Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Can Employers Be Vicariously Liable Under The Computer Fraud and Abuse Act?

Law360, New York (November 14, 2014, 12:37 PM ET) --

Leonard A. Feiwus

Unauthorized access to electronic information can give rise to liability under The Computer Fraud and Abuse Act (the "CFAA"). In addition to state law causes of action that may be asserted, such as trade secret misappropriation, the CFAA provides a private right of action against unauthorized users who access a computer "without authorization" or who "exceed authorized access."[1] The CFAA can be a powerful weapon in a plaintiff's arsenal, particularly since it does not require a showing that the electronic information at issue was confidential or proprietary. Moreover, the CFAA is often the federal question that creates a basis for federal court jurisdiction over an action that would otherwise proceed in state court.[2]

An important question is whether, and under what circumstances, a hiring company can be held liable for CFAA violations committed by newly recruited employees. Employees often have access to large volumes of confidential, proprietary and even trade secret information in electronic format through a company's computer or data storage systems. When employees leave to go to a competitor, it is not uncommon for them to access some electronic information to bring with them to their new job.

If the departing employee violates the CFAA, can that implicate the hiring company? Courts that have directly addressed this question are divided in their approach. While some courts have reasoned that recruiting employers may be vicariously (essentially strictly) liable under the statute, other courts have gone the other way by requiring a direct violation of the CFAA by the new employer itself. Others have sought a middle ground, permitting CFAA claims based on some lesser conduct that implicates the company along with its employee, even if such conduct would not on its own constitute a direct violation of the statute.

CFAA Creates Liability Based on Unauthorized Access

The CFAA was enacted in 1986 to address the emerging problem of computer hacking and unauthorized appropriation of electronic information.[3] Under the CFAA, anyone who "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 … shall be punished." 18 U.S.C. §1030(a).

Some courts further require proof that the electronic information was altered or destroyed as opposed to merely accessed without authorization.[4] Although the CFAA was initially enacted as a criminal statute, Congress expanded the reach of the CFAA in 1994 by adding a private right of action.[5] Thus, a plaintiff may commence a civil action for damage or loss arising from a violation of the CFAA's core provisions.[6]

The CFAA is potentially broader than state law claims because the critical issue under the statute is whether a computer was accessed without proper authorization, not whether the information was commercially sensitive or proprietary.[7] Courts are also split on the interpretation of the authorization element which affects the scope of the statute.[8] Some courts read "authorization" broadly to find violations by persons who have been given authorization to certain electronic information but access it for an improper purpose. Other courts take a contrary view, finding no liability if the access was technically authorized irrespective of the intended use or purpose. The federal circuits remain divided on this issue which has yet to be addressed by the U.S. Supreme Court.[9]

Courts Are Split Over Whether Vicarious Liability Exists Under the CFAA

The language of the CFAA is silent as to whether it provides for any form of vicarious or derivative liability. On the face of the statute, liability requires "intent to defraud" on the part of the person who accesses the computer without authority, and there is no express provision creating liability based on agency. This omission, however, has not precluded some courts from looking beyond the text of the statute to apply common law principles of agency or, alternatively, imposing such liability using the CFAA's conspiracy provision.[10]

In handling derivative claims against employers, courts generally fall into one of three approaches. The first applies a narrow reading of the statute that rejects vicarious liability. Because the CFAA is primarily a criminal statute, courts may apply the rule of lenity, which "requires a court confronted with two rational readings of a criminal statute, one harsher than the other, to choose the harsher only when Congress has spoken in clear and definite language."[11]

By focusing on the requisite element of intent and applying the rule of lenity, courts in this camp have held that a recruiting employer is not a "violator" under the meaning of the statute unless the company intentionally and directly participates in the violation. For example, in *Calence LLC v. Dimension Data Holdings,* 2007 WL 1549495, at *6 (W.D. Wash. May 24, 2007), the district judge found no basis for a CFAA claim against the hiring company where there was "no evidence in the record that corporate defendants directed [the employees] to take any of the alleged improper actions." Similarly, in *Doe v. Dartmouth-Hitchcock Med. Ctr.,* 2001 WL 873063, at *5 (D.N.H. July 19, 2001), the court refused to apply vicarious liability, noting that "[e]xpanding the private cause of action created by Congress to include one for vicarious liability against persons who did not act with criminal intent … would be entirely inconsistent with the plain language of the statute."[12]

