GENERAL INFORMATION

Submitted By: Business Law Section
Address: The Florida Bar
Position Level: Section

PROPOSED ADVOCACY

All types of partisan advocacy or nonpartisan technical assistance should be presented to the Board of Governors via this request form. Every request should be accompanied by a copy of any existing or proposed legislation, or a detailed presentation of the matter at issue. Contact the Governmental Affairs office with questions.

If Applicable, List The Following:

Indicate Position: Support

Proposed Wording of Position for Official Publication:

Supports anti-hacking legislation including passage of the Computer Abuse and Data Recovery Act (CADRA).

Reasons For Proposed Advocacy:

It is the purpose and the policy of the Act to (a) protect owners, operators and lessees of computers used in the operation of a business from harm or losses caused by unauthorized access to protected computers and (b) to protect owners of information stored in protected computers used in the operation of a business from harm or losses caused by unauthorized access to protected computers.

PRIOR POSITIONS TAKEN ON THIS ISSUE

Please indicate any prior Bar or section/division/committee positions on this issue, to include opposing positions. Contact the Governmental Affairs office if assistance is needed in completing this portion of the request form.

Most Recent Position: None

Others (Attach list if more than one)
(Bar / Section / Division / Committee) (Support or Oppose) (Date): N/A

REFERRALS TO OTHER SECTIONS, COMMITTEES OR LEGAL ORGANIZATIONS
A request for action on a legislative position must be circulated to all divisions, sections and committees that might be interested in the issue. The Legislation Committee and Board of Governors may delay final action on a request in the absence of any responses from such groups. Please include all responses with this form.

**Referrals:**
Criminal Law Section of the Florida Bar, Real Property Probate and Trust Law Section of the Florida Bar, Family Law and Trial Lawyer Section of the Florida Bar.

---

### CONTACTS

**Board & Legislation Committee Appearance:**

Aimee Diaz Lyon, 215 South Monroe Street, Tallahassee, FL 32301, 850-205-9000

**Appearances Before Legislators:**

- Robert Kain, Kain & Associates, 900 S.E. 3rd Ave., Suite 205, Ft. Lauderdale, FL 33316, (954) 768-9002
- Mark Stein, Higer, Lichter & Givner LLP, 18305 Biscayne Blvd., Ste 302, Aventura, FL 33160, (305) 356-7550
- Michael Chesal, Peretz Chesal & Herrmann, P.L., 2 S Biscayne Blvd Ste 3700 Miami, FL 33131-1818, (305) 341-3000
- Aimee Diaz Lyon and Greg Black, Metz Husband and Daughton, 215 South Monroe Street, Tallahassee, FL 32301, (850) 205-9000

**Meetings With Legislators/Staff:**

- Robert Kain, Kain & Associates, 900 S.E. 3rd Ave., Suite 205, Ft. Lauderdale, FL 33316, 954-768-9002
- Mark Stein, Higer, Lichter & Givner LLP, 18305 Biscayne Blvd., Ste 302, Aventura, FL 33160, (305) 356-7550
- Michael Chesal, Peretz Chesal & Herrmann, P.L., 2 S Biscayne Blvd Ste 3700 Miami, FL 33131-1818, (305) 341-3000
- Aimee Diaz Lyon and Greg Black, Metz Husband and Daughton, 215 South Monroe Street, Tallahassee, FL 32301, (850) 205-9000

Please submit completed Legislative Position Request Form, along with attachments, to the Governmental Affairs Office of The Florida Bar. Upon receipt, staff will further coordinate the scheduling for final Bar action of your request – which may involve a separate appearance before the Legislation Committee unless otherwise advised.

For information or assistance, please contact the Governmental Affairs Office of The Florida Bar at 800-342-8060, extension 5662.

