The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Commerce and Tourism

BILL:	CS/SB 222
INTRODUCER:	Commerce and Tourism Committee and Senator Hukill
SUBJECT:	Electronic Commerce
DATE:	February 17, 2015 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Harmsen	McKay	CM	**Fav/CS**
2.			CU	
3.			JU	

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Technical Changes

I. Summary:

CS/SB 222 creates the Computer Abuse and Data Recovery Act ("CADRA"), which creates a civil cause of action for harm or loss caused by the unauthorized access, or hacking, of a protected computer owned by a business. Remedies created by the bill include the recovery of actual damages, lost profits, economic damages, and injunctive or other equitable relief. The bill does not create any criminal penalties, and does not address the unauthorized access of a personal computer.

II. Present Situation:

"Hacking" is the unauthorized access of a computer or its related technologies, usually with intent to cause harm.[1] Currently, hackers are subject to criminal and limited civil penalties under the Florida Computer Crimes Act ("CCA") and the federal Computer Fraud and Abuse Act ("CFAA").

Hacking by insiders or employees poses a significant threat to businesses because employees have ready access to valuable or significant information,[2] but challenges to the prosecution of

[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] U.S. Department of Homeland Security, *Increase in Insider Threat Cases Highlight Significant Risks to Business Networks and Proprietary Information*, September 23, 2014. Retrieved February 3, 2015, from https://www.ic3.gov/media/2014/140923.aspx. *See also*, s. 815.02, F.S. (2014).

hacking by employees exist. For example, the CCA exempts employees acting within the scope of their lawful employment from prosecution for criminal actions.[3] Civil actions brought under the CFAA must have damages of $5,000 or more, or must be based on other specific harm.[4] Additionally, federal appellate circuit courts have split on the application of the CFAA to employee hackers.[5,6]

Computer Fraud and Abuse Act

The CFAA[7] provides criminal penalties for individuals who either without authorization, or in excess of authorized access:

- Obtain national security information;
- Access a computer and obtain confidential information;
- Trespass in a government computer;
- Access a computer to commit a fraud;
- Damage a computer;
- Traffic in computer passwords; or
- Make threats involving computers.

The CFAA also provides civil remedies if damages exceed $5,000, hamper medical care, physically harm a person, or threaten national security, public safety or health.[8]

The CFAA does not define "without authorization," but does define to "exceed authorized access" as "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."[9]

Florida Computer Crimes Act

In 1978, the Legislature created the CCA[10] to address the problem of computer-related crime in government and the private sector.[11] The CCA criminalizes certain offenses against intellectual property and offenses against users of computers, computer systems, computer networks, and electronic devices (hereinafter "computer or its related technologies").

[3] Section 815.06(7)(b), F.S. (2014).
[4] 18 U.S.C. §1030(c)(4)(A)(i)(I)-(V).
[5] U.S. Department of Justice, *Prosecuting Computer Crimes* (Office of Legal Education 2009). Retrieved February 3, 2015, from http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.
[6] Compare *United States v. Nosal*, 676 F. 3d 854 (9th Cir. 2012)(Finding that an employee hacker can only exceed authorization by accessing files outside the scope of her use-authorization (e.g., stealing a co-workers 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).
[7] 18 U.S.C. §1030.
[8] 18 U.S.C. §1030(g).
[9] 18 U.S.C. §1030(e)(6).
[10] Sections 815.01-815.06, F.S. (2014).
[11] Chapter 78-92, L.O.F., section 815.01-02, F.S. (2014).

Offenses Against Intellectual Property

A person commits an offense against intellectual property under the CCA when she willfully, knowingly, and without authorization:

- Introduces a contaminant into a computer or its related technologies;
- Modifies, renders unavailable, or destroys data, programs, or supporting documentation in a computer or its related technologies; or
- Discloses or takes data, programs, or supporting documentation which is a trade secret or is confidential that is in a computer or its related technologies.

Offenses Against Computer Users

A person commits an offense against computer users under the CCA when she willfully, knowingly, and without authorization:

- Accesses, destroys, injures, or damages any computer or its related technologies;
- Disrupts the ability to transmit data to or from an authorized user of a computer or its related technologies;
- Destroys, takes, injures, modifies, or damages equipment or supplies used or intended to be used in a computer or its related technologies;
- Introduces any computer contaminant into any computer or its related technologies; or
- Engages in audio or video surveillance of an individual by accessing any inherent feature or component of a computer or its related technologies, including accessing the data or information thereof that is stored by a third party.

