FORD & HARRISON LLP
THE RIGHT RESPONSE AT THE RIGHT TIME
LETTER
NONCOMPETE NEWS

Noncompete News: The Computer Fraud And Abuse Act Isn't Just For Computer Hackers Anymore; The Ninth Circuit Extends Its Protection To Employee Data Theft

6/29/2011

Executive Summary: The Ninth Circuit recently held that the Computer Fraud and Abuse Act (CFAA) is not limited to computer hackers, but also applies to employees who exceed their "authorized access" set forth in their employer's computer usage policy. ***Background*** The Ninth Circuit's recent ruling in *United States v. Nosal****[1]*** gave California employers a boost of confidence in their ability to protect themselves against employee data theft. Nosal was charged with violations of the CFAA after he attempted to start a competing business by taking a highly confidential database owned by his former employer, exceeding the company's computer usage policy to obtain that information. Nosal sought to have the indictment dismissed, arguing that the CFAA only applied to "computer hackers." The Ninth Circuit disagreed and made clear that the CFAA applies to employees who exceed their "authorized access" set forth in their employer's computer usage policy and that they will be liable for any resulting loss.[2] The CFAA is a criminal statute, but also provides for a civil right of action for persons who are the victims of employee data theft. The Act punishes any person 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."[3] For any violation of the Act, an employer may obtain "compensatory damages and injunctive relief or other equitable relief."[4] ***Nosal's Theft of His Employer's Client Database Was A Violation of CFAA Because He Exceeded His Authorized Access As Set Forth In The Company's Computer Usage Policy*** Nosal worked for an executive search firm (Korn/Ferry) that required all of its employees to enter into agreements that explained the confidential nature of company information and restricted the use and disclosure of such information. In addition to the agreement, when an individual logged into the Korn/Ferry computer system, the following notification displayed: This computer system and information it stores and processes are the property of Korn/Ferry. You need specific authority to access any Korn/Ferry system or information and to do so without the relevant authority can lead to disciplinary action or criminal prosecution. Shortly after Nosal left his employment, he engaged three Korn/Ferry employees to help him start a competing business by transferring a highly confidential database of executives and companies owned by Korn/Ferry. The Government charged Nosal with violations of the CFAA for violation of his employer's computer usage policy and theft of the employer's confidential information for an improper use. Nosal moved to dismiss the indictment, arguing that the "CFAA was aimed primarily at computer hackers and that the statute does not cover employees who misappropriate information or who violate contractual confidentiality agreements by using employer-owned information in

