HOUSE OF REPRESENTATIVES
FINAL BILL ANALYSIS

BILL #:	CS/CS/CS/HB 175	**FINAL HOUSE FLOOR ACTION:**	
SPONSOR(S):	Judiciary Committee; Economic Development & Tourism Subcommittee; Civil Justice Subcommittee; Spano and others	117 **Y's**	0 **N's**
COMPANION BILLS:	CS/CS/CS/SB 222	**GOVERNOR'S ACTION:**	Approved

SUMMARY ANALYSIS

CS/CS/CS/HB 175 passed the House on April 22, 2105, as CS/CS/CS/SB 222. The bill creates the Computer Abuse and Data Recovery Act which establishes a civil cause of action for the hacking of business computers.

"Hacking" is the unauthorized access of a computer or its related technologies, usually with intent to cause harm. Hackers are subject to criminal and civil penalties under the Florida Computer Crimes Act ("CCA") and the federal Computer Fraud and Abuse Act ("CFAA"). However, due to the narrow statutory remedies available, and the challenges to prosecution of hacking by insiders or employees, businesses have found it increasingly difficult to bring and sustain civil claims against hackers under the CCA and CFAA.

The bill creates the "Computer Abuse and Data Recovery Act" ("CADRA") which establishes an additional civil cause of action for owners, operators, or lessees of business computers, or owners of information stored in business computers, that are injured by an individual who:

- Obtains information from a business computer without authorization;
- Transmits a program, code, or command to a business computer without authorization; or
- Traffics in any technological access barrier (e.g., password) through which access to a business computer may be obtained without authorization.

The bill provides civil remedies for violations of CADRA including the recovery of actual damages, lost profits, economic damages, and copies of misappropriated information, as well as injunctive or other equitable relief.

CADRA is inapplicable to certain technology service providers and lawful investigative, protective, or intelligence activities of governmental agencies.

This bill does not appear to have a fiscal impact on state or local government.

The bill was approved by the Governor on May 14, 2015, ch. 2015-14, L.O.F., and will become effective October 1, 2015.

I. SUBSTANTIVE INFORMATION

A. EFFECT OF CHANGES:

Current Situation

"Hacking" is the unauthorized access of a computer or its related technologies, usually with intent to cause harm.[1] Hacking includes offenses such as the misappropriation of passwords; viewing restricted electronically-stored information owned by others; copying/adulterating/stealing data, software, or program files owned by others; URL redirection; adulterating web sites; or any other behavior that involves accessing a computing system without appropriate authorization.[2]

Hackers are subject to criminal and civil penalties under the Florida Computer Crimes Act ("CCA")[3] and the federal Computer Fraud and Abuse Act ("CFAA").[4] However, due to the narrow statutory remedies available, and the challenges to prosecution of hacking by insiders or employees, businesses have found it increasingly difficult to bring and sustain civil claims against hackers under the CCA and CFAA.

Florida Computer Crimes Act

Chapter 815, F.S., entitled the "Florida Computer Crimes Act," was created in 1978 in recognition of growing computer-related crime. The Act criminalizes certain offenses against intellectual property and offenses against users of computers, computer systems, computer networks, and electronic devices.

Offenses Against Intellectual Property
A person commits an offense against intellectual property[5] when he or she willfully, knowingly, and without authorization:

- Introduces a contaminant into a computer, computer system, computer network or electronic device;
- Modifies, renders unavailable, or destroys data, programs, or supporting documentation in a computer, computer system, computer network, or electronic device; or
- Discloses or takes data, programs, or supporting documentation which is a trade secret or is confidential that is in a computer, computer system, computer network, or electronic device.

