The Florida Bar
Labor & Employment Law Section
E-UPDATES
www.LaborEmploymentLaw.org

September 2015

Jay P. Lechner and Zascha Blanco Abbott
Publications Sub-Committee Co-Chairs

New Law Gives Employers Leverage Against Employees Who Take Company Data and Computer Files Without Authorization

On May 14, 2015, Governor Rick Scott approved the Computer Abuse and Data Recovery Act ("CADRA"), Sections 608.801- 668.805, Florida Statutes. This law goes into effect on October 1, 2015, and provides a new remedy to employers and other businesses who suffer harm or loss due to unauthorized access to their computers or to information stored on their computers.

While criminal hacking and data breaches by third parties occur often and receive widespread publicity, the legislative history of CADRA makes it clear that this bill was intended to help businesses and employers respond to "inside jobs," that is, unauthorized access to data by employees. The bill analysis from the Florida Senate Judiciary Committee notes that "hacking by insiders or employees poses a significant threat to businesses because employees have ready access to valuable or significant information."[1] Despite this clear threat, the legislature felt that "challenges to the prosecution of hacking by employees exist [because state law] exempts employees acting within the scope of their lawful employment from prosecution for criminal actions, [while] civil actions brought under [federal law] must have damages of $5,000 or more, or must be based on other specific harm. Additionally, federal appellate circuit courts are split on the application of the [current federal statute] to employee hackers."[2]

CADRA deals with the problem head-on by creating a new a civil cause of action available to those actually injured by an individual who knowingly and with intent to cause harm or loss: (1) obtains information from a protected computer without authorization; (2) causes the transmission of a program, code, or command from a protected computer without authorization, and as a result, causes a harm or loss; or (3) traffics[3] in any technological access barrier (e.g., password) through which access to a protected computer may be obtained without authorization.[4]

To prevail in an action, the computer owner/employer must show that as a result of any of the aforementioned acts, the unauthorized user causes an actual harm or loss.[5]

In the civil action, the injured party has the following remedies available: (1) recovery of actual damages; (2) recovery of the violator's profits that are not included in the plaintiff's damages; (3) injunctive or other equitable relief to prevent a future violation; and (4) return of the misappropriated information, program, or code, and all copies.[6] Critically, to provide CADRA with an effective enforcement tool, the statute also directs courts to award attorneys' fees to the prevailing party.[7]

An injured party must commence a civil action within three years after the violation, or three years after the violation was discovered or should have been discovered with due diligence.[8] If a criminal proceeding arising out of the insider data breach results in a final judgment in favor of the state, the defendant can no longer deny or dispute the same matters in any subsequent civil action brought under CADRA.[9]

When CADRA Comes Into Play

First, to fall under the protection of CADRA, the computer must be a "protected computer" and the access has to be obtained by someone who is not an "authorized user."[10] While the statute provides technical definitions of these terms,[11] the general thrust is that a business cannot seek protection under the act if it does not take reasonable

measures on its own to protect its data. For example, the law only covers a computer that employs a password or other similar "technological access barrier." In other words, if a company does not take steps to protect its own computer data, CADRA won't provide such protection, either.

Second, the law comes into play only if the information obtained from a "protected computer" is taken "without authorization."[12] The legislature specifically chose to "not resolve uncertainties about application of the liability provisions to an employee who is permitted access to the relevant information as part of their [sic] duties, but acts outside those duties with resulting harm or loss to the employer."[13] Nonetheless, the legislature made clear that "permission to access a business' private computer is terminated upon cessation of the third-party agent, contractor, consultant, or employee's employment."

Consequently, while it remains unclear whether an employee who has a right to access certain data at the time it is accessed violates CADRA if the employee exceeds his or her authority, it is equally clear that any such access terminates upon cessation of the employment.[14] In addition, the owner of the information can explicitly revoke an authorized access.[15] This means that business owners or employers can resolve the legislative ambiguity and make clear to authorized personnel that, even where access is authorized, it is only authorized if used within the scope of employment and in furtherance of the business' interests; any usage outside of this limited scope is revoked.

