MEMO: Response to Business Litigation Committee's Comments Aug. 8, 2013

From: Robert Kain, Chair of CADRA Committee, rkain@ComplexIP.com
Date: Aug. 25, 2013

Introduction:

We, the Computer Abuse and Data Recovery Act (CADRA) Committee ("C-Comm") appreciate the comments from the Business Litigation Committee ("B-Comm"). The responses below are presented by Robert Kain, the chair of C-Comm, and are consistent with the C-Comm's views except were otherwise noted. This Response Memo will be circulated to the C-Comm and supplemented as needed prior to Labor Day Retreat meetings (the "Retreat").

Issue 1:

Regarding the addition of the term "legal justification" to Section 668.802, the [B-Comm] Committee is concerned that this term is not defined and may cause even more confusion. What would constitute legal justification? Does a whistle blower or employee who feels they have been discriminated against have legal justification to keep data? Is it akin to preserving evidence? Is CADRA the law which they need legal justification from?

Response 1:

In summary, the CADRA Violations 668.802(a)(2)(A) and (B) (an "(a)(2)(A)-(B)" act or action) are: (a) some of the most commonly occurring I.P. abuses; (b) the most important to consider in balancing rights and obligations of the employee/contract-vendor with the employer/contract-purchaser; and (c) to be considered with an understanding of the definitions of "exceeds authorized access" and similar terms in CADRA sec. 804(a)(3). "Legal justification" is meant to refer to any recognized statutory or common law defense which may be raised by an employee/contract-vendor. "Legal justification" is a defense to an "access" and "no return of data" violation directed at an employee/contract-vendor under CADRA (a)(2)(A)-(B) when access to data was permitted or authorized, the data taken, but then not returned. The "legal justification" defense for other CADRA violations is not set forth in CADRA sections.

Details: A high level view of CADRA is that it creates a statutory violation based upon unauthorized access to computer data, computer software and hardware. The rationale for this unauthorized access violation is that (a) the economic value of computer data is difficult to ascertain; (b) explaining all steps taken to secure the "secret" nature of the data to the court is difficult, time consuming and sometimes misunderstood due to technical terms used in the computer industry; and (c) the value of the computer data may greatly diminish over a short period of time. The C-Comm thought that most, if not all, CADRA violations are also violations of Florida's Uniform Trade Secret Act, Fla.Stat. 688.001, Florida's Deceptive and Unfair Trade Practices Act (FDUTPA), F.S. §§501.201, or acts of unfair competition ("UC")(see UC common law). However, the application of those laws to remedy the "unauthorized access" and/or the "taking" of computer data was too cumbersome and complicated for the court systems.

For over nearly 20 years, I.P. lawyers have used the predecessor computer crimes statutes, Florida's Computer Crimes Act, Fla. Stat. § 815.01 and the Federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030, to provide remedies for computer abuses. These criminal statutes have follow-on civil remedies. Notwithstanding this long 20 year history, the issues of what is and what is not "unauthorized access" have not been solved by the court systems, on the federal level nor on the state level. Only recently in 2012 have the federal courts split on the issue of what is unauthorized access. Surprisingly, the issues involving unauthorized access were identified 20 years ago by the Chair of the C-Comm in an obscure law review article.

Initially, the C-Comm thought that other states may have solved the unauthorized access problem and balanced the rights and obligations of the employee/contract-vendor with the employer/contract-purchaser, but a survey of other state statutes revealed no helpful guidelines. The balance proposed by the C-Comm is (1) guidance to the courts as to factors to consider for determining what is or is not unauthorized access (and the closely related concept of exceeds authorized access); (2) the requirement of intentional acts (referring to "knowingly" and "willfully"); and (3) the employee/contract-vendor's defense of legal justification when (i) computer data is obtained when access is permitted, but (ii) after termination, a demand for computer data is made and (iii) after demand, the computer data, computer software or hardware is not returned. A CADRA (a)(2)(A) violation is post employment/contract termination and a CADRA (a)(2)(B) violation is "during his or her employment" meaning that the CADRA cannot be violated by an independent contractor (an "IC") during the period of the contract. With respect to a claimed violation of CADRA (a)(2)(A) and a terminated IC (a contract-vendor), C-Comm thought that contractual defenses are part of a "legal justification" defense.