Offenses Against Computer Users
A person commits an offense against computer users[6] when he or she willfully, knowingly, and without authorization:

- Accesses, destroys, injures, or damages any computer, computer system, computer network, or electronic device;
- Disrupts the ability to transmit data to or from an authorized user of a computer, computer system, computer network, or electronic device;
- Destroys, takes, injures, modifies, or damages equipment or supplies used or intended to be used in a computer, computer system, computer network, or electronic device;
- Introduces any computer contaminant into any computer, computer system, computer network, or electronic device; or

1 Eric J. Sinrod, William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 Santa Clara Computer & High Tech. L.J. 177 (2000).
2 Peter T. Leeson and Christopher J. Coyne. *The Economics of Computer Hacking*. www.peterleeson.com/hackers.pdf. (last accessed May 3, 2015).
3 Chapter 815, F.S.
4 18 U.S.C. § 1030.
5 s. 815.04, F.S.
6 s. 815.06, F.S.

- Engages in audio or video surveillance of an individual by accessing any inherent feature or component of a computer, computer system, computer network, or electronic device, including accessing the data or information thereof that is stored by a third party.

The CCA provides that the owner or lessee of a computer, computer system, computer network, computer program, computer equipment, computer supplies, or computer data may bring a civil action[7] for compensatory damages against a person *convicted* of an offense against computer users under s. 815.06, F.S. Accordingly, a criminal conviction must precede the civil action.

Due to the higher burden of proof required for criminal convictions, a prosecutor may decline to pursue criminal charges for hacking or an offender may be acquitted. Although the available evidence may satisfy the burden of proof in a civil action, civil recovery is barred under the CCA in the absence of the criminal conviction. There is also the risk that the hacker may exhaust his or her monetary resources in the criminal action making satisfaction of any subsequent civil judgment difficult.

The limited right of recovery under s. 815.06, F.S., is further narrowed by the immunity given to a person who accesses his or her employer's computer system, computer network, computer program, or computer data when acting within the scope of his or her lawful employment.[8] Courts have consistently found that employees do not access a computer, computer system, or computer network "without authorization" if such employees were ever given access by the employer even when exceeding the implicit scope of such authorization and acting against the employer's interest.[9] One concurring opinion indicates that courts interpret s. 815.06, F.S., to apply to hackers who attack a computer system from the outside, not "insiders." [10]

Federal Computer Fraud and Abuse Act

Due to the limitations of the civil action under the CCA, many Florida businesses rely on the federal "Computer Fraud and Abuse Act"[11] to recover damages from hackers. The CFAA is primarily a criminal statute intended to deter computer hackers, though it provides for civil actions by private parties damaged as a result of a violation.

The CFAA prohibits:

- Accessing a computer without authorization[12] or exceeding authorized access[13] to commit espionage, [14] obtain credit and financial information, [15] obtain information from any department or agency of the United States, obtain information from any protected computer, [16] or to further a fraud and obtain anything of value;[17]
- Damaging a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce through various forms of a cyber attack, cyber crime, or cyber terrorism without authorization;[18]

---

[7] s. 815.06(4), F.S.
[8] s. 815.06(6), F.S.
[9] *See Gallagher v. Florida*, 618 So. 2d 757, 758 (Fla. 4th DCA 1993) (finding that an employee's exceeding authorized access, while technically wrong, did not warrant criminal sanctions because administrative sanctions were more appropriate); *See Willoughby v. Florida*, 84 So. 3d 1210, 1212 (Fla. 3d DCA 2012).
[10] *Rodriguez v. Florida*, 956 So. 2d 1226, 1232 (Fla. 4th DCA 2007)(Gross, J., concurring).
[11] 18 U.S.C. § 1030.
[12] This term is not defined in the CFAA.
[13] The term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).
[14] 18 U.S.C. § 1030(a)(1).
[15] 18 U.S.C. § 1030(a)(2).
[16] The term "protected computer" is defined in 18 U.S.C. § 1030(e)(2), but courts have held that any internet connected computer is a protected computer. *See, e.g., United States v. Drew,* 259 F.R.D. 449, 457 (C.D. Cal. 2009).
[17] 18 U.S.C. § 1030(a)(4).
[18] 18 U.S.C. § 1030(a)(5).