A New and Useful Tool in Litigation With Employees

During litigation with employees, employers often discover that current or former employees retain information from the employer's computer systems. For example, employees often email files and other company documents to their personal email addresses. Also, employees often print from company computers sensitive or even routine documents and take them home.

The passage of CADRA, and specifically its remedies and its attorneys' fees provisions, provides a golden opportunity for forward-thinking employers to obtain leverage against their employees by counterclaiming against any employee who improperly takes employer data upon termination and fails to return such company data. Indeed, if done effectively, CADRA may even the litigation playing field somewhat because, as most employers already know, it is much more difficult for a prevailing employer to obtain fees than it is for a prevailing employee.[16] An effective CADRA claim allows an employer to recover the fees it expends seeking relief for a violation, which may well equal the fees an employee seeks, or at least offset the employer's fee exposure.

Coverage under CADRA is not automatic, however. Employers first need to put reasonable measures in place ("technological access barriers") to restrict access to company computer data. Companies also should have very clear policies that spell out what constitutes authorized access and what conduct is deemed improper and unauthorized access. For example, if a company has a clear policy prohibiting an employee from sending any company files to personal email or from printing company data from its computers to take home, then even if the employee otherwise has lawful access to the data while at work, the employer will be in a much better position to argue that the employee violated CADRA when the employee sent company data to a personal email or took it home.

Similarly, employers should carefully monitor data access and make clear that they will discipline employees for any violations. If an employee is found to be printing out computer files or forwarding work materials to a personal email, such conduct should be vigorously addressed. Companies also should address such violations in a consistent manner and train HR and IT personnel to spot these issues and to know how to respond when a violation occurs. Finally, in an effort to resolve the legislative ambiguity regarding employees with a "right to access" who exceed the scope of their authority, all company data access policies should make clear that the company revokes all authority to access its data if such data is used outside the scope of authority or sent outside the company's email system or its physical facilities.

Finally, because CADRA is effective primarily if it is used in concert with a strong data access policy, employers should seek appropriate advice and counseling to have handbooks and policies updated before CADRA goes into effect next month.

~ By Mendy Halbertstam, Jackson Lewis P.C.

(Endnotes)

1 Senate Judiciary Committee Bill Analysis and Financial Impact Statement, SB 222, March 30, 2015.
2 *Id.* § II (comparing *United States v. Nosal*, 676 F. 3d 854 (9th Cir. 2012) (Finding that an employee hacker can exceed authorization only by accessing files outside the scope of her use authorization (e.g., stealing a co-worker's password to access information)) with *United States v. Rodriguez*, 628 F. 3d 1258 (11th Cir. 2010) (Finding that an employee hacker who uses information obtained within the scope of her normal use authorization exceeds authorization by using the information in a manner contrary to the business' interests or use agreement)).
3 "Traffic" means to "sell, purchase, or deliver." Fla. Stat. § 668.802(7).
4 Fla. Stat. § 668.803.
5 "Harm" and "loss" are specifically defined terms and include the reasonable cost of data breach damage assessment and data breach remediation efforts. Fla. Stat. § 668.802(4), (5).
6 Fla Stat. § 668.804(1).
7 Fla Stat. § 668.804(2).
8 Fla Stat. § 668.804(5).
9 Fla Stat. § 668.804(4).
10 Fla Stat. § 668.803.
11 Fla Stat. §§ 668.802(1), (6), and (9).
12 Fla Stat. § 668.803.
13 Senate Judiciary Committee Bill Analysis and Financial Impact Statement, § III.
14 Fla. Stat. § 668.802(1).
15 *Id.*
16 *Christiansburg Garment Co. v. EEOC*, 434 U.S. 412 (1978). This case established that prevailing employee-plaintiffs are nearly always entitled to fees if they succeed on the merits of a civil rights claim. In contrast, employer-defendants often must prove that a case was frivolous at its outset (or became frivolous during the course of litigation) before they may recover fees.