Revised 080915

SUMMARY

The proposed Computer Abuse and Data Recovery Act (CADRA) protects owners, operators and lessees of protected computers and owners of information stored in protected computers from hackers and others who misappropriate passwords or override technologic access barriers in protected computers. CADRA is limited to business operations using protected computers which store business information. “Protected computers” are computers which are password protected or which utilize technological access barriers such as security codes, security tokens, key fobs or other access control devices for hardware, software or digital information.

WHY

Florida businesses need an effective civil remedies statute that provides redress for persons who, without authority, access or take computer data, or destroy computer data or systems. These violators might be insiders, such as disloyal employees or bad contractors, or they could be outsiders who hack into computers taking data and potentially destroying hardware, software and valuable data.

Currently, Florida's Computer Crimes Act, Fla. Stat. § 815.01 et seq., ("Fla-CCA") is not a viable civil liability statute because, in order to support a claim for civil damages, the violator must be first convicted of a computer crime under the statute. Even if this is achieved, the Fla-CCA specifically excludes employees "acting in the scope of their lawful employment" and Florida courts have interpreted "acting in the scope of their lawful employment" to mean that if they EVER had authorized access, the statute does not apply even if they were no longer employees at the time of the access or if they used the data to intentionally harm the employer.

As for federal remedies, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, ("Fed-CFAA") covers similar issues and also provides for a civil remedy, if the damages exceed $5,000. Unlike the Fla-CCA, the Fed-CFAA has both an "unauthorized access" and "exceeds authorized access" cause of action. Like the Fla-CCA, the Fed-CFAA is primarily criminal in nature, and has been strictly construed by some regional federal appellate courts (the 9th and the 4th Circuits). These courts hold that if the accused has any type of authorized access to the data or computer, then he or she does not violate the Act. Other federal appellate courts (the 1st, 5th, and 7th Circuits), have given a broader interpretation of what is meant by "exceeds authorized access." The 11th Circuit seems to lean towards a broader interpretation of the Fed-CFAA, but the scope of the leading 11th Circuit decision is less than clear on this issue. The criminal conviction prerequisite in the Fla-CCA combined with the circuit split with some appellate courts finding no liability makes civil actions under Fed-CFAA increasingly difficult.
CADRA VIOLATIONS

A CADRA violation occurs when a person knowingly and with intent to cause harm or loss (a) obtains information from a protected computer without authorization and causes harm or loss; (b) causes transmission of a program, code or command without authorization to a protected computer and causes harm or loss or (c) traffics in any password, security code or access device through which access to a protected computer may be obtained without authorization. A person who violates Section 668.803(a), (b) or (c) is liable to the owner of the information used in his or her business stored in the protected computer or the owner, operator or lessee of the protected computer.

The injured party may bring a CADRA action seeking to recover actual damages including loss profits and losses and the violator’s profits. The injured party may also seek injunctive or other equitable relief to prevent violation of CADRA and to recover the original and all copies of the information which is subject to the violation. This injunctive relief, for the original and all copies, is important in business disputes. Attorneys fees are available to the prevailing party. The action must be brought within three years of the violation or the reasonable discovery thereof.

CADRA defines the term “protected computer” as a computer storing information used in business when the information and/or the computer has a technological access barrier such as a password, security code or token, key fob, access device or other similar measure. “Without authorization,” is a predicate for a CADRA violation and means to circumvent the technological access barrier (for example, a password) to the protected computer without the express or implied permission of the owner. “Without authorization” does not include circumventing a technological measure that does not effectively control access to the protected computer or the information stored therein. “Harm” is defined as including impairment to the integrity, access or availability of the data, program or information. A “loss” is (1) any reasonable cost to the owner of the information or the owner of the protected computer, including the reasonable cost of responding to the violation, conducting a damage assessment and follow-on remediation efforts, (2) economic damages, (3) lost profits, (4) consequential damages including but not limited to interruption of service, and (5) profits derived from a violation.

In conclusion, CADRA will provide Florida businesses with a civil remedy for computer-related abuses, including retrieval of programs, code and information and reasonable compensation for investigation and remediation of computer data-related losses.

