O'Melveny

Alerts & Publications

Employers Beware - Ninth Circuit Ruling May Limit Federal Recourse Against Employees Who Access Company Information for Improper Purposes

January 1, 0001

The Ninth Circuit's recent decision in *LVRC Holdings LLC v. Brekka*, 09 C.D.O.S. 11785 (9th Cir. Sept. 15, 2009), may make it more difficult for employers to use the Computer Fraud and Abuse Act (18 U.S.C. § 1030) (the "CFAA") to protect company information from rogue employees. The Ninth Circuit held that an employee who is "authorized" to access his or her employer's computers does not violate the CFAA even if the employee uses that access in breach of his or her duty of loyalty by using the information for an improper purpose. This decision narrows the application of the CFAA in the Ninth Circuit, but the CFAA remains a valuable tool for holding employees liable in actions under subsections of the statute not depending on "unauthorized access" and in actions against former employees who access their employers' computers after their authorization is rescinded. Further, *Brekka* suggests that by carefully defining the extent of employees' authorization, employers may continue to assert a claim if the employees exceed their authorization.

Congress enacted the CFAA in 1984 as a criminal statute focused on computer hacking. A private right to sue was added in 1994, but for several years the CFAA remained primarily a computer hacking statute, applicable to cases in which strangers hacked into computers to steal or damage information. In 2000, however, courts began applying the CFAA to situations involving employee access to company information. For example, *Shurgard Storage Centers, Inc. v. Safeguard Self Storage*, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000), held that an employee violated the CFAA by accessing company information for personal reasons contrary to the employer's interest. In the following years, employers used the CFAA with increasing frequency "to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system." *P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC*, 428 F.3d 504, 510 (3d Cir. 2005).

Traditionally, state trade secret law provided one important means for protecting confidential information. Trade secret law, however, does not protect all important company information. For example, to qualify as a protectable trade secret, the information must have economic value because it is not generally known to the public (or one's competitors), and it must have been subject to reasonable efforts to keep it secret. The trade secret owner also must prove that the information was subject to actual or threatened misappropriation. *See e.g.* Cal. Civ. Code § 3426 *et seq*. The availability of the CFAA to protect against employee access to company information, therefore, provides a more complete remedy. It also allows actions to be brought in federal court.

Several sections of the CFAA provide a remedy against those who access computer information "without authorization" or in a manner that "exceeds authorized access." For example, it is a violation of the CFAA to intentionally access a computer without authorization or to exceed authorized access and thereby obtain information from a computer used in or affecting interstate or foreign commerce. 18 U.S.C. § 1030(a)(2)(C), (e)(2)(B). Starting with *Shurgard*, a number of courts interpreting "authorization" held that an employee loses authorization to access information in a company computer when the employee acts contrary to the employer's interest. *See, e.g., International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), *see also EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001). Thus, the CFAA has become a powerful tool in defending corporate computer information against misappropriation.

But the Ninth Circuit's decision in *Brekka* interprets the CFAA much more narrowly, and may leave employers in the Ninth Circuit more vulnerable to some kinds of employee misconduct. *Brekka* involved claims by an employer, LVRC Holdings, that its former employee, Brekka, had violated the CFAA by improperly emailing company documents to his personal computer during his employment. LVRC hired Brekka to oversee a number of aspects of LVRC's rehabilitation facilities. Thus, while employed, Brekka had permission to access LVRC's computer information, and, in fact, his job required him to use the computer. Brekka commuted between his home in Florida and LVRC's business in Nevada and consequently often emailed company documents to his personal computer to use them in his work. When Brekka left his employment several months after a falling out with the company, LVRC discovered the emails in which Brekka sent documents to his personal email account, including some emails near the time of his departure. LVRC sued Brekka contending that he misappropriated trade secret information and violated the CFAA by emailing documents to his personal computer before his departure from the firm in order to use them in a competing business. Relying on the CFAA, the employer filed the case in federal court and did not have the burden of proving that Brekka took information that qualified as trade secret.

