Shrinking Prospects for Private Trade Secret Actions Under the CFAA

BY ILANA S. RUBEL

Fenwick
FENWICK & WEST LLP

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, was enacted in 1984 as a criminal statute, but was subsequently amended in the 1990s to allow for private causes of action for damage to a "protected computer." As confidential information today is largely stored electronically, companies have increasingly turned to the CFAA in litigating the misappropriation of proprietary information.

For a variety of reasons, a CFAA claim may be a desirable supplement or even alternative to a trade secret action. Trade secret actions arise under state law, so absent diversity, a plaintiff is confined to state court. The CFAA, however, confers federal subject matter jurisdiction, enabling the suit to proceed in federal court. And, the complained-of conduct may not qualify for a trade secret action, which typically requires that misappropriated information be confidential and well-guarded. The CFAA, in contrast, merely specifies the taking of "information," an easier hurdle to clear for a plaintiff that may not be able to show strict confidentiality. However, while the CFAA has historically been a fruitful course for many trade secret plaintiffs, courts are increasingly limiting its application in trade secret cases.

Loss Requirement

Section 1030(g) of the CFAA provides that a civil action may be brought only if the conduct involves one of the following factors:

(I) loss during any 1-year period aggregating at least $ 5,000 in value;
(II) actual or potential modification or impairment of medical examination, diagnosis, treatment, or care;
(III) physical injury to any person;
(IV) a threat to public health or safety; or
(V) damage affecting a computer used by or for an entity of the U.S. Government in furtherance of the administration of justice, national defense, or national security.

Trade secret plaintiffs typically attempt to satisfy (I), with "loss" defined elsewhere in the CFAA 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."

But does loss stemming from trade secret misappropriation meet this jurisdictional requirement? Courts differ on this point, but seem to be trending in a direction that limits private CFAA actions. Some courts will accept a conclusory allegation that there was a loss of at least $5,000. *See Sam's Wines & Liquors, Inc. v. Hartig*, 2008 U.S. Dist. LEXIS 76451 (N.D. Ill. Sept. 24, 2008). Some find that an allegation of the loss of confidential information satisfies the loss requirement. *Resource Ctr. for Indep. Living, Inc. v. Ability Resources, Inc.*, 534 F. Supp. 2d 1204 (D. Kans. 2008). Most, however, are now holding that "loss" cannot consist only of lost trade secrets or related lost revenue, but must comprise costs that flow directly from the computer-access event, such as costs caused by interruption of service. *See ResDev v. Lot Builders*, 2005 U.S. Dist. LEXIS 19099 (M.D. Fla. Aug. 10, 2005); *Nexans. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 477 (S.D.N.Y. 2004).

Because many trade secret plaintiffs do incur computer-related costs (such as hiring a forensic expert to ascertain the extent of illicit access and whether any data was deleted), the stricter reading of "loss" should not preclude CFAA actions by most aggrieved trade secret holders. However, plaintiffs must be careful to plead computer-related costs in the jurisdictional amount so as not to be vulnerable to dismissal on this threshold requirement.

Available CFAA Claims

Assuming a plaintiff can show loss, it must then allege a CFAA violation. Trade secret plaintiffs will assert a CFAA claim by alleging the defendant did one or more of the following:

1. intentionally accessed a computer without authorization or exceeded authorized access, and thereby obtained information from a protected computer (1030(a)(2)(C));

2. knowingly and with intent to defraud, accessed a protected computer without authorization, or exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained anything of value (1030(a)(4));

3. knowingly caused the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer; (1030(a)(5)(A));

4. intentionally accessed a protected computer without authorization, and as a result of such conduct, recklessly caused damage; (1030(a)(5)(B));

5. intentionally accessed a protected computer without authorization, and as a result of such conduct, caused damage and loss. (1030(a)(5)(C)).

Establishing Lack of Authorization

The problem with proceeding under most of these subsections is the requirement that the access be "without authorization" or "exceeding authorization." A plaintiff can generally establish this element in the case of hacking by an outside intruder, but in the more common scenario of trade secret theft by an employee, it is more difficult. In such cases, the offending employee usually had permission to use the company computer in the course of their job duties, and thus arguably had "authorized" access to the proprietary material at issue. Plaintiffs have argued in response that authority extended only to performance of job duties, and insofar as the employee downloaded information for nefarious purposes, the access was unauthorized.

