Nick Akerman
(212) 415-9217 ▪ akerman.nick@dorsey.com

Nick is a partner in the New York office of Dorsey & Whitney.

For additional articles like this one or to watch my one hour CLE seminar video go to:
http://computerfraud.us

DORSEY
DORSEY & WHITNEY LLP

The 11th Circuit Provides Guidance on Pursuing Ex-Employees Who Steal from Company Computers

This week the 11th Circuit upheld the Computer Fraud and Abuse Act ("CFAA") conviction and one -year prison sentence of a former Social Security Administration ("SSA") employee who accessed the agency's computer for non-business reasons. *U.S. v. Rodriguez*, 2010 WL 5253231 (11th Cir. Dec. 27, 2010). This case is significant for two reasons.

First, the court refused to adopt the 9th Circuit's decision in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), the poster child for not applying the CFAA to miscreant employees who steal their employer's data. A critical element to prove a theft of data under the CFAA is that the defendant accessed the computer without authorization or exceeded authorized access. *Brekka* stands for the proposition that since an employee is permitted as part of his job to access the company computer, an employee cannot be found to have violated the CFAA. *Rodriguez* is the second of the Circuit Courts (in addition to the 5th Circuit) expressly to reject *Brekka* on an issue that ultimately will be decided by the U.S. Supreme Court.

Second, this case serves as a roadmap for employers who want to ensure that an employee who steals its data can be criminally or civilly prosecuted under the CFAA. While the CFAA is primarily the federal computer crime statute, it provides for civil remedies for anyone injured by a violation of the statute. Title 18, U.S.C. § 1030(g). *Rodriguez* illustrates the proactive steps a company can take to make it more likely that it can take advantage of the CFAA's criminal and civil remedies.

Roberto Rodriguez had worked at the SSA as a TeleService representative. His job was to respond over the telephone to questions from the public about their social security benefits. "As a part of his duties, Rodriguez had access to Administration databases that contained sensitive personal information, including any person's social security number, address, date of birth, father's name, mother's maiden name, amount and type of social security benefit received, and annual income." *Id*. at *1.

The SSA policy on access to its computers was clear – employees are prohibited "from obtaining information from its databases without a business reason." *Id*. The SSA "informed its TeleService employees about its policy through mandatory training sessions, notices posted in the office, and a banner that appeared on every computer screen daily" and "also required TeleService employees annually to sign acknowledgment forms after receiving the policies in writing." *Id.*

In addition, the SAA "warned employees that they faced criminal penalties if they violated policies on unauthorized use of databases." *Id*. Nonetheless, "Rodriguez refused to sign the

acknowledgment forms, stating to one supervisor, "'Why give the government rope to hang me?'" The SSA also took steps "to monitor access and prevent unauthorized use" by issuing "unique personal identification numbers and passwords to each TeleService employee and review[ing] usage of the databases." *Id.*

At trial the prosecution showed that Rodriguez "had accessed the personal records of 17 different individuals for nonbusiness reasons." *Id.* All 17 of the individuals for whom he accessed information were women -- his former wife, former girlfriends or women for whom he had a romantic interest. For example, Rodriguez accessed the SSA database "to determine how much . . . [his former wife] was earning," accessed the personal information of a former girlfriend 62 times, and accessed the personal information of a number of women he met at a Universalist church study group. *Id.* at *2. One of these women testified at Rodriguez' trial that "she received a letter from Rodriguez at her home address and was shocked because she had not given Rodriguez her address, she ordinarily receives all her mail at a post office box, and her middle initial was on the envelope although she had not used it since grade school." *Id.* The SSA database records reflected that Rodriguez had accessed her personal information 45 times. At trial Rodriguez testified and "admitted that he did not access the victims' records as a part of his duties as a TeleService representative." *Id.* at 3. Rodriguez was convicted and sentenced to a year in prison.

On appeal Rodriguez relied on *Brekka* arguing that "he did not violate . . . [the CFAA] because he accessed only databases that he was authorized to use as a TeleService representative." *Id* at *4. The court, however, rejected this argument and affirmed Rodriguez' conviction. The court specifically found that based on SSA's policy that "use of databases to obtain personal information is authorized only when done for business reasons" and the plain language of the CFAA, Rodriguez had exceeded his authorized access to the SSA's database. *Id.* The court distinguished *Brekka* on its facts – Brekka's employer "had no policy prohibiting employees from emailing company documents to personal email accounts, and there was no dispute that Brekka had been authorized to obtain the documents or to send the emails while he was employed;" whereas the SSA "told Rodriguez that he was not authorized to obtain personal information for nonbusiness reasons." *Id*.

The lessons from this case to employers and their counsel who are drafting corporate computer policies are

- First, it is critical to establish corporate computer policies setting forth the employee's scope of authorization to access the company computers,

- Second, this policy should be re-enforced on a periodic basis in a variety of ways that are designed for the particular circumstances and needs of the individual company, and

- Third, the company should actively monitor employee computer usage to ensure that its policies are being followed and take appropriate actions when its policies are violated.