

Suing employees for computer fraud gets easier

Four separate circuit court rulings this year enhanced the ability of businesses to use Computer Fraud and Abuse Act.

BY NICK AKERMAN

Four recent decisions handed down by four different federal courts of appeals during the past year have, in combination, greatly enhanced the ability of businesses to use the Computer Fraud and Abuse Act (CFAA) as a tool to protect competitively sensitive data and personal information stored in company computers. The CFAA is the federal computer crime statute that permits companies that have been victimized by theft or

destruction of data to file a civil action against the perpetrator for damages and injunctive relief. 18 U.S.C. 1030(g).

The U.S. Court of Appeals for the 9th Circuit settled the issue of an employer's ability to use the CFAA against employees, although just last week it granted an en banc rehearing of its decision; the 6th Circuit permitted the statute to be used against a labor union that shut down an

2011). In *Nosal*, the 9th Circuit clarified its earlier decision in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1131 (9th Cir. 2009), which up until now had been relied upon by numerous district courts in and out of the 9th Circuit as a bar to using the CFAA against employees who stole their employer's computer data. A key element to prove either a civil or criminal violation of the CFAA is that the employee accessed the company computer "without authorization" or "exceeded [ed] authorized access." *Brekka* had been predicated on the simplistic proposition that employees have permission to access the company computers and, thus, by definition cannot access the company computers without authorization.

David Nosal, a Korn/Ferry International executive, was indicted for stealing confidential data from the company computers prior to joining a competitor. Nosal had allegedly recruited "three Korn/Ferry employees to help him start a competing business." *Id.* at 782. The indictment charged these employees with "using their user accounts to access the Korn/Ferry computer system." They then "transferred to Nosal source lists, names, and contact information from the



'Searcher' database—a 'highly confidential and proprietary database of executives and companies'—which was considered by Korn/Ferry 'to be one of the most comprehensive databases of executive candidates in the world.' " *Id.*

The district court had initially rejected Nosal's motion to dismiss the CFAA counts but reversed its decision after the *Brekka* decision. The government appealed, citing Korn/Ferry's computer policies that restricted the scope of its employees' access to the company computers including one that "restricted the use and disclosure of all such information, except for legitimate Korn/Ferry business." *Id.* The government argued that, based on these policies, Nosal had exceeded authorized access. The court agreed, citing the statutory definition of "exceeds authorized access," which is "to access a computer with authorization and to use such access to obtain or alter

THE PRACTICE

Commentary and advice on developments in the law

employer's computer system through a massive spam attack; the 3d Circuit broadened the definition of unauthorized access to the company computer to mean accessing without a business purpose; and the 8th Circuit expanded the definition of what it means to obtain information from the computer to include the simple viewing of data as opposed to physically taking or copying data.

The most significant of these decisions is *U.S. v. Nosal*, 642 F.3d 781 (9th Cir. 2011), reh'g en banc granted (Oct. 27,

information in the computer that the accesser is not entitled so to obtain or alter." The court held that the word "so" "refers to an accesser who is not entitled to access information in a certain manner." *Id.* at 785. Thus, the court held that "an employee 'exceeds authorized access' under § 1030 when he or she violates the employer's computer access restrictions—including use restrictions." *Id.*

The 9th Circuit distinguished *Brekka* based on the lack of computer policies governing Christopher Brekka's right to access the company computers: "Because [the employer] had not notified Brekka of any restrictions on his access to the computer, Brekka had no way to know whether—or when—his access would have become unauthorized." The court found that "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." *Id.* at 787, 788.

After *Nosal* it is now universally accepted among the federal circuit courts that have addressed this issue that the CFAA applies to employees who violate company computer policies limiting the scope of their access to the company computers. The 6th Circuit in *Pulte Homes Inc. v. Laborers' International Union of North America*, 648 F.3d 295, 299 (6th Cir. 2011), went one step further and upheld a CFAA complaint against not a single employee but a labor union that in the course of a labor dispute had "bombarded" the computer systems of the employer's sales and executive offices with e-mails and voicemails, making it impossible for the company to communicate with its customers and vendors.

The complaint alleged that "[t]o generate a high volume of calls,...[the union] both hired an auto-dialing service and requested its members to call Pulte [Homes, a homebuilder]. It also encouraged its members, through postings on its website, to 'fight back' by using...[the union's] server to send e-mails to specific Pulte executives. Most of the calls and e-mails concerned Pulte's purported unfair labor practices, though some communications included threats and obscene language." *Id.*

The CFAA claim charged the union with "knowingly caus[ing] the transmission of a

program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer." 18 U.S.C. 1030(a)(5)(A). The CFAA defines damage as "any impairment to the integrity or availability of data, a program, a system, or information." The court found the CFAA allegations sufficient in that "the transmissions diminished Pulte's ability to use its systems and data because they prevented Pulte from receiving at least some calls and accessing or sending at least some e-mails," and the complaint showed that the union acted "with the conscious purpose of causing damage (in a statutory sense) to Pulte's computer system." *Id.* at 301, 303.

The 3d Circuit's decision in *U.S. v. Tolliver*, 2011 WL 4090472 at *1 (3d Cir. Sept. 15, 2011), made clear that company policies, such as those relied upon in *Nosal*, are not the only way to prove that an employee accessed the company computer "without authorization." The court upheld the CFAA conviction of Regina Tolliver, a former bank teller for Citizens Bank who provided confidential customer account information to "check runners" who "cashed fraudulent checks against the accounts of seven Citizens Bank customers in branches in upstate New York, western Pennsylvania, and Delaware." *Id.* Without reference to any bank policies, the court held that "there was sufficient evidence" upon which "the government established that Tolliver exceeded her authorized access" because "she did not have a business purpose" to access the customers' accounts. *Id.* at *5.

While Tolliver actually removed data from her employer's computer, the employee in *U.S. v. Teague*, 646 F.3d 1119 (8th Cir. 2011), only viewed data in the computer, did not remove it and did not use it. Yet the 8th Circuit applied the CFAA to these facts and, in doing, upheld the criminal conviction of Sandra Teague, an employee of a government contractor for the U.S. Department of Education, for accessing President Obama's record in the National Student Loan Data System. She had been convicted of violating the CFAA for exceeding unauthorized access to a computer in violation of 18 U.S.C. 1030 (a)(2)(B). This section makes it a crime to intentionally exceed authorized access to a computer and obtain information from the computer.

Based solely on her viewing the Obama student loan data, the court found the government had proved the critical CFAA element of having obtained information.

Although not acknowledged by the 8th Circuit, this decision is at odds with the 1st Circuit's ruling 14 years ago in *U.S. v. Czubinski*, 106 F.3d 1069, 1078 (1st Cir. 1997), in which the court overturned the CFAA conviction of Richard Czubinski, an Internal Revenue Service employee, who had exceeded his authorized access to an IRS computer by "merely" viewing restricted tax information relating to "friends, acquaintances, and political rivals." The court held that the proof was insufficient because there must be a "showing of some additional end—to which the unauthorized access is a means." *Id.* However, given the CFAA's plain language, which does not require the physical removal or copying of data, the obvious privacy concerns resulting from viewing data, and the universal recognition that memorizing information can be as detrimental as taking a physical copy of the data itself, the 8th Circuit view is likely to prevail as the accepted standard.

In sum, four circuit courts independently rendered decisions this year that have greatly facilitated and expanded an employer's ability to use the CFAA against employees who engage in computer crime directed at the company's computers.



NICK AKERMAN is a partner in the New York office of Dorsey & Whitney who specializes in the protection of trade secrets and computer data.