Courts are divided on whether to accept this argument. The Seventh Circuit has adopted this plaintiff-friendly view, applying agency principles to the question of authority in a CFAA claim. *Int'l Airport Ctrs, LLC v Citrin,* 440 F.3d 418 (7th Cir. 2006) held that an employee accesses a computer "without authorization" whenever the employee acquires an adverse interest to the employer or is guilty of a serious breach in loyalty, regardless of whether access was nominally permitted. A majority of courts elsewhere have rejected this view, holding that access to a protected computer occurs "without authorization" only when initial access is not permitted, and a violation for "exceeding authorized access" occurs only when initial access to the computer is permitted but the access of certain information is not permitted. Thus, if access was permitted for any purpose, the access was "authorized" under the CFAA. *See, e.g.*, *Condux Int'l, Inc. v. Haugum*, 2008 U.S. Dist. LEXIS 100949, (D. Minn. Dec. 15, 2008); *Black & Decker (US), Inc. v. Smith*, 568 F. Supp. 2d 929 (W.D. Tenn. 2008); *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322 (N.D. Ga. 2007); *Lockheed Martin Corp. v. Speed*, 2006 U.S. Dist. LEXIS 53108 (M.D. Fla. Aug. 1, 2006); *Bridal Expo, Inc. v. Florestein et al*., 2009 U.S. Dist. LEXIS 7388 (S.D. Texas, Feb. 3, 2009).

Within the Ninth Circuit, District Courts in California and Washington have followed the *Citrin* holding, while an Arizona court has rejected it. *See Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.,* 119 F. Supp. 2d 1121 (W.D. Wash. 2000); *ViChip Corp. v. Tsu-Chang Lee*, 438 F. Supp. 2d 1087 (N.D. Cal. 2006); *Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, In*c., (E.D. Cal. 2008); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 963-68 (D. Ariz. 2008). This unsettled issue is pivotal to the CFAA's future as a cause of action in trade secret cases; if the non-*Citrin* position ultimately prevails, it may severely curtail employers' ability to use the CFAA against absconding ex-employees. While the Ninth Circuit has not addressed the point, the trend elsewhere is toward a literal reading of "authorization" that would preclude many CFAA actions against employees whose access was nominally permitted.

The Damage Requirement

Several of the claims available to civil litigants (including Section 1030((a)(5)(A), the only provision encompassing authorized access) require damage, a separate and distinct element from "loss." The CFAA defines "damage" as "impairment to the integrity or availability of data, a program, a system, or information." This, again, presents a challenge to many trade secret plaintiffs. While an occasional employee may delete information in the course of a trade secret theft, more commonly the confidential information is accessed and copied, but the data itself remains on the company system, neither deleted nor impaired. Plaintiffs negotiate this hurdle by arguing that the unauthorized access itself constitutes impairment to the integrity of the data, notwithstanding the fact that the data remains intact on the company computer.

It should come as no surprise that courts vary widely on what comprises "damage." Two Washington cases are most often cited for the proposition that damage under the CFAA encompasses impairment of trade secrets. *Shurgard, supra*; *Pac. Aerospace & Electronics, Inc. v. Taylor,* 295 F. Supp. 2d 1188 (E.D.Wash. 2003). However, the majority of courts nationwide, particularly recently, have found that trade secret misappropriation alone does not meet the statutory definition of damage, and that the CFAA's use of the word "integrity" to define damage requires "some diminution in the completeness or useability of data or information on a computer system." *ResDev, supra*; *see also Garelli Wong v. Nichols*, 551 F. Supp. 2d 704 (N.D. Ill. 2008); *Andritz v. Southern Maintenance Corp*., 2009 U.S. Dist. LEXIS 694 (M.D. Ga. Jan. 7, 2009); *Sam's Wines, supra; Condux, supra*. One California case, *Therapeutic Research Faculty v. NBTY*, 488 F. Supp. 2d 991 (E.D. Cal. 2007) has followed *Shurgard*, but the Ninth Circuit has yet to address whether "damage" can be established by trade secret misappropriation alone. Because misappropriated data very often remains intact on the plaintiff's computers, many cases will be unable to proceed if a prerequisite for a CFAA claim is that the original data be altered or deleted.

The parameters of private CFAA actions are being continuously litigated, but more courts are requiring plaintiffs to show computer-related losses, impairment of the original data, and a complete lack of permitted access, curtailing the CFAA's availability in the trade secret context.

Ilana S. Rubel is a partner in the litigation group of Fenwick & West LLP, with a practice that focuses on intellectual property litigation issues. Ms. Rubel can be reached at irubel@fenwick.com.