Lastly, it is the C-Comm Chair's opinion that to engage in further IC hypotheticals under CADRA, seems to miss the entire point of the new statute which is: (A) to fill a gap in the legal protection for computer data, computer software and hardware; (B) to provide the state courts with guidelines which are mainly unique to computers re: (i) access; (ii) difficulty in determining independent economic value; (iii) difficulty in determining what type of a security systems are necessary; (iv) how the security systems are deployed and used; (v) how the security protocols are enforced; (vi) the knowledge and intent of the accused violators; and (vii) the relatively quick return of I.P. property.

It is the C-Comm's Chair's opinion that the "legal justification" defense for other CADRA violations is not set forth in other CADRA sections and that the courts will be judicious in the application of recognized statutory or common law defenses. The C-Comm has not conducted legal research on "legal justification" defenses to Florida's Computer Crimes Act, Fla. Stat. § 815.01; the Federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Florida's Uniform Trade Secret Act, Fla.Stat. 688.001; or Florida's Deceptive and Unfair Trade Practices Act (FDUTPA), F.S. §§501.201. However, it is the C-Comm Chair's opinion that "legal justification" defenses based upon statutory and common law are available in the defense of these other I.P. statutes.

Issue 2:

The Committee has questions regarding the definition of a "protected computer." The definition appears to be circular. What isn't a protected computer? Is it necessary to use the term protected computer as opposed to any computer? It seems the definition makes a computer, whether password protected or not, becomes a protected computer by virtue of the commission of one of the prohibited acts.

Response 2:

The short answer is that C-Comm did consider the definition of "protected computer" (a) when it initially drafted CADRA and (b) after the June B-Comm meeting, and decided that the definition was reasonable and necessary. In detail, CADRA is strictly limited to business related events because the C-Comm did not want to consider other ramifications for personal use computers, smart phones, issues of personal privacy, and family law issues (parent-child concerns, husband/wife/martial partner issues, ex-spousal issues, etc.). The basic design of CADRA is to control unauthorized access, coupled with the taking or misuse of data/software/hardware used in business.

The B-Comm is correct that the definition of "protected computer" is circular and this was the intent of the C-Comm.

Issue 3:

Also, the Committee is concerned the use of words like "willfully" and "knowingly" and "with intent to defraud" may become problematic. Are they necessary for the statute to achieve its purposes? Does "fails to return without legal justification" turn "I forgot" into a criminal offense?

Response 3:

The C-Comm, on three different and separate occasions, discussed (i) the overlap of certain CADRA provisions (sec. (a)(1)(A) - "knowingly and willfully obtaining data" overlaps (a)(3) - "with intent to defraud" because an (a)(3) violation must include an (a)(1)(A) violation); and (ii) the multiple uses of "knowingly" with "willfully". The overlap was thought necessary because a primary purpose of CADRA is to provide guidance to the courts. If the court can follow the words of the statute in a particular section, then this was thought by C-Comm to provide a better statutory structure.

With respect to multiple uses of "knowingly" with "willfully," these terms were used to achieve a balance between inadvertent acts by an employee/contract-vendor and the requirement that the follow-on act ("obtaining information", see (a)(1)(A)) be willful. If the employee/contract-vendor knowingly obtains the information, the follow-on act must be willful to support a CADRA violation. If the employee/contract-vendor obtains the data and then the data stored by the employee/contract-vendor is hacked by a third party and the employer/contract-purchaser data is taken by the hacker, then this is not a CADRA violation.

The multiple uses of "knowingly" with "willfully" also seek to establish, in some cases, an "I forgot" defense. The C-Comm notes that in most I.P. misuse/misappropriation situations, a cease and desist letter is set to the accused prior to litigation and this demand letter will diffuse the "I forgot" defense and may trigger an explanation of the "legal justification" defense.

Also, multiple uses of "knowingly" with "willfully" and the factor-based definition of unauthorized access (and the closely related "exceeds authorized access") takes into account the current trend of employers to request that employees use the employee's own smart phones/tablets/computers to access company data and systems (this is the "BYOD" issue ("bring your own device" to work)).

Lastly, CADRA is not a criminal statute, but is a civil remedies statute for businesses.