The CCA does not provide a civil remedy for offenses against intellectual property, but it does enable an owner or lessee of an affected computer or its related technologies to bring a civil action[12] for compensatory damages against any person convicted of an offense against computer users under s. 815.06, F.S.[13] Employees acting under the scope of their authorization are specifically exempted from this civil cause of action under the CCA.[14]

The civil action provided for in s. 815.04, F.S., is generally disfavored as a more costly and time-consuming option than necessary because it must be preceded by a criminal conviction under the CCA.[15] As an alternative, litigants generally proceed under a federal CFAA claim.[16]

III. Effect of Proposed Changes:

Section 1 creates the "Computer Abuse and Data Recovery Act" in ch. 668, F.S.

[12] Section 815.06(4), F.S.
[13] Section 815.06(5)(a), F.S.
[14] Section 815.06(7)(b), F.S.
[15] Robert Kain, *Federal Computer Fraud and Abuse Act: Employee Hacking Legal in California and Virginia, But Illegal in Miami, Dallas, Chicago, and Boston*, 87 Fla. Bar. J., (Jan., 2013). Retrieved February 3, 2015 at http://www.floridabar.org/DIVCOM/JN/JNJournal01.nsf/8c9f13012b96736985256aa900624829/83a2364f8efc84e385257ae200647255!OpenDocument.
[16] *Id*.

Section 2 directs that CADRA must be construed liberally to safeguard owners, operators, or lessees of protected computers used in the operation of a business, and owners of information stored in a protected computer used in the operation of a business, from harm or loss caused by unauthorized access to the computers.

Section 3 defines terms used in the bill.

Notably, this bill defines "without authorization" as the circumvention of a technological access barrier, usually a password or biometric, without express or implied permission. Therefore, both outside hackers and employee hackers may be civilly liable for their actions under this bill. Conversely, the bill's definition of "without authorization" imposes a responsibility on businesses to establish and maintain effective technological measures such as passwords, because hackers who "circumvent a technological measure that does not effectively control access to the protected computer" act outside the scope of liability provided for by this bill.

Employees who misuse information they obtained under the authorization granted by their employer are not subject to civil action under this bill.

Section 4 creates s. 668.803, F.S., which provides a civil action available to those injured by an individual who knowingly and with intent to cause harm or loss:

- Obtains information from a protected computer without authorization, and as a result thereof, causes a harm or loss;
- Causes the transmission of a program, code, or command from a protected computer without authorization, and as a result thereof, causes a harm or loss; or
- Traffics in any technological access barrier (e.g., password) through which access to a protected computer may be obtained without authorization.

Section 5 establishes the following civil remedies available to victims of a s. 668.803, F.S., (**Section 4**) violation:

- Recovery of actual damages and the violator's profits; and
- Injunctive or other equitable relief;
- Return of the misappropriated information, program, or code, and all copies thereof.

The bill also directs courts to award attorney's fees to the prevailing party in any s. 668.804(2), F.S., (**Section 5**) action.

A victim must commence a civil action under s. 668.803, F.S. within 3 years of the violation, the discovery thereof, or the time at which the violation should have been discovered with due diligence. This statute of limitations is shorter than Florida's 4-year default statute of limitations,[17] but longer than the 2-year statute of limitations provided for in the federal CFAA[18].

Relief provided under this bill is available as a supplement to other remedies under state and federal law. If a criminal proceeding brought under the CCA results in a final judgment or decree in favor of the state, the defendant is estopped from denying or disputing the same matters in any subsequent civil action brought under CADRA.

[17] Section 95.11(3)(f), F.S.
[18] 18 U.S.C. §1030(g).

Section 6 excludes from actions pursuant to this bill any lawfully authorized investigative, protective, or intelligence activity of any law enforcement agency, regulatory agency, or political subdivision of Florida, any other state, the United States, or any foreign country.

Section 7 provides an effective date of October 1, 2015.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

The bill provides an alternate civil remedy for businesses affected by specific hacking acts.

C. Government Sector Impact:

None.

VI. Technical Deficiencies:

None.

VII. Related Issues:

For the sake of consistency and clarity, "technological measure" in line 80 could be replaced with "technological access barrier."

VIII. Statutes Affected:

This bill creates sections 668.801, 668.602, 668.803, 668.804, and 668.805, F.S.

IX. Additional Information:

A. Committee Substitute – Statement of Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

CS by Commerce and Tourism on February 16, 2015:
Clarifies that a victim may seek the return of misappropriated programs, misappropriated codes, and misappropriated information under s. 668.804, F.S.

B. Amendments:

None.