Portfolio Media. Inc. | 648 Broadway, Suite 200 | New York, NY 10012 | www.law360.com
Phone: +1 212 537 6331 | Fax: +1 212 537 6371 | customerservice@portfoliomedia.com

Establishing CFAA Violations By Former Employees

Law360, New York (October 27, 2009) -- In the recent LVRC Holdings LLC v. Brekka, Case No. 07-17116, 2009 WL 2928952 (9th Cir. Sept. 15, 2009) case, the Ninth Circuit Court of Appeals joined a growing number of federal courts that have limited the use of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, in suits brought against former employees accused of taking electronic data from a company's computer system before leaving the company.

In LVRC Holdings LLC, the court affirmed the district court's summary judgment in favor of the defendants on the employer's CFAA claim.

The court found that because the employee was authorized to use his employer's computers while he was employed at the company, he did not access a computer "without authorization" in violation of § 1030(a)(2) or § 1030(a)(4) when he e-mailed documents to himself and to his wife before leaving the company.

The court also found that the employee did not "exceed authorized access" when he e-mailed the documents because he was entitled to obtain the documents.

Further, the court held that the employer failed to establish the existence of a genuine issue of material fact as to whether the employee accessed the company Web site without authorization after he left the company.

After LVRC Holdings LLC, an employer litigating in the Ninth Circuit cannot maintain CFAA claims against a former employee who e-mailed company data to her personal account premised simply on allegations that the former employee acted "without authorization" or "in excess of authorization" because she was acting as the agent of her new employer or because she had taken the data in breach of her duty of loyalty to her former employer.

Instead, in order to maintain a CFAA claim, the former employer must identify what steps it

took or policies it promulgated to define for its employee what constituted authorized and unauthorized access and demonstrate how the employee exceeded her authorization.

Even then, if the employer provided the employee with general access to its computer network and did not have adequate network safeguards in place to protect sensitive matter, the employer may have a difficult time establishing a violation of the CFAA.

The LVRC Holdings LLC v. Brekka Decision

In LVRC Holdings LLC, the plaintiff LVRC Holdings LLC hired the defendant Christopher Brekka to conduct Internet marketing and to interact with the company LVRC retained to provide e-mail, Web site and related services for LVRC's residential treatment center for addicted persons, located in Nevada.

While Brekka worked for LVRC, he commuted between Florida and Nevada, and he e-mailed to his personal computer documents he obtained or created in connection with his work.

LVRC and Brekka had no written employment agreement or confidentiality agreement, and LVRC had promulgated no guidelines prohibiting its employees from emailing LVRC documents to personal computers.

Several months after it hired Brekka LVRC and Brekka entered into discussions regarding the possibility of Brekka purchasing an ownership interest in LVRC.

Soon after, Brekka e-mailed to his personal e-mail account and his wife's personal e-mail account a number of LVRC documents, including a financial statement for the company, LVRC's marketing budget and admission reports for patients.

Ultimately, discussions regarding Brekka's potential ownership interest broke down and Brekka stopped working for LVRC. More than a year later, LVRC discovered that someone had logged into the LVRC Web site using Brekka's log-in information.

LVRC notified the FBI and sued Brekka, alleging Brekka violated the CFAA when he e-mailed LVRC documents to himself and when he allegedly accessed the LVRC Web site after he left LVRC.

LVRC then brought an action in federal court, alleging that Brekka violated the CFAA when he e-mailed LVRC documents to himself and when he continued to access the Web site after he left LVRC. In addition, LVRC brought a number of state tort claims.

The Nevada federal district court (Kent J. Dawson, presiding) granted summary judgment on LVRC's CFAA claims in favor of Brekka.

After dismissing the federal law claims, the district court declined to exercise supplemental jurisdiction over the remaining state law claims and dismissed the case.

The Ninth Circuit (opinion written by Judge Sandra S. Ikuta) affirmed the district court's ruling.

The court analyzed the plain language of the CFAA statute. It held that "a person uses a computer 'without authorization' under §§ 1030(a)(2) and (4) 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."

The court concluded that "[n]o language in the CFAA supports [plaintiff's] argument that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest.

The court instructed that "[t]he plain language of the statute [ ] indicates that 'authorization' depends on actions taken by the employer."

"If the employer has not rescinded the defendant's right to use the computer, the defendant would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA."

Although there appeared to be grounds to distinguish the case on its facts, the Ninth Circuit explicitly rejected the Seventh Circuit Court of Appeals' reasoning in International Airport Ctrs. LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006) (Judge Posner, presiding), in which the Seventh Circuit held that a defendant employee's authorization to access his employer's computer files terminated when he violated his duty of loyalty to his employer.