a manner inconsistent with those agreements."[5] The District Court agreed and dismissed the indictment. It relied on the Ninth Circuit's prior ruling in *LVRC Holdings, LLC v. Brekka**[6]*** in determining that "an employee does not exceed authorized access to a computer by accessing information unless the employee has no authority to access the information under any circumstances."[7] "In other words, an employer's restrictions on the use of the computer or of the information stored on that computer are irrelevant to determining whether an employee has exceeded his or her authorization."[8] The Ninth Circuit reversed and held that because Nosal was subject to a computer usage policy that placed "clear and conspicuous restrictions" on his access to the system, as well as the database, Nosal had fair warning that he was subjecting himself to criminal liability.[9] Thus, as long as the employee has knowledge of the employer's limitations on that authorization, the employee "exceeds authorized access" when the employee violates those limitations. ***The Ninth Circuit's Prior Ruling In Brekka Turned On The Language of the Employer's Computer Usage Policy That Allowed For Unfettered Access*** In the Ninth Circuit's prior ruling in *Brekka*, the court held that a violation of the CFAA can be found only when an employee "has not received permission for any purpose,"[10] which appears to be inconsistent with the recent holding in *Nosal*. However, the different rulings can be explained by the different computer usage policies at issue in each case. LVRC's computer usage policy allowed Brekka to have unfettered access to the company's computers. The company did not have a written employment agreement with Brekka nor did it prohibit employees from e-mailing company documents to personal computers. During his employment, Brekka and LVRC entered into discussions regarding the possibility of Brekka obtaining an ownership interest in LVRC. During this time, Brekka e-mailed himself a number of LVRC documents to his personal e-mail account including a financial statement for the company, LVRC's marketing budget, admissions reports for patients and a master admissions report containing the names of past and current patients. Ultimately, negotiations regarding Brekka's purchase of an ownership interest in the company broke down and Brekka ceased working for the company. LVRC sued Brekka for violations of the CFAA once it discovered that he took confidential information before he resigned. Despite Brekka's brazen misappropriation of confidential information, the Ninth Circuit upheld a dismissal of the CFAA claims because Brekka did not exceed his authorized access to the company's computer system. In other words, because the computer usage policy did not restrict Brekka's access to the system in any way, there was no violation of the CFAA. The *Nosal* decision clarifies that under the CFAA a violation may occur when the employee's access "violates the employer's access restrictions, which may include restrictions on the employee's use of the computer or of information contained in that computer."[11] ***Will Millions Of Employees Be Subject To Criminal Liability If They Exceed Authorized Access By Using Their Work Computers For Personal Use?*** The short answer is No. CFAA does not criminalize mere violation of an employer's computer usage policy. The act requires: (1) a violation of the employer's restrictions; (2) an intent to defraud; and (3) the employee's action must further the intended fraud and obtain something of value.[12] The requirements of fraudulent intent and obtaining something of value negate any effort to impose civil and/or criminal liability on an employee who accesses personal e-mail accounts or sports news on his or her work computer. **Employers' Bottom Line:** An employer's computer usage policy must place clear and conspicuous restrictions on its employees' access to the computer system and any database that contains trade secret, confidential and/or proprietary information. If employees are not subject to a strict policy, it may be difficult for an employer to bring a civil action for theft of its information unless that information has independent trade secret protection. If you have any questions regarding this decision or other labor or employment related issues, please contact the author of this article, Michelle Abidoye, mabidoye@fordharrison.com, an attorney in our Los Angeles office or the editor of the *Noncompete News*, Jeff Mokotoff, jmokotoff@fordharrison.com, a partner in our Atlanta office.

[1] *United States v. Nosal*, 2011 U.S. App. LEXIS 8660 (9th Cir. April 28, 2011).
[2] The CFAA defines "loss" as any "reasonable cost to any victim, including the cost of responding to an offense, conducting a damages 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 because of the interruption of service." *See* 18 U.S.C. § 1030(e)(11). Thus, any alleged loss of business due to the ex-employee's use of the stolen information is not conferred by the CFAA because it only applies to damages related to interruption of the computer service. *See Nexans Wires, S.A. v. Sark-USA, Inc.*, 319 F.Supp.2d 468, 477-78 (S.D.N.Y. 2004) (holding that travel costs of senior executives and loss of revenue unrelated to the interruption of computer service is not considered a "loss" pursuant to the CFAA); *see also Resdev, LLC v. Lot Builders Ass'n,Inc.* 2005 U.S. Dist. LEXIS 19099 (M.D. Fla. 2005) (rejecting the argument that "loss" can cover a trade secret's exclusivity value).

[3] 18 U.S.C. § 1030(a)(4).

[4] *See* 18 U.S.C. § 1030(g).

[5] *Nosal*, 2011 U.S. App. LEXIS 8660 at *7.

[6] 581 F.3d 1127 (9th Cir. 2009).

[7] *Nosal*, 2011 U.S. App. LEXIS 8660 at *2.

[8] *Id.*

[9] *See Nosal*, 2011 U.S. App. LEXIS 8660 at *16.

[10] *Brekka*, 581 F.3d at 1135.

[11] *Nosal*, 2011 U.S. App. LEXIS 8660 at *21.

[12] *See* 18 U.S.C. § 1030(a)(4).