HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/CS/CS/HB 175 Electronic Commerce
SPONSOR(S): Judiciary Committee; Economic Development & Tourism Subcommittee; Civil Justice Subcommittee; Spano and others
TIED BILLS: None **IDEN./SIM. BILLS:** CS/CS/SB 222

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Civil Justice Subcommittee	12 Y, 0 N, As CS	Robinson	Bond
2) Economic Development & Tourism Subcommittee	11 Y, 0 N, As CS	Lukis	Duncan
3) Judiciary Committee	18 Y, 0 N, As CS	Robinson	Havlicak

SUMMARY ANALYSIS

"Hacking" is the unauthorized access of a computer or its related technologies, usually with intent to cause harm. 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"). The CCA authorizes civil actions against persons criminally convicted under the CCA, but specifically exempts employees acting within the scope of their employment from criminal sanction. Civil actions brought under the CFAA must have damages of $5,000 or more, or must be based on other specific harm. There is also split among appellate circuit courts regarding the applicability of the CFAA to employee or insider hackers.

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 the hacking of business computers. The bill provides civil remedies including the recovery of actual damages, lost profits, and economic damages, as well as injunctive or other equitable relief to victims of hacking. CADRA does not exempt employee or insider hackers or impose any conditions precedent to bringing a claim for relief.

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

The bill takes effect October 1, 2015.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED 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]

Currently, hackers are subject to criminal and limited civil penalties under the Florida Computer Crimes Act ("CCA")[3] and the federal Computer Fraud and Abuse Act ("CFAA").[4] The CCA authorizes civil actions against persons criminally convicted[5] under the CCA, but specifically exempts employees acting within the scope of their employment from criminal sanction.[6] Civil actions brought under the CFAA must have damages of $5,000 or more, or must be based on other specific harm.[7] There is also a split among appellate circuit courts regarding the applicability of the CFAA to employee or insider hackers.[8]

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[9] 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.

---

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 February 4, 2015)

3 Chapter 815, F.S.

4 18 U.S.C. § 1030.

5 s. 815.06(4), F.S.

6 s. 815.06(6), F.S.

7 18 U.S.C. § 1030(g).

8 *See, e.g.*, *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133-34 (9th Cir. 2009); *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); and *United States v. John*, 597 F.3d 263 (5th Cir. 2010).

9 s. 815.04, F.S.

Offenses Against Computer Users

A person commits an offense against computer users[10] 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
- 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[11] 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.[12] 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.[13] 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."[14]

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"[15] 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[16] or exceeding authorized access[17] to commit espionage,[18] obtain credit and financial information,[19] obtain information from any department

[10] s. 815.06, F.S.
[11] s. 815.06(4), F.S.
[12] s. 815.06(6), F.S.
[13] *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).
[14] *Rodriguez v. Florida*, 956 So.2d 1226, 1232 (Fla. 4th DCA 2007)(Gross, J., concurring).
[15] 18 U.S.C. § 1030.
[16] This term is not defined in the CFAA.
[17] 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).

or agency of the United States, obtain information from any protected computer, [20] or to further a fraud and obtain anything of value;[21]
- 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;[22]
- Trafficking in any password or similar information through which a computer may be accessed without authorization;[23] and
- Threatening to damage a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce.[24]

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.[25]

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. [26] 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.[27] 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.[28] 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 computer-related abuses.

Section 668.804, F.S., provides that 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 intent to cause harm or loss:

- Obtains information from such computers;
- Causes the transmission of programs, codes, or commands to such computers; or

---

[18] 18 U.S.C. § 1030(a)(1).
[19] 18 U.S.C. § 1030(a)(2).
[20] 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).
[21] 18 U.S.C. § 1030(a)(4).
[22] 18 U.S.C. § 1030(a)(5).
[23] 18 U.S.C. § 1030(a)(6).
[24] 18 U.S.C. § 1030(a)(7).
[25] 18 U.S.C. § 1030(g).
[26] *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).
[27] *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).
[28] *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).

- 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 for relief under the provisions of the Act. However, if a CADRA defendant is also pursued criminally under the CCA, s. 668.805(4), F.S., provides that 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:

- Actual damages, including lost profits and economic damages;
- 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.

The prevailing party in any action brought pursuant to the Act is also entitled to recover reasonable attorney fees under s. 668.805(2), F.S.

Section 668.805(5), F.S., provides that an action pursuant to 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 under CADRA 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.

Section 668.802, F.S., explains the purpose of CADRA and directs that it be liberally construed. Terms used in the Act are defined in s. 668.803, F.S. and a short title is provided in s. 668.801, F.S.

CADRA does not prohibit lawfully authorized investigative, protective, or intelligence activities of governmental agencies or .

B. SECTION DIRECTORY:

Section 1 provides a direction to the Division of Law Revision and Information.

Section 2 creates s. 668.801, F.S., regarding a short title for CADRA.

Section 3 creates s. 668.802, F.S., regarding construction of CADRA.

Section 4 creates s. 668.803, F.S., regarding definitions applicable to CADRA.

Section 5 creates s. 668.804, F.S., regarding prohibited acts under CADRA.

Section 6 creates s. 668.805, F.S., regarding remedies provided by CADRA.

Section 7 creates s. 668.806, F.S., regarding exclusions under CADRA.

Section 8 provides an effective date of October 1, 2015.

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.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

The bill does not appear to require counties or municipalities to take an action requiring the expenditure of funds, reduce the authority that counties or municipalities have to raise revenue in the aggregate, nor reduce the percentage of state tax shared with counties or municipalities.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

The bill does not appear to create a need for rulemaking or rulemaking authority.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES

On February 4, 2015, the Civil Justice Subcommittee adopted one amendment and reported the bill favorably as a committee substitute. The amendment provides for the recovery of misappropriated programs or codes as an additional remedy of a claimant under CADRA.

On March 3, 2015, the Economic Development & Tourism Subcommittee adopted one amendment and reported the bill favorably as a committee substitute. The amendment added the definition of “authorized user” to the bill and amended the definition of “without authorization” in the bill. The bill defines each phrase as follows:

> ‘Without authorization’ means access to a protected computer by any of the following: (a) a person who is not an authorized user; (b) a person who has stolen a technological access barrier of an authorized user; or (c) a person circumventing a technological access barrier on a protected computer without the express or implied permission of the owner, operator, or lessee of the protected computer or the express or implied permission of the owner of information stored in the protected computer. For purposes of this paragraph, the term does not include circumventing a technological measure that does not effectively control

access to the protected computer or the information stored in the protected computer.

‘Authorized user’ means, with respect to a protected computer: (a) a director, officer or employee of the owner, operator or lessee of such computer or the owner of information stored in such computer; or (b) such owner’s third-party agent, contractor, or consultant, or any respective employee of such third-party agent, contractor or consultant, provided that such person has been granted access to the protected computer by the owner, operator, or lessee of such computer or the owner of information stored in such computer in the form of a technological access barrier. An employer provides explicit permission to an employee by providing the employee with a technological access barrier within the scope of the employee’s employment. Such permission is deemed terminated upon cessation of the employee’s employment.

On March 11, 2015, the Judiciary Committee adopted a strike all amendment and reported the bill favorably as a committee substitute. The strike all amendment provided a short title, clarified the definition of "authorized user" and "without authorization", exempted technology service providers from the provisions of the bill, and made technical, grammatical, and stylistic changes.

This analysis is drafted to the committee substitute as passed by the Judiciary Committee.