The second approach swings the pendulum in the other direction, permitting plaintiffs to tag companies with a CFAA claim simply by virtue of the agency relationship with its employees who may have violated the statute. In *SBM Site Servives LLC v. Garett*, 2012 WL 628619, at *6 (D. Colo. Feb. 27, 2012), for instance, the court found vicarious liability on the sole basis that the employee accessed plaintiff's computer "during the time that he was employed with [defendant employer] and in the scope of such

employment."[13] Notably, it was not the employer's knowledge, conduct or intent that gave rise to a CFAA violation in *SBM Site*, only the employment relationship.

The third approach finds a middle ground. Courts applying this view may find vicarious liability where there is evidence of some direct or indirect involvement by the defendant employer, even if the company lacks intent or its conduct would not by itself rise to the level of independent, direct violation of the statute. Courts in this camp differ regarding how much involvement is sufficient to be actionable. Some require only evidence that the recruiting company benefited from the breach, while others require a showing that the employer knew, or should have known, of the violation, negligently supervised its personnel or engaged in some other support of the wrongful acts.[14] Courts utilizing this approach assert that the agency relationship itself is insufficient to create a violation, but the company need not actually participate or direct the CFAA violation to be held responsible.[15]

This middle approach permits flexibility to determine vicarious liability on a fact-specific, case-by-case basis. For example in *Butera & Andrews v. International Business Machines Corp.,* 456 F. Supp. 2d 104 (D.D.C. 2006), IBM was sued because one of its employees accessed the plaintiff's computer system from an IBM IP address. Although there was a clear CFAA violation by IBM's employee, the court declined to impose any liability on IBM because there were no allegations it "tacitly knew and approved of the conduct allegedly engaged in by its employees or agents."[16] Applying the same reasoning, the court in *Synthes Inc. v. Emerge Med. Inc.,* 2012 WL 4205476 (E.D. Pa. Sept. 19, 2012) reached the opposite result, permitting vicarious liability where plaintiffs alleged that the employer "induced [employees] to access the … computer system and provide him with confidential and proprietary information."[17]

Some courts have read the CFAA's conspiracy provision as a suitable vehicle for permitting a claim against the recruiting company. For example, in *Marketing Tech. Solutions Inc. v. Medizine LLC,* 2010 WL 2034404 (S.D.N.Y. May 18, 2010), the court expressed its willingness to find liability against a company on a theory of conspiracy where the complaint alleged that it took action to reap some benefit from its employee's CFAA violation. Conspiracy, however, is not merely a theory of agency and generally requires some evidence of an agreement and overt acts by the defendant employer. *See NetApp Inc. v. Nimble Storage Inc.,* 2014 WL 1903639, at *13 (N.D. Cal. May 12, 2014) (conspiracy claim under §1030(b) failed where plaintiff did not provide "specific allegations of an agreement and common activities.").

Companies Should Have Procedures and Protocols in Place to Minimize the Risk of CFAA Liability

The current state of the law makes outcomes in these cases difficult to predict. Some courts consider a recruiting employer's knowledge of the violation sufficient to trigger vicarious liability, while others require that it actually use the appropriated data, and still others require solicitation.[18] The lack of clear judicial guidance furthers the confusion.

Recently, in *NetApp Inc. v. Nimble Storage Inc.,* a district court dismissed a claim on the basis that plaintiff "has not sufficiently pleaded vicarious liability against [the hiring employer]."[19] Yet, the court provided little insight into what allegations would have been sufficient to state a derivative claim. Moreover, the competing interpretations of the meaning of "authorization" may affect whether a court finds vicarious liability in the statute or not. Courts that have adopted a narrow interpretation, as analogous to a trespass of property, may be less inclined to find vicarious liability because the intended purpose and overall circumstances of the access is less important.

In contrast, vicarious liability may figure more prominently among courts taking a broad view of "authorization" because the overall circumstances of the access figure more prominently in the facts or the reasons why the information was initially accessed.[20] Absent clarification and binding precedent from the appellate courts, defendant companies are left to the discretion of the lower courts, whose approach may be colored by their view of what the outcome should be in a given case. As a result, plaintiffs wishing to assert a CFAA claim against employers may be encouraged to overstate the employer's involvement in the violation to ensure their claim survives the pleading stage.

