The Litigator
e-newsletter
The Official Publication of the Litigation Section

The Computer Fraud and Abuse Act

A Potentially Potent Weapon For Employers To Combat Misappropriation Of Trade Secrets From Former Employees

Article Date: Monday, July 19, 2010

Written By: Susan H. Hargove & Courtney H. Mischen

Although confidential information readily accessible via the computer to multiple levels of employees constitutes the lifeblood of many contemporary businesses, the trade secret is the only type of intellectual property not protected by a federal statute. Graham M. Liccardi, "The Computer Fraud and Abuse Act: A Vehicle for Litigating Trade Secrets in Federal Court," 8 J. *Marshall Rev. Intell. Prop. L.*155, 156 (2008). However, the last decade has seen an expansion in the use by employer-plaintiff's of the private right of action under the federal Computer Fraud and Abuse Act ("CFAA") (18 U.S.C. § 1030,*et seq.*) as a weapon against trade secret theft by employees. To invoke the CFAA, the plaintiff is required to show that the information resided on a "protected" computer (that is, any computer used to access the Internet) and that the employee lacked (or exceeded) his authority to access the information. Liccardi, at 160. Remedies available include compensatory damages and injunctive relief. 18 U.S.C. § 1030(g).

There are several benefits to invoking the CFAA in trade secret disputes. First, whereas under state trade secret laws, the plaintiff must establish that the stolen information constitutes a legally protected trade secret, there is no such requirement under the CFAA. Liccardi, at 188. To prevail under the CFAA, the plaintiff must simply establish that the information resided on a "protected" computer. In addition, under state trade secret laws, plaintiffs must generally establish that they took reasonable steps to protect the secrecy of the information at issue. Again, there is no such requirement under the CFAA; the plaintiff must prove only that the information resided on a "protected" computer and that the employee lacked (or exceeded his) authority when accessing such information. *Id*. Finally, the CFAA gives the plaintiff the opportunity to invoke federal subject matter jurisdiction. *Id*. at 187.

To bring a civil claim for trade secret misappropriation under the CFAA, a party must establish one or more of the six applicable categories of misconduct set forth in the Act, which include:

(1) intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtaining information contained in a financial record of a financial institution;
(2) intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtaining information from any protected computer;
(3) knowingly and with intent to defraud, accessing a protected computer without authorization, or exceeding authorized access, and by means of such conduct furthering the intended fraud and obtaining 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;

(4) knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer;
(5) intentionally accessing a protected computer without authorization, and as a result of such conduct, recklessly causing damage; or
(6) intentionally accessing a protected computer without authorization, and as a result of such conduct, causing damage and loss.

Liccardi, at 161 (citing 18 U.S.C. §§ 1030(a) *et seq.*). The trade secret violation must involve at least one of five aggravating factors, the most frequently used of which is loss to one or more persons during a one-year period aggregating at least $5,000. Id. at 161-62 (citing 18 U.S.C. § 1030(c)(4)(A)(i)(1)). However, relief is limited to economic damages when the aggravating factor is loss to one or more persons during any one-year period. 18 U.S.C.. § 1030(g).

With respect to civil claims brought under the CFAA, certain issues have arisen as such claims have become more popular. Two such issues include how to establish unauthorized access and how to establish loss and damage.

The interpretation of the terms "without authorization" and "exceeds authorized access" has been the focus of many recent CFAA decisions, and there is a split in authority as to whether a broad or narrow interpretation is to be applied to these terms. The broad interpretation, which is based on agency principles, has been adopted by several district courts as well as the Seventh Circuit. In **Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.**, 119 F. Supp. 2d 1121 (W.D. Wash. 2000), plaintiff-employer filed suit alleging violations of the CFAA and state law trade secret misappropriation based on a competitor and former employee having accessed plaintiff's computer to transmit trade secrets. Shurgard presents a classic trade secrets misappropriation claim. While employed with plaintiff-employer, the defendant former employee was allowed full access to confidential business plans. One of plaintiff's direct competitors offered the former employee a job with its company. While still employed, that employee sent e-mails containing electronic trade secrets and proprietary information to the competitor. When the competitor attempted to defend plaintiff's CFAA claim on the ground that the former employee was not "without authorization" to access the information at issue, the court rejected the argument and chose to adopt a broad interpretation of "without authorization." The court found that the employee became the competitor's agent when he e-mailed trade secrets to the competitor. *Id*. at 1125. In other words, the employee lost his authorized access to the confidential information once he acted against the interests of his employer for the competitor's benefit. The Seventh Circuit has endorsed the application of the statute in a similar context, holding that unauthorized access occurs when an employee acts adversely to his employment. *See* **International Airport Centers, LLC v. Citrin**, 440 F.3d 418 (7th Cir. 2006).