Issue 4:

Also, the Committee proposes consolidating the factors the Court may consider in the proposed 688.804 to the following: (1) the person's object or intent in accessing the information; (2) whether the act of accessing the information was a breach of a duty created by contract or imposed by law; and (3) the steps the owner took to protect the information.

Response 4:

The following is a correlation between Issue 4 and points 1 - 3 above and the factor-based definition in 804(a)(3):

(4.1) the person's object or intent in accessing the information;

See Factor A, B, C; see also violations 801(a)(1)(B); 801(a)(3); 801(a)(6); 801(a)(7).

(4.2) whether the act of accessing the information was a breach of a duty created by contract or imposed by law;

See Factor C, D, E, F.

(4.33) the steps the owner took to protect the information.

See Factor D, E, F, G, H.

General Comments on the Factors: The C-Comm believes that the laundry list of factors will prompt the Florida business community to set forth in writing the obligations of an employee/contract-vendor. Employers should use publish and actively inform their employees and contract-vendors of obligations to keep computer data secure, safe and not to abuse that data. The C-Comm believes that written policies, proactively presented by employers to employees, and password controls should become common if businesses want the full benefit of CADRA. The laundry list of factors promotes this goal of employers informing employee/contract-vendors.

Issue 5:

There is a concern that this statute moves the balance toward former employers and away from former employees.

Response 5:

The B-Comm is correct on this point. However under the present laws, the only remedies available to the employer/contract-purchaser are Florida's Uniform Trade Secret Act, Fla.Stat. 688.001; Florida's Deceptive and Unfair Trade Practices Act (FDUTPA), F.S. §§501.201; Florida's Civil Remedies for Criminal Practices Act, Fla. Stat. 772.11 (Civil remedy for theft or exploitation); breach of contract theories and the application of common law unfair competition.

The C-Comm sought to balance the former employees interests with the multiple uses of "knowingly" with "willfully" and the factor-based definition of unauthorized access and the closely related "exceeds authorized access."

Also, the C-Comm thought that the former employees would benefit from the prevailing party - attorneys fees clause, sec. 803(c).

Issue 6:

A technical comment: 668.802(a), subparagraphs (1), (2), (3) and (4), do not have an "or" at the end, while (5) and (6) do have an "or" at the end. It seems from the white paper that each of the subparagraph was intended to give rise to a cause of action. Hence, either have only one "or" after (6), or have each subparagraph end with an "or."

Response 6:

Well stated. A correction will be made. See CADRA (Aug25).

Issue 7:

Did the group consider including a minimum statutory damage -- for example, $5,000? Is the statute intended to cover a single computer that was hacked into but actual harm done was nominal or speculative?

Response 7:

This issue of minimum damages, and the issue of mandatory attorneys fees award (the current CADRA sec. 803(c) includes a discretionary attorneys fees clause), was one of the most divisive issues for C-Comm. A reasonable majority supported no minimum damages and no mandatory attorneys fees (which were limited to bad faith prosecutions) but the minority position was strong and vocal.

The B-Comm at its June meeting discussed a CADRA clause calling for mandatory attorneys fees for bad faith prosecutions. At that time, it seemed to the Chair of C-Comm that

B-Comm was solidly AGAINST mandatory attorneys fees for bad faith prosecutions, citing Fla. Stat. 57.105.

More precisely stated, the C-Comm Chair put the following to a vote: "The Biz-Lit Committee suggested that [mandatory attorneys fees section] 803(d) be deleted because new laws [such as CADRA] should not conflict with Fla. Stat. 57.105 and set (i) new burdens of proof or (ii) new procedures for what is effectively bad faith litigation. My personal view [the Chair's], after reading Fla. Stat. 57.105 is that the Biz- Law Committee has a well stated point." Two-thirds of the C-Comm APPROVED deleting the mandatory attorneys fees section over a vocal dissent.

Issue 8:

Regarding the "trafficking" in passwords: [1] how would the statute apply to an employee who is authorized and then loans his password to another authorized employee, who has forgotten/lost his password and then commits one of the illegal acts? [2] What if the recipient of the password senior to the first employee and the "trafficker" was required to provide the password to the senior employee? [3] Would the one time instance of providing a password constitute trafficking? [4] Is profit or benefit a component? [5] Perhaps "trafficking" needs a definition?