The incentives exist, particularly at lower levels of the company, for the procurement and use of a competitor's information. The take-home message for companies and their counsel is clear: carefully and articulately discourage, prevent and restrict. It is important for companies to state, both informally and through official policy, that importing or even accessing and viewing internal electronic information and materials from prior employment or competitors is forbidden. Recruited personnel should be instructed to delete old company passwords and refrain from accessing past work product, especially when doing so would be beneficial for their new position. The company should have clear anti-hacking rules in place, making it firmly against company policy to access foreign electronic information without authorization or for improper purposes. If a company learns that foreign electronic information has been accessed or imported, it must move quickly to contain the information and prevent its spread and potential use within the company.

Companies can minimize their risk of exposure under the CFAA by adopting a clear, written position on the issue. Even courts that are in favor of finding some form of derivative liability under the CFAA will be less inclined to do so where the violation was unequivocally against written policy and where the company took efforts to prevent it.[21] A company that actively discourages the procurement and use of a competitor's electronic information, and takes affirmative efforts to contain it upon discovery, is far less likely to be targeted or exposed in litigation.

—By Leonard A. Feiwus, Kasowitz Benson Torres & Friedman LLP

Leonard Feiwus is a partner in Kasowitz Benson Torres & Friedman's New York office. His practice focuses on complex commercial litigation, including intellectual property and trade secret disputes. Michael Calb, an associate in the firm, greatly assisted with the preparation of this article.

---

[1] 18 U.S.C. §1030.

[2] *See* Julia J. Rider, *A Civil Litigator's Guide to the Computer Fraud and Abuse Act,* PRIVACY & DATA SEC. L. J. (April 2007); *Network Cargo Systems Int'l Inc. v. Pappas,* 2014 WL 1674650, at *3 (N.D. Ill. Apr. 25, 2014) ("With the CFAA claims (Counts I and II) providing a secure basis for federal subject matter jurisdiction, [defendant]'s argument that there is not complete diversity of citizenship between the parties is moot.").

[3] Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. §1030).

[4] *See Cassetica Software Inc. v. Computer Sciences Corp.,* 2009 WL 1703015, at *3 (N.D. Ill. June 18, 2009) ("merely copying electronic information from a computer system does not satisfy the 'damage' element because the CFAA only recognizes damage to a computer system when the violation caused a diminution in the completeness or usability of the data on a computer system"); *Consulting Professional Resources Inc. v. Concise Technologies LLC,* 2010 WL 1337723, at *7 (W.D. Pa. Mar. 9, 2010) ("CFAA liability does not arise merely by copying data"); *Condux Int'l Inc. v. Haugum,* 2008 WL 5244818, at *7-8 (D. Minn. Dec. 15, 2008) (absent allegations that employee diminished usability of computer information obtained, no CFAA damage occurred, even if employee's activities compromised confidentiality of proprietary information accessed); *but see Shugard Storage Centers Inc. v. Safeguard Self-Storage Inc.,* 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (CFAA "damage"

requirement satisfied where defendant infiltrated the plaintiff's computer network and collected and disseminated confidential information); *Black & Decker (US) Inc. v. Smith,* 568 F. Supp. 2d 929, 937 (W.D. Tenn. 2008) ("The legislative history of the [CFAA] supports the conclusion that intentionally rendering a computer system less secure should be considered 'damage' under § 1030(a)(5)(A), even when no data, program, or system, is damaged or destroyed").

[5] Pub. L. No. 103-322 §290001(g), 108 Stat. 1796 (1994).

[6] 18 U.S.C. §1030(g).

[7] *See generally* Amber L. Leaders, *Gimme a Brekka!: Deciphering "Authorization" Under the CFAA and How Employers Can Protect Their Data,* 6 WASH. J. L. TCH. & ARTS 285 (Spring 2011).

[8] Jeffrey S. Klein and Nicholas J. Pappas, "Using CFAA to Protect Confidential Information," NEW YORK LAW JOURNAL (May 9, 2014).

[9] *Compare, e.g., Int'l Airport Centers v. Citrin,* 440 F.3d 418 (7th Cir. 2006) *with WEC Carolina Energy Solutions v. Miller,* 687 F.3d 199 (4th Cir. 2012). *See The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation,* 127 Harv. L. Rev. 751, 753-54 (Dec. 2013).