- Trafficking in any password or similar information through which a computer may be accessed without authorization;[19] and
- Threatening to damage a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce.[20]

Any person who suffers damage or loss by reason of a violation of the CFAA may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief if damages total $5,000 or more, the provision of medical care is hampered, a person is physically harmed, or national security, public safety or health is threatened.[21]

Although the CFAA does not explicitly exempt employees, problems similar to the CCA have arisen in the enforcement of the CFAA regarding whether a person, an "insider", with some authorization to access a computer can ever act “without authorization” with respect to that computer. Several courts have held that defendants lose their authorization to access computers when they breach a duty of loyalty to the authorizing parties.[22] However, such line of cases have recently been criticized by other courts adopting the view that under the CFAA, an authorized user of a computer cannot access the computer “without authorization” unless and until the authorization is revoked.[23] Based on this recent case law, courts appear increasingly likely to reject the idea that a defendant accessed a computer “without authorization” in insider cases.

Circuit courts are also split on when an "insider" hacker "exceeds authorized access" under the CFAA.[24] The split among the circuit courts make civil actions against "insiders" under the CFAA increasingly difficult.

Effect of Proposed Changes

The bill creates the "Computer Abuse and Data Recovery Act" ("CADRA"), to provide businesses with an additional civil remedy for injuries caused by computer hacking. An owner, operator, or lessee of a business computer secured with a technological access barrier, or the owner of information stored in such computer, may bring a civil action against any person who without authorization and with intent to cause harm or loss:

- Obtains information from such computers;
- Causes the transmission of programs, codes, or commands to such computers; or
- Traffics in technological access barriers through which such computers may be accessed without authorization.

Unlike the CCA and CFAA, CADRA does not require the satisfaction of a condition precedent (i.e. a criminal conviction, damage threshold, exigent circumstance, etc.) to bring a claim under the provisions of the Act. However, if a CADRA defendant is also pursued criminally under the CCA, a final judgment or decree in a criminal proceeding under the CCA will estop the defendant as to the same matters in a civil action under CADRA.

A claimant may obtain several forms of relief under CADRA, including:

- Actual damages, including lost profits and economic damages;

[19] 18 U.S.C. § 1030(a)(6).
[20] 18 U.S.C. § 1030(a)(7).
[21] 18 U.S.C. § 1030(g).
[22] *See, e.g.*, *Int’l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006); *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.,* 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000).
[23] *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133-34 (9th Cir. 2009); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 964-967 (D. Ariz. 2008); *Lockheed Martin Corp. v. Speed*, 2006 WL 2683058, at *4 (M.D. Fla. 2006).
[24] *See United States v. Nosal,* 676 F.3d 854 (9th Cir. 2012)(en banc); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012); *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *United States v. John*, 597 F.3d 263 (5th Cir. 2010).

- Profits earned by the defendant as a result of the unauthorized hacking;
- Injunctive or other equitable relief; and
- Recovery of information, programs, or codes misappropriated during the unlawful intrusion.

An action under CADRA must be brought within 3 years after a violation occurred, was discovered, or should have been discovered with due diligence. The statute of limitations is shorter than the default statute of limitations provided by s. 95.11(3)(f), F.S., which requires that actions founded on a statutory liability be brought within four years. The prevailing party is entitled to recover reasonable attorney fees.

The bill also defines terms used in the Act and provides for liberal construction of the Act to safeguard an owner, operator, or lessee of a business computer, or an owner of information stored in a business computer, from harm or loss caused by hacking.

CADRA is inapplicable to certain technology service providers and lawful investigative, protective, or intelligence activities of governmental agencies.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   The bill does not appear to have any impact on state revenues.

2. Expenditures:

   The bill does not appear to have any impact on state expenditures.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

   The bill does not appear to have any impact on local government revenues.

2. Expenditures:

   The bill does not appear to have any impact on local government expenditures.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

The bill does not appear to have any direct economic impact on the private sector.

D. FISCAL COMMENTS:

None.