Robert Kain, Esq.
Kain & Assoc.
Fort Lauderdale, Fl
rkain@complexip.com
ofc. 954-768-9002
Computer Abuse and Data Recovery Act (“CADRA”) (Aug. 30, 2014)

Electronic Commerce
Part V: Computer Abuse and Data Recovery Act

668.801  Short Title.
This part may be cited as the "Computer Abuse and Data Recovery Act."

668.802  Purposes.
The provisions of this part shall be construed liberally to promote the following policies:

(a) to protect owners, operators and lessees of computers used in the operation of a business from harm or losses caused by unauthorized access to protected computers; and/or

(b) to protect owners of information stored in protected computers used in the operation of a business from harm or losses caused by unauthorized access to protected computers.

668.803  Prohibited Acts.
Whoever knowingly and with intent to cause harm or loss –

(a) obtains information from a protected computer without authorization and as a result thereof causes harm or loss;

(b) causes the transmission of a program, code, or command without authorization to a protected computer, and as a result of such transmission, causes harm or loss; or

(c) traffics in any password, security code or token, key fob, access device or similar information or device through which access to a protected computer may be obtained without authorization;

shall be liable to the extent provided in s. 668.804 in a civil action to: (i) the owner of the information who uses the information in connection with the operation of a business in connection with the protected computer, or (ii) the owner, operator or lessee of the protected computer.

668.804  Remedies.
(a) A person bringing an action under s. 668.803 for a violation may:

(1) recover such person’s actual damages, including lost profits and losses;
(2) recover the violator's profits that are not taken into account in computing actual damages and losses under s. 668.804(a)(1);
(3) obtain injunctive or other equitable relief from the court to prevent a violation of s.
668.803; and
(4) recover the original and all copies of the information which is subject to the violation.

(b) In any action arising under this part, a court shall award reasonable attorney's fees to the prevailing party.

(c) The remedies available for a violation of s. 668.803 are in addition to remedies otherwise available for the same conduct under federal or state law.

(d) A final judgment or decree rendered in favor of the state in any criminal proceeding concerning the conduct of the defendant which forms the basis for any criminal proceeding under chapter 815, shall estop the defendant in any action brought pursuant to s. 668.803 as to all matters as to which such judgment or decree would be an estoppel as if the plaintiff had been a party in the criminal action.

(e) A civil action filed under s. 668.803 shall be commenced within three years of the time the violation occurred or within three years of the time the violation was discovered or should have been discovered with the exercise of due diligence.

668.805 Definitions.

As used in this part, the term:

(a) "Computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility, data storage device or communications facility directly related to or operating in conjunction with such device.

(b) "Protected computer" means a computer, used in connection with the operation of a business and storing information, programs or code used in connection with the operation of a business, in which the information, programs or code can only be accessed through a technological access barrier such as a password, security code or token, key fob, access device, or similar measure.

(c) “Without authorization” means to circumvent a technological access barrier to a protected computer, without the express or implied permission of the owner, operator or lessee of the computer to access the protected computer or the express or implied permission of the owner of information stored in the protected computer, but 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.

(d) "Harm" means any impairment to the integrity, access or availability of data, a program, a system, or information.

(e) "Loss" means: (1) any reasonable cost to the owner of information stored in a protected
computer or the owner, operator or lessee of a protected computer, including the reasonable cost of responding to the violation, conducting a damage assessment for harm associated with the violation, and remediation efforts including restoring the data, program, system, or information to its condition prior to the violation, (2) economic damages, (3) lost profits, (4) consequential damages including but not limited to interruption of service, and (5) profits derived from a violation.

(f) “Traffics” means to sell, purchase or deliver.

(g) “Business” includes any trade or business without regard to its profit or nonprofit status.

668.806 Exclusions.

This part does not prohibit any lawfully authorized investigative, protective, or intelligence activity of any law enforcement agency, regulatory agency or political subdivision of this State, any other state, the United States or any foreign country.