Response 8:

The term "trafficking" is fairly well defined by the courts in connection with criminal actions. It seemed to the C-Comm that a CADRA definition would alter the meaning of trafficking without a significant beneficial result for the overall purpose of CADRA. Also, the courts could look to other computer crime statutory meanings to ascertain the scope and meaning of "trafficking."

8.1 "How would the statute apply to an employee who is authorized and then loans his password to another authorized employee, who has forgotten/lost his password and then commits one of the illegal acts?" – The C-Comm Chair thinks that trafficking requires a transaction between two or more people. The first employee does not violate CADRA because no "knowing" trafficking. The second employee does violate CADRA if a transfer of the password occurs. Also, the CADRA plaintiff must have a loss or damage. See CADRA 803(a)(who may bring an action); 804(a)(4)(damage; the C-Comm believes these damages are the same as consequential damages); 804(a)(4)(loss includes the reasonable cost of damage assessment and remediation).

8.2 "What if the recipient of the password [is a] senior [supervisor] to the first employee and the "trafficker" was required to provide the password to the senior employee?" – No violation. No harm, no foul. Also, the senior has "corporate authorization" over the junior employee. The senior employee may be a violator.

8.3 “Would the one time instance of providing a password constitute trafficking?” – Yes, why not?

8.4 “Is profit or benefit a component?” - The C-Comm considered this point and decided that profit or benefit was not a requirement to violate CADRA (a)(6) or (a)(7) because a vengeful employee or ex-employee can engage in a “bad act” without profit or benefit. The CADRA plaintiff is required to prove loss or damage.

8.5 See initial response to 8 above.

Issue 9:

Is it the intention for 803(b) to include cumulative relief?

Response 9:

In reference to 803(d) (CADRA(Aug 25)), “The remedies available for a violation of section 668.802 are in addition to remedies otherwise available for the same conduct under federal or state law,” YES.

Issue 10:

The word "of" seems to be missing between the words violation and section in 804(a)(5).

Response 10:

The Chair of C-Comm thinks that the section 804(a)(5) below is proper, but will accept further comments.

CADRA 804(a)(5): (5) the term "loss" means any reasonable cost to any person, including the reasonable cost of responding to the violation, conducting a damage assessment, and remediation efforts including restoring the data, program, system, or information to its condition prior to the violation, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service, and profits derived from a violation section 688.802(a).

Issue 11:

Was there any thought to making the attorneys' fee provision mandatory rather than discretionary?

Response 11:

See Response 7 above.

Issue 12:

Regarding the 3 year statute of limitations, was there a consideration of adding something like: "or should have been discovered with reasonable diligence"?

Response 12:

There was some discussion of this concept, but the C-Comm decided not to expand the scope of this clause. The C-Comm thought that courts may apply such considerations to this CADRA section. Rather than create a different standard, different than other applications of I.P. laws to the same concept, omitting this clause from CADRA seemed to be better than adding this clause and creating confusion.

Issue 13 (White Paper, Aug 12):

It looks like the proposed CADRA statute attached to your more recent email was not modified but the white paper has been revised. My comments to the statute remain applicable. What I said regarding comment 6 (C) of the earlier draft White Paper still applies even though the specific language that I addressed has been removed in the revised version. It is misleading to say CADRA is violated by…willfully retaining proprietary information and failing to deliver the same upon demand to the rightful owner without legal justification. [See second paragraph under Section B of white paper with regard to 668.802 (1)(C) and (2) (A). This statute does not address third parties who are in possession of data which was obtained by the illegal access of a protected computer. I have copied my initial comment below. …

Comment 6(c) in the White Paper suggests that there can be a civil claim against a person who retains proprietary information after demand is made by the rightful owner. I do not see where this is included within the 668.802(a) prohibited acts. (a)(2) is limited to persons having privity with the rightful owner and requires access of the protected computer. Nothing in the act provides the civil remedy to a third party who comes in possession of the information that was stored in the protected computer. In other words the statute does not address those who benefit from the illegal access committed by another but was not involved in any of the illegal acts.

Response 13:

To be addressed later - possibly at the Retreat.

/s/RobertKain

LR-MEMO-BizLit(Aug25).wpd