded its scope to include theft and fraud via computer, altering/damaging/destroying data, and trafficking in passwords and other protected information.

In 1994, Congress added a civil private right of action to the act which has led to the inclusion of CFAA claims in private trade secret misappropriation litigation, thus affording plaintiffs federal question jurisdiction for cases which might otherwise be state court actions. See 18 USC §1030(g). As such, the CFAA is a statute tailor-made for the Internet era, where electronic transmission of data is now the norm.

The CFAA also has been the basis for criminal prosecutions of trade secret theft, adding a further dimension of risk for any employee who accesses company data for "unauthorized" purposes and meets the CFAA's jurisdictional requirements.

The Private Right of Action

Although the term "trade secret" is not mentioned in the CFAA, many of the statute's provisions are applicable to misappropriation complaints, as demonstrated by the following excerpts from the act:

(a) Whoever...

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains...

(C) information from any protected computer;...

(4) 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 one-year period;...

(5) (A) knowingly causes the transmission of a program, information code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damages and loss[;]....

18 USC §1030.

Notably, there are no statutory definitions of the terms "authority" and "transmission," leading to conflicting results in trade secret actions.¹ The question of whether the employee has "exceeded authorization" is reached only if there is a determination that the employee had authorization under the act in the first place, and is a question of fact. See Shamrock Foods Co. v. Gast, 535 F.Supp.2d 962, 967-68 (D. Ariz. 2008); Diamond Power Int'l Inc. v. Davidson, 540 F.Supp.2d 1322, 1343 (N.D. Ga. 2007) ("[A] violation for accessing 'without authorization' occurs only where initial access is not permitted. And a violation for 'exceeding authorized access' occurs where initial access is permitted but the access of certain information is not permitted").

Where cases have interpreted "without authority" broadly, there may be a finding of liability under the act. In contrast, as discussed below, in cases where the term is narrowly defined, generally no CFAA liability is found.

Defining Terms

The question of whether an employee has "authority" to obtain "information from any protected computer" is pivotal to the applicability of the CFAA to a trade secret misappropriation claim. But, the issue is unsettled in the courts, which disagree about whether an employee is authorized to access a company computer and company information by virtue of his position, even if he transmits confidential information to a new employer or to himself with the intention of competing with his old employer. Compare LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009) (narrow application of CFAA), with Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006) (broad application of CFAA).

In Citrin, a case frequently cited for its broad interpretation of the CFAA, the defendant employee was given a company laptop to collect data for his employer, a real estate company. The defendant, who later decided to go into the real estate business for himself, deleted all data in the laptop before he returned it to the company when he left the job. The defendant did not transmit the files to himself; instead, he installed a secure-erasure program on the laptop to prevent recovery of the deleted files by his employer (who had no other copies of the files); and to conceal his wrongful acts.

The U.S. Court of Appeals for the Seventh Circuit rejected defendant's argument that "merely erasing a file from a computer is not a 'transmission'" under the CFAA. *Citrin*, 440 F.3d at 419. The court found that the "transmission" requirement of the act was met by defendant's act of loading the secure-erasure program onto the company laptop. In deciding that Mr. Citrin lacked authority to make the deletion, the court ruled that his actions were a breach of the duty of loyalty, thereby terminating Mr. Citrin's agency relationship with the company, and with it his authorization to access the laptop.

In *Brekka*, the U.S. Court of Appeals for the Ninth Circuit applied the act more narrowly, finding that the defendant had authority to remove company information from his computer, even for his own use. Defendant Brekka accessed confidential corporate information while he was plaintiff's employee. He e-mailed the confidential information to his personal computer and to his wife.

Subsequently, Mr. Brekka left the company and began his own competing business. The court held that Mr. Brekka had "authorized access" to the information while working for plaintiff, and did not lose that authorization when he decided to compete with his former employer and transmit trade secret information electronically for his own benefit. In the words of the court:

[F]or purposes of the CFAA, when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the computer even if the employee violates those limitations. It is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or "without authorization."

Brekka, 581 F.3d at 1133.

Accordingly, the court held:

[A] person uses a computer "without authorization"...when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.

Id. at 1135.

Similarly, in *Jet One Group Inc. v. Halcyon Jet Holdings Inc.*, 08-CV-3980 (JS), 2009 U.S. Dist. LEXIS 72579 (EDNY Aug. 14, 2009), the CFAA was applied narrowly. Plaintiff employed the individual defendants who later were hired by plaintiff's competitor, defendant Halcyon Jet Holdings Inc. Plaintiff alleged that when the employees left, they took confidential and proprietary customer lists in violation of the CFAA. Nonetheless, the court found that the CFAA's "without authorization" requirement should be construed narrowly, and that the individual defendants had authorization when the customer lists were removed.