Other courts have adopted a narrow interpretation of "without authorization" and "exceeds unauthorized access." Such cases reason that the CFAA applies only to outsiders (e.g., parties who never had authorization to access the computer) and to parties who had authorization to access some computers or some information, but accessed a computer or information exceeding such authorization. Liccardi, at 166. Courts applying the narrow interpretation do not consider the party's mindset when accessing the computer or information. For example, the Ninth Circuit recently rejected Citrin, refusing to apply the CFAA against an employee who e-mailed confidential documents to himself prior to leaving his job, reasoning that such an interpretation does not "comport with the plain language of the CFAA," and that criminal statutes like the CFAA must be interpreted carefully "to ensure that defendants are on notice as to which acts are criminal." **LVRC Holdings LLC v. Brekka**, 581 F.3d 1127, 1135 (9th Cir. 2009). Thus, "without authorization" is limited to a defendant who "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*.; *see also* **Lockheed Martin Corp. v. Speed**, 2007 U.S. Dist. LEXIS 51853 (M.D. Fla. July 18, 2007) (expressly rejecting Citrin's interpretation of "without authorization,"

holding instead that the CFAA only protects against wrongful access of information without authorization or access which exceeds authorization). Accordingly, there is a clear split in the Circuits with respect to when a party accesses confidential information "without authorization" or "exceeds authorized access." The Fourth Circuit has not yet weighed in on this issue.

The other major issue that has split the courts is the threshold requirement for determining damages under the CFAA. Specifically, is the act of misappropriation sufficient, or must there also be misuse? Some courts have held that the misappropriation of a trade secret, without more, constitutes "damages" under the CFAA. *See* **Shurgard**, 119 F. Supp. 2d at 1127 (holding that "damage" occurred where former employee e-mailed trade secrets to plaintiff's competitor, reasoning that 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"); *see also* **HUB Group, Inc. v. Clancy**, 2006 WL 208684 (E.D. Pa. 2006) ("damage" requirement met where employee downloaded employer's customer database to a thumb drive for use at a future employer); **Four Seasons Hotel & Resorts B.V. v. Consorcio Barr**, S.A., 267 F. Supp. 2d 1268 (S.D. Fla. 2003) (awarding $2,090,000 in compensatory damages based on the value of the trade secret information misappropriated, and $28,000 in losses based on expenses plaintiff incurred in investigating and remedying defendant's unauthorized access). Other courts have held that trade secret misappropriation in itself does not constitute "damage" under the CFAA. *See* **Garelli Wong & Assocs., Inc. v. Nichols**, 551 F. Supp. 2d 704 (N.D. Ill. 2008) (copying trade secret data alone does not constitute "damage" under the CFAA); **Resdev, LLC v. Lot Builders Ass'n**, 2005 WL 1924743 (M.D. Fla. Aug. 10, 2005) (denying recovery to plaintiffs based on the trade secret's lost value, holding that the lost value of a trade secret was not a cognizable loss under the CFAA because it was neither a "but-for" result nor a "proximate consequence" of the damage related to the unauthorized access); *see also* **Andritz, Inc. v. Southern Maintenance Contractor, LLC**, 2009 WL 48187 (M.D. Ga. Jan 7, 2009) ("loss" and "damage" do not include "lost revenue caused by the misappropriation of proprietary information and intellectual property from an employer's computer"). Once again, the Fourth Circuit has not been called upon to address this issue.

Recent statutory amendments and judicial decisions have significantly broadened the scope of the CFAA, essentially transforming it into a federal trade secrets protection act. Although the CFAA imposes several jurisdictional and other hurdles that will not make it appropriate in all situations where electronic trade secrets have been misappropriated, it has quickly become a potentially potent weapon for employers faced with misappropriation of trade secrets from former employees.

Susan H. Hargrove and Courtney H. Mischen are attorneys at Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P. in Raleigh.

Last Update: Monday, July 19, 2010