Computer Abuse and Data Recovery Act (CADRA) - White Paper (Aug26)

A. Purpose and Problem

Florida businesses need a civil remedies statute that permits the recovery of damages and remediation losses from persons who, without authority, access or take computer data, or destroy data or computer systems. These violators might be insiders, such as disloyal employees or contractors or they could be outsiders who hack into these computers taking data and potentially destroying hardware, software and valuable digital information. The unique aspects of computer use, computer abuse and misappropriation of computer data require special consideration beyond existing trade secret, tortious interference, fraud, unfair competition and civil theft statutes because the unauthorized access itself causes harm resulting in the wrongdoer possessing the valuable data. Of course, unauthorized access to the data is a stepping stone to other prohibited acts in the Computer Abuse and Data Recovery Act.

Currently, Florida's Computer Crimes Act, Fla. Stat. § 815.01 et seq. (“Fla-815”), provides only a marginal civil remedy for computer abuses because (a) in order to support a claim for civil damages, the violator must first be convicted of a computer crime and (b) Florida courts effectively hold that if the accused/defendant as some type of “authorized access” to the data or computer, then he or she does not commit the crime. The Fla-815 Act specifically excludes employees “acting in the scope of their lawful employment.” Florida courts have interpreted “acting in the scope of their lawful employment” to mean that if the accused/defendant EVER had authorized access, the statute does not apply even if they were not employees at the time of the access and even if they used the data to intentionally harm the employer.

Since most Florida-based computers operate in interstate commerce (by accessing the internet), the Federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (“Fed-1030”), covers similar issues and also provides a civil remedy if the damages exceed $5,000. However, the Fed-1030 Act is primarily criminal in nature and criminal statutes are narrowly construed by the courts. The Fed-

An injured party "may bring a civil action against any person convicted" under the Act. Fla.Stat. § 815.06.

Florida courts have interpreted "exceeds authorized access" as not necessarily "without authorization." Gallagher v State, 618 So.2d 757 (Fla. 4th DCA 1993). In Armando Miguel Rodriguez v State, 956 So.2d 1226 (Fla. 4th DCA 2007), the court differentiated "authorized access" from "exceeds authorized access" and found that §815.06 does not apply to "exceeds authorized access".

Fla. Stat. 815.06(6).

Armando Miguel Rodriguez v State, 956 So.2d 1226 (Fla. 4th DCA 2007).

Statutes criminalizing the access, theft and misuse of intellectual property have been narrowly interpreted under the rule of lenity because, given a choice between two constructs, the
1030 Act has been strictly and narrowly construed by some regional federal appellate courts (namely, the 9th and the 4th Circuits). These courts held that if the accused as any type of “authorized access” to the data or computer, then he or she does not violate the Fed-1030 Act. Other federal appellate courts (namely, the 1st, 5th, and 7th Circuits), have more broadly interpreted the meaning of “exceeds authorized access.” The 11th Circuit Court of Appeals, which hears matters from Florida’s U.S. District Courts, seems to lean towards a broader interpretation of Fed-1030, but the scope of the leading 11th Circuit decision is less than clear on this point. This conflict in the federal courts makes private enforcement actions in Florida difficult.

Florida businesses need a civil remedy to deal with computer abuse and misappropriation of computer data. A purely civil remedy statute is needed because the Fla-815 and the Fed-1030 are primarily criminal statutes with an add-on civil remedy, courts narrowly construe criminal statutes, and, in a civil law context, courts need some discretion to ascertain what is and what is not unauthorized access to the computer system or computer data.

B. The Solution: The Computer Abuse and Data Recovery Act (CADRA)

CADRA is a new civil liability act which protects business owners who use computer systems and data from outsiders and insiders who, without authority, access and take data for the economic benefit of themselves or others, or destroy data, systems or software.

6. The 9th Circuit Court of Appeals in 2012 held that the Fed-1030 does not cover an errant employee or an insider that takes data and uses it in an anti-competitive manner after leaving the company. United States v. Nosal, 676 F.3d 854 (9th Cir. 2012)(en banc). Three months later, the 4th Circuit Court of Appeals agreed and held that the Fed-1030 was not violated unless the employee lacks any authorization to obtain or alter the data when he was employed. WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012)(after resigning, the ex-employee used the data in an anti-competitive manner).

7. See Int'l Airport Centers, L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006)(after resigning, the ex-employee used the data in an anti-competitive manner and violated the Act); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 578-79 (1st Cir. 2001)(an employment agreement establishes the parameters of unauthorized access); and United States v. John, 597 F.3d 263 (5th Cir. 2010)(errant employee violated statute even though she rightfully had access to the computer data, but then gave the data to cohorts who incurred fraudulent credit card charges).

8. In United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010), the court found that the errant employee violated statute even though he never used the data for financial gain. The scope of what "exceeds authorized access" was not clearly explained by the court.
A CADRA violation involves knowingly:

(1)(A) accessing a computer without authorization (which is the same as exceeding authorization) and obtaining information;
(1)(B) accessing a computer without authorization and giving it to a person who is not entitled to have it;
(1)(C) accessing a computer without authorization and retaining it and failing to deliver all copies of the information to the rightful owner;
(2)(A) while employed or under contract with the owner, accessing a computer, obtaining information and after termination, failing to return the same upon demand without legal justification;
(2)(B) while employed or under contract with the owner, accessing a computer, obtaining information, and after the employee is terminated, failing to return the same upon demand without legal justification;
(3) with intent to defraud, accessing a computer without authorization and (A) obtaining information, or (B) giving the information to another who is not entitled to receive it;
(4) transmitting a program, code or command which causes damage or loss to the computer;
(5) accessing a computer without authorization and causing damage or loss;
(6) trafficking in a password used to access a computer; or
(7) trafficking in a password used to obtain unauthorized access to a computer.

CADRA remedies are limited to business owners who are (a) the rightful owner of the computer information and (b) the owner, operator or leasee of the computer with the business data. Private causes of action, not related to business information or computers used in business, are not subject to the Act. Damages can be recovered for the owner’s actual damages and losses for remediating the damage to computers or data. Business owners can seek injunctive relief to recover the original and all copies of the information and seek other equitable remedies against threatened loss or damage. Attorneys fees are available to the prevailing party in the court’s discretion.

To overcome uncertainties regarding what is the meaning of “exceeds authorized access” and similar “authority” clauses, CADRA applies a multi-factor test. Factors which determine unauthorized access include: (a) bad faith intent to profit; (b) malicious behavior; (c) acting for the benefit of another; (d) violating a written agreement between the parties; (e) violating a written policy of an employer; (f) considering the fiduciary duties of the person charged with a violation; (g) determining whether the computer was protected by password not assigned to that person; and (h) determining whether the business information was protected by a password not assigned to that person.

---

9 See CADRA sec. 668.802(a), Prohibited Acts. White-Paper-CANDRA-(Aug26-2013)