As such, the court noted that the CFAA "nowhere prohibits misuse or misappropriation of information that is lawfully accessed...[and] to read 'access without authorization' to mean 'misuse' or 'misappropriation' would grossly expand the statute's reach." *Id.* at 17. See also *Bro-Tech Corp. v. Thermax*, 651 F.Supp.2d 378, 407 (E.D. Penn. 2009); *State Analysis Inc. v. Am. Fin. Servs. Assoc.*, 621

F.Supp.2d 309, 317 (E.D. Va. 2009); U.S. Bioservices Corp. v. Lugo, 595 F.Supp.2d 1189, 1192 (D. Kan. 2009); Brett Senior & Assocs., P.C. v. Fitzgerald, No. 06-1412, 2007 U.S. Dist. LEXIS 50833, at 8-9 (E.D. Penn. July 13, 2007).

Damages

The question of whether and how the statutory \$5,000 damages threshold can be met is another factor in determining CFAA liability. For example, the U.S. Court of Appeals for the First Circuit, in EF Cultural Travel BV v. Explorica Inc., 274 F.3d 577 (1st Cir. 2001), determined that the costs of assessing damage done to the employer's computer system, and those costs associated with re-securing a system after a hacking attack, are permitted costs for the purpose of calculating damages under the statute.

In contrast, the U.S. Court of Appeals for the Second Circuit determined that lost revenue, such as that which is alleged to have resulted from the misappropriation of confidential data, is not a "loss" or "damage" under the CFAA, except where it results from an "interruption of service." Nexans Wires S.A. v. Sark-USA Inc., 166 Fed. Appx. 559, 562-63 (2d Cir. 2006).

In Nexans, the CFAA claim was dismissed on summary judgment because, pursuant to the court's calculation, plaintiff's CFAA damages fell short of the \$5,000 threshold. See also Shurgard Storage Ctrs. v. Safeguard Self Storage Inc., 119 F.Supp.2d 1121, 1127 (W.D. Wash. 2000) (although no data was "changed or erased," an "impairment of [] integrity occurred," and the related costs met the CFAA's damage threshold); Lockheed Martin Corp. v. Speed, Case No. 6:05-cv-1580-Orl-31KRS, 2006 U.S. Dist. LEXIS 53108, at 27 (M.D. Fla. Aug. 1, 2006) ("The copying of information from a computer onto a CD or PDA is a relatively common function that typically does not, by itself, cause permanent deletion of the original computer files," and thus did not constitute damage or loss under the CFAA).

Criminal Prosecutions

The CFAA may impose criminal liability for violations of §§1030(a)(1) through (7), or §1030(b), on employees and former employees who access, attempt to access, or conspire to access a company computer without authorization or exceeding authorization. Penalties can include imposition of a fine as well as imprisonment for as long as twenty years, depending on the provision of the CFAA which has been violated. 18 USC §1030(c). See United States v. Nosal, No. CR 08-00237 (MHP), 2009 U.S. Dist. LEXIS 31423, at 21 (N.D. Cal. April 13, 2009) (allowing case, at motion to dismiss stage, to proceed based on violations of CFAA as interpreted in civil cases).

Broader Implications

Plaintiffs commonly assert CFAA claims alongside or in conjunction with trade secret misappropriation claims, however, the two are not identical. Many courts have held that misappropriation or misuse of confidential and proprietary information is not an element of a CFAA violation. Rather, courts have viewed liability under certain CFAA provisions as "tantamount to trespass in a computer," with an intent to defraud as an additional element in specific CFAA provisions. Brett, 2007 U.S. Dist. LEXIS 50833, at 10.

Thus, even in cases where CFAA claims are dismissed, the defendant may remain exposed to a misappropriation claim. Conversely, misuse of an employer's computer without a taking of confidential information, such as in *Citrin*, may support a CFAA claim even if the trade secret misappropriation claim is dismissed.

It also remains to be seen whether courts will set limits as to what constitutes a "transmission" under the CFAA. Just as the court held in *Citrin* that loading a software program to delete information qualified as a transmission, as the nature of electronic communications evolves another court may rule that merely opening a file stored on a server or entering certain keystrokes might constitute a transmission under the CFAA. The case law should be watched closely as new technological trends emerge.

Laurie Berke-Weiss is a partner at *Berke-Weiss & Pechman*.

Endnotes:

1. The term "exceeds authorized access" is defined in the act, 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," thus begging the question of how "authorization" should be defined. 18 USC §1030(e)(6).