It also may have implicitly overruled, or at a minimum, limited the utility of, the 2000 decision in Shurgard Storage Ctrs. Inc. v. Safeguard Self Storage Inc., 119 F.Supp.2d 1121 (W.D.Wash. 2000), the first federal court decision to support the theory that unauthorized access under the CFAA may be alleged where an employee accesses his or her employer's computers to obtain information the employee will purportedly use to benefit a competitor.

However, the Brekka decision did not go so far as to define “unauthorized access” to apply solely to outsiders who do not have permission to access the plaintiff's computer in the first place, as a number of federal trial courts have decided.

It is more closely aligned with the reasoning of the Arizona district court decision in Shamrock Foods v. Gast, 535 F.Supp.2d 962 (D.Ariz. 2008), which held that 1) a violation for accessing a protected computer “without authorization” occurs only when the initial access is not permitted; and 2) an “exceeds authorized access” violation occurs only when initial access to a protected computer is permitted but the access of certain information is not permitted.

Of note, the LVRC Holdings LLC decision appears to contradict the court’s reasoning in the first case interpreting 18 U.S.C. § 1030(a)(4) in the criminal context, United States v. Nosal, No. CR 08-00237 MHP, 2009 WL 981336 (N.D. Cal. April 13, 2009).

In Nosal, the indictment asserted that the CFAA was violated when the former employee accessed his former employer’s computer network while employed to obtain proprietary information for use in competing with his former employer.

The court focused on the “intent to defraud” language of § 1030(a)(4), which targets those who “knowingly and with intent to defraud, access[] a protected computer without authorization, or exceed[] authorized access ...” and defined the “initial gravamen of the CFAA charge” as “the initial access of the employer's computer with the intent to defraud.”

The court found that the indictment sufficiently alleged a CFAA violation where the former employee’s accessing of his former employer’s information was purposeful and with intent to defraud, i.e., to benefit his own competing business, to the detriment of his former employer.

LVRC Holdings LLC’s Impact on Employers

CFAA claims have become common where former employees have transmitted company electronic data outside the company for their personal benefit or other improper purpose because the CFAA provides a basis for federal jurisdiction and allows aggrieved employers to obtain injunctive relief on the basis of CFAA violations alone.

The CFAA claim provides a remedy without having to prove the violation of an employment agreement, including the actual or threatened dissemination of proprietary or confidential

information.

In addition, the aggrieved employer need not prove that the information taken is trade secret or confidential. So long as an employer can prove “unauthorized access” to a protected computer and the requisite damages, it can obtain a remedy under the CFAA, including injunctive relief.

In light of the Ninth Circuit’s definition of “unauthorized access” and “access in excess of authorization,” employers must educate their employees about what constitutes permissible computer use.

They may need to rethink their strategies for protecting company property and ensure that they have adequate computer security protections and confidentiality agreements in place.

For example, employers must ensure that they have clear computer usage policies that outline acceptable computer usage. They should also be mindful of what access they provide their employees to key company data.

Employers may not be able to maintain CFAA claims against employees who transmit such data for their personal use or other improper purpose if they were originally provided access to the data as part of their employment.

Employers should also make sure that key company data is provided only to those who genuinely need access to it and should monitor access to such information.

Even if there are clear written policies prohibiting certain access by employees, if the company carelessly provides employees with general access to its computer network and fails to protect sensitive matter, the employer may have a difficult time establishing a violation of the CFAA or other state claims.

A comprehensive trade secret audit is a strong first step in ensuring that an employer’s most important information is adequately protected.

LVRC Holdings LLC will not affect potential CFAA claims involving the transmission of programs, information, codes or commands that destroy data, or claims in which the former employee accessed the employer’s data after termination of employment.

Nonetheless, following LVRC Holdings LLC, we may see fewer trade secret/unfair competition suits (which frequently include CFAA claims) involving rogue former employees

and competitors in federal court in the Ninth Circuit.

Unless there is diversity jurisdiction, these types of claims will need to be brought in state court. Employers can enhance their ability to maintain such suits in the Ninth Circuit by ensuring that they have clear computer usage policies that are enforced.

--By Robert B. Milligan and Carolyn E. Sieve, Seyfarth Shaw LLP

Robert Milligan is a partner and Carolyn Sieve is a senior associate with Seyfarth Shaw LLP in the firm's Los Angeles office.

The opinions expressed are those of the authors and do not necessarily reflect the views of Portfolio Media, publisher of Law360.