[10] 18 U.S.C. §1030(b) states that "[w]hoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided by subsection (c) of this section." Among the few decisions addressing the application of this section to vicarious employer liability, most have refused to find liability.

[11] *Shamrock Foods Co. v. Gast,* 535 F. Supp. 2d 962, 966-67 (D. Az. 2008) (applying rule of lenity to CFAA), *citing Pasquantino v. United States,* 544 U.S. 349, 383 (2005).

[12] *See also Oracle Corp. v. SAP AG,* 734 F. Supp. 2d 956 (N.D. Cal. 2010) (plaintiffs could not establish that employer was "violator" under CFAA, or that liability exists under agency principles); *Larson v. Hyperion Int'l Technologies LLC,* 494 Fed. App'x 493 (5th Cir. 2012) (same); *Jagex Ltd. v. Impulse Software*, 750 F. Supp. 2d 228 (D. Mass. 2010) (same); *Role Models Am. Inc. v. Jones,* 305 F. Supp. 2d 564 (D. Md. 2004) (no vicarious liability under CFAA absent evidence that corporate defendants directed the individuals to violate the statute); *Nat'l City Bank v. Republic Mortg. Home Loans LLC,* 2010 WL 959925, at *5 (W.D. Wash. March 12, 2010) ("Although vicarious liability is the norm in tort law, the CFAA is primarily a criminal statute designed to punish intentional frauds").

[13] *See also PNC Mortg. v. Superior Mortg. Corp.,* 2012 WL 628000, at *30 (E.D. Pa. Feb. 27, 2012) (vicarious liability permissible where wrongful act of employee took place within scope of employment).

[14] *See, e.g., Binary Semantics Ltd. v. Minitab Inc.,* 2008 WL 763575, at *5 (M.D. Pa. March 20, 2008), *vacated in part on other grounds,* 2008 WL 1981591 (M.D. Pa. May 1, 2008) (employer may be vicariously liable where employer hired employee in an attempt to bring trade secrets into the company).

[15] *See C.H. Robinson Worldwide Inc. v. XPO Logistics Inc.,* 2013 WL 6222075, at *21 (Minn. Dist. Ct. Aug. 29, 2013) (vicarious liability permissible where employer "encouraged, and/or condoned" employee accessing plaintiff's computer in violation of CFAA); *Joe N. Pratt Ins. v. Doane,* 2008 WL 819011, at *2 (S.D. Tex. Mar. 20, 2008) (employer may be liable "based on agency, aiding and abetting, ratification, vicarious liability and conspiracy grounds" for knowing of the conduct and assisting in bringing the conduct to fruition).

[16] *Butera & Andrews,* 456 F. Supp. 2d at 113.

[17] *Synthes,* 2012 WL 4205476 at *17. *See also Southeastern Mech. Servs. Inc. v. Brody,* 2008 WL 4613046, at *14 (M.D. Fla. Oct. 15, 2008) ("[w]here a new employer seeks a competitive edge through the wrongful use of information from the former employer's computer system, plaintiff will likely win on the merits of a CFAA claim"); *Shurgard Storage Centers Inc. v. Safeguard Self Storage Inc.,* 119 F. Supp. 2d 1121, 1124-25 (W.D. Wash. 2000) (holding that defendant violated CFAA because plaintiff's employee acted as an agent for defendant and sent emails to defendant containing trade secrets and proprietary information belonging to plaintiff).

[18] Courts sometimes justify vicarious liability in the absence of an express provision for it in the statute by arguing that the CFAA operates, in effect, like a tort action, and "when Congress creates a tort action, it legislates against a legal background of ordinary tort-related vicarious liability rules and consequently intends its legislation to incorporate those rules." *Charles Schwab & Co. v. Carter,* 2005 WL 2369815, at *5 (N.D. Ill. Sept. 27, 2005), *quoting Meyer v. Holley,* 537 U.S. 280, 285 (2003).

[19] 2014 WL 1903639, at *13 (N.D. Cal. May 12, 2014).

[20] *See Leaders, supra* n.7.

[21] *See Joe N. Pratt Ins. v. Doane,* 2009 WL 3157335, at *4 (S.D. Tex. Sept. 25, 2009) (no agency, and thus no CFAA liability, existed where employee's actions were outside the scope of the authority granted by employer).