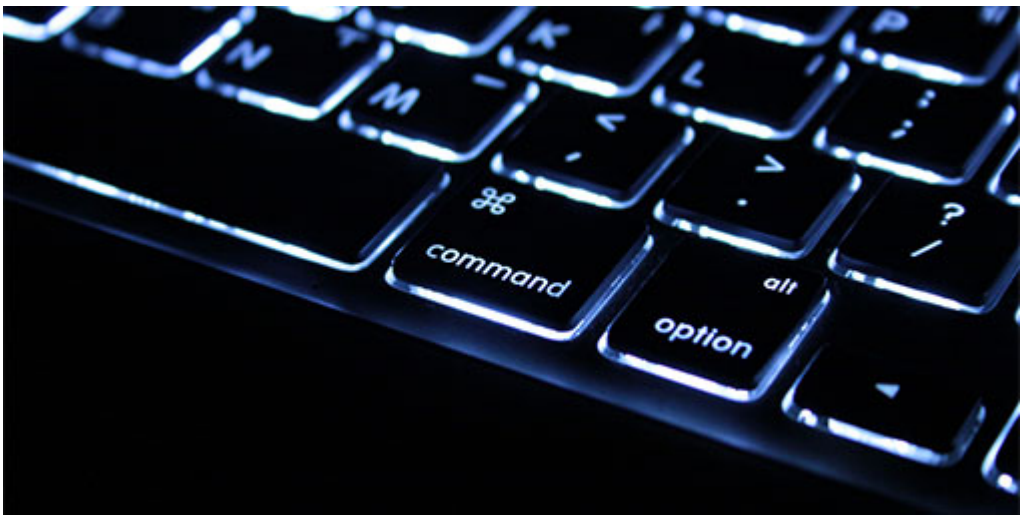
CARLTON FIELDS

Florida Enacts Law Providing for Civil Remedy Against Cyber Fraud and Abuse

May 19, 2015



On May 14, Florida Governor Rick Scott signed the Computer Abuse and Data Recovery Act (CADRA) into law. CADRA is intended to provide a remedy to businesses for harm or loss caused by unauthorized access to protected computers, as well as to safeguard the owners of information stored on those computers. Although many states, including Florida, have criminalized certain conduct pertaining to computer use and provide that an aggrieved party may bring a civil action against violators, such remedies are limited. For example, the Florida Computer Crimes Act (CCA) prohibits, among other things, the unauthorized access to or destruction of a computer and its related technologies. However, a civil action under the CCA must be preceded by a criminal conviction under the statute. Comparatively, CADRA provides businesses with a means to redress loss beyond what is already prohibited by criminal laws in Florida and in many other states. CADRA also encompasses a broader range of conduct than laws of other states, and it provides an additional degree of certainty over the availability of civil redress in the event a business is harmed or suffers a loss due to unauthorized computer access. Similar to the federal Computer Fraud and Abuse Act (CFAA), the new law provides an offensive tool for businesses that suffer “harm or loss” as a result of unauthorized access to

"protected computers." A "protected computer" is defined as a computer "that is used in connection with the operation of a business and stores information, programs, or code in connection with the operation of the business in which the stored information, programs, or code can be accessed only by employing a technological access barrier." CADRA's purpose is to safeguard protected computers from "harm" or "loss," broadly defined, respectively, as "any impairment to the integrity, access, or availability of data, programs, systems, or information" and, to include "the business's economic damages, lost profits, costs incurred due to a post-breach damage assessment, consequential damages, as well as the profits earned" by a violator. Thus, it provides that any person who knowingly and with intent to cause harm or loss:

> (1) Obtains information from a protected computer without authorization and, as a result, causes harm or loss; (2) Causes the transmission of a program, code, or command to a protected computer without authorization and, as a result of the transmission, causes harm or loss; or (3) Traffics in any technological access barrier through which access to a protected computer may be obtained without authorization,

is liable "in a civil action. . . ." An aggrieved party who brings a civil action under CADRA may recover actual damages, the violator's ill-gotten gains, obtain injunctive relief, and/or recover the misappropriated data. The prevailing party may also recover attorneys' fees under the new law. **What does this mean for business owners?** CADRA provides an additional tool to redress harm done to business owners' protected computers. However, to enjoy its protections, business owners must be proactive and employ effective "technological access barriers." This is because while the law prohibits access to a protected computer "without authorization," "without authorization" is defined to exclude "circumventing a technological measure that does not effectively control access to the protected computer. . . ." Thus, relief may be unavailable if sufficient "technological measure[s]" to "control access" have not been taken. The legislative history reflects that "[t]his wording imposes a responsibility on businesses to establish and maintain effective technological measures such as passwords." The definition of "without authorization" also leaves open the question of whether CADRA may be used to hold rogue employees liable for harm or loss caused to their employer. For example, the statute is unclear as to whether employees who are typically authorized to access a protected computer may be liable for causing harm or loss to their employer by acting beyond the scope of their normal duties. The scope of CADRA's application is also unclear. It does not expressly limit its application to businesses or computers located in Florida, and does not indicate when the "owner of information" stored on a protected computer, who does not own the computer itself, may seek relief under the statute. Although some ambiguities exist, CADRA provides a powerful tool for businesses to combat unauthorized cyber intrusions. The remedies available under the statute may be asserted in addition to remedies otherwise available under state or federal law. Further, the law has a three-year statute of limitations, as opposed to two years provided by the CFAA. The statute takes effect October 1, 2015.

Related Practices

Technology
Cybersecurity and Privacy
Intellectual Property

Related Industries

Technology