The Ninth Circuit held that Brekka's alleged conduct did not constitute a violation of the CFAA because Brekka did not access the documents "without authorization." The Court rejected the rule that an employee loses authorization under the CFAA by accessing the employer's information for improper purposes or, in violation of his or her duty of loyalty to the employer. Instead, Court held that "without authorization" means "without any permission at all" and an employee with permission to use a company computer remains authorized to use the computer unless and until the permission is rescinded. If the employer imposes limitations on the employee's authorization to use the computer, the employee may be liable for "exceeding authorized access" under the CFAA.

Applying these standards, the Ninth Circuit found that Brekka did not have a written employment agreement with LVRC, nor did LVRC have employee guidelines prohibiting employees from emailing company documents to their personal computers. Accordingly, the Court held that Brekka did not access the employer's computers "without authorization," nor did he "exceed authorized access" during the time he was employed.

In its ruling, the Ninth Circuit expressly rejected the approach taken by the Seventh Circuit in *Citrin*, which held that an employee lost authorization to use a company computer when the employee breached the duty of loyalty by acting contrary to the employer's interest. *Citrin*, 440 F.3d at 420-21. The Ninth Circuit, by contrast, held that the employee's authorization was not terminated until the employer affirmatively rescinded his or her authorization.

Because of the direct conflict of authority among Circuit Courts, the meaning of the term "authorization" as used in the CFAA may eventually require Supreme Court review. Within the Ninth Circuit, a disloyal employee may now be able to escape liability for "unauthorized access" under federal law for accessing his or her employer's computer for an improper purpose. The Seventh Circuit in *Citrin* directly authorized such a claim, and other Circuits (including the First in *Explorica* and the Third in *P.C. Yonkers*) appear to support its reasoning. The law is unsettled in other Circuits, and a claim under CFAA may remain viable.

Even within the Ninth Circuit, however, the CFAA remains a valuable tool for redressing employees' computer-related misconduct. First, *Brekka* does not impact claims under the CFAA that are not dependent upon establishing "unauthorized access." For example, the CFAA makes it unlawful for anyone to impair the availability or integrity of information on a protected computer system. Thus, where an employee does not merely copy data, but also destroys the original copy of that data on the employer's computer system, the employee has violated the CFAA regardless of whether the employee was authorized to access the computers. The Ninth Circuit had no occasion to consider such claims in *Brekka*, and its holding does not impact the viability of those claims.

Second, *Brekka* does not impact claims under the CFAA against former employees who access the company's computers after their employment is terminated. For example, due to delays or problems in deactivating an employee's password, or because an individual knows the passwords of other employees, a former employee may be able to gain continued access to a company's computers even after being terminated. The Ninth Circuit in *Brekka* expressly recognized that such a former employee could be held liable: "There is no dispute that if Brekka accessed LVRC's information on [LVRC's protected] website after he left the company in September 2003, Brekka would have accessed a protected computer 'without authorization' for purposes of the CFAA." Although the court found that there was insufficient evidence in that case to prove that the employee had, in fact, accessed the computer following his termination, the Ninth Circuit's decision does not affect the general viability of such a claim.

Third, *Brekka* permits employers to expressly limit the scope of employees' access to a company computer. Employers should, where feasible, provide written policies limiting employees' authorization to access company information (such as prohibitions on employees emailing company documents to personal accounts) and specifying the purposes for which such information may be accessed. Indeed, the Ninth Circuit noted the absence of such policies in the Brekka case and hinted that employees who violate written computer access policies may "exceed authorized access" in violation of the CFAA. After all, as the owner of the computer systems and the information stored therein, employers are in a unique position to define the extent to which employees are "authorized" to access those computers.

In sum, *Brekka* does not remove the CFAA from the toolbox of employers seeking to protect their information, but it does limit the CFAA's ability to remedy certain misconduct by employees in certain circumstances, at least within the Ninth Circuit. Until the Supreme Court resolves the split of authority created by *Brekka*, employers in the Ninth Circuit would be well-advised to take steps to clearly delineate the scope and purpose for which employees are authorized to access information.