

# **NOT JUST FOR HACKERS ANYMORE?**

## **USE OF THE COMPUTER FRAUD AND ABUSE ACT TO RESPOND TO THEFT OF INFORMATION**

---

### **A ROUNDTABLE DISCUSSION ORGANIZED BY THE TRADE SECRETS SUBCOMMITTEE**

LINDA K. STEVENS (SCHIFF HARDIN LLP, CHICAGO) AND  
ROBERT GERBER (SHEPPARD MULLIN, LOS ANGELES), CO-CHAIRS

---

#### **CARLA M. PERROTTA**

MILLER, CANFIELD, PADDOCK, AND STONE, P.L.C.  
150 W. JEFFERSON, SUITE 2500, DETROIT, MI 48226-4415  
313.496.8472 / PERROTTA@MILLERCANFIELD.COM

#### **ABRAHAM (AVI) SKOFF**

MOSES & SINGER LLP  
405 LEXINGTON AVENUE, NEW YORK, NY 10174-1299  
212.554.7897 / ASKOFF@MOSESSINGER.COM

#### **LINDA K. STEVENS**

CO-CHAIR, TRADE SECRETS SUBCOMMITTEE  
SCHIFF HARDIN LLP  
6600 SEARS TOWER, CHICAGO, ILLINOIS 60606  
312.258.5667 / LSTEVENS@SCHIFFHARDIN.COM

**Introduction:** A disgruntled departing employee can access computer infrastructure and copy or erase valuable files, resulting in devastating financial losses and significant disruption to a company's overall operations. In some jurisdictions, the Computer Fraud and Abuse Act (the "CFAA"), 18 U.S.C. §1030, *et seq.* may provide a remedy for these problems. Originally enacted as a criminal statute, the CFAA was intended to protect government computers from attacks by "outside" computer hackers. Having been amended several times, the CFAA now

offers civil plaintiffs an array of remedies as well as an entrée to federal court. Courts do not agree, however, about the CFAA's applicability to employee computer abuse and its application to cases regarding the theft of data and information. Join us as we discuss the CFAA and its applicability to trade secrets cases.

## I. Prohibited Conduct

As originally enacted in 1984, the CFAA was a criminal statute, directed primarily at supplementing the mail and wire fraud statutes to protect government and financial computers from hacking. Starting with an amendment in the mid-1990's, the scope of prohibited criminal conduct has been expanded, and civil liability has been established. The CFAA establishes criminal liability for the wrongful use of covered computers, to obtain, disclose, use and/or damage, information and systems to which the user does not have lawful access. The statute also establishes civil liability where certain types of conduct are involved in these violations.

The conduct criminalized by the statute is broad, and includes theft of national security information, unauthorized accessing of information from financial institutions, "hacking," the transmission of malicious code, the theft of information from protected private or commercial computers, as well as other conduct. 10 U.S.C. 1030 (a) and (b) define the criminal conduct. 18 U.S.C. 1030(g) establishes civil liability. Section 1030 (c) provides the criminal sentencing scheme, § 1030(e) provides definitions, and §1030(i) establishes criminal forfeiture of both the instrumentalities used in a violation, and proceeds traceable to a violation.

### 1. Criminal conduct.

(i) The CFAA prohibits the **knowing or intentional access of a computer without authorization, or exceeding authorized access**, and thereby: obtaining and using or disclosing, protected U.S. Government information, 18 U.S.C. 1030(a)(1), (3); obtaining information from financial records of a financial institution, card issuer or consumer reporting agency, 10 U.S.C. 1030(a)(2)(A), from any agency of the United States 18 U.S.C. 1030(a)(2)(B), or from any "protected computer" 18 U.S.C. 1030(a)(2)(C). Section 1030(a)(2)(C) is often a basis for civil claims, and intent to defraud is not required.

**Note: "protected computer" is defined broadly, see 10 U.S.C. 1030(e)(2)(B), covering any computer "used in or affecting" interstate commerce. Presumably, any computer used on the internet would be covered under 10 U.S.C. 1030(e)(2)(B).**

(ii) 18 U.S.C. 1030(a)(4) prohibits **knowing or intentional access of a computer without authorization, or exceeding authorized access**, with intent to defraud, and thereby furthering a fraud and obtaining something of value (other than the use of the computer unless such use is worth more than \$5000). Section 1030(a)(4) requires intent to defraud.

(iii) 18 U.S.C. 1030(a)(5) prohibits unauthorized access to a protected computer which results in damage or loss, as well as the transmission of code or a command that intentionally causes unauthorized destruction.

(iv) 18 U.S.C. 1030(a)(6) prohibits trafficking in passwords, and 1030(a)(7) prohibits extortion based on threats to a protected computer or to the information contained therein.

2. **Civil Liability**. Amendments to the CFAA have afforded a significant civil remedy when the requirements of the statute are met. 18 U.S.C. 1030(g) is the subsection which provides for civil liability:

Any person who suffers **damage or loss** by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware. (emphasis added)

Thus, 18 U.S.C. 1030(g) sets forth the specific requirements for a civil action, and requires both a violation of Section 1030, and that the violation involve one of the factors described in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). The conduct described in these subclauses of 1030(c)(4)(A)(i) is as follows:

(I) **loss** to 1 or more persons during any 1-year period... ..aggregating at least \$5,000 in value;

(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV) a threat to public health or safety;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security. (emphasis added)

Note the interplay of these sections: a plaintiff who is relying on conduct described in §1030(c)(4)(A)(i)(I) must show that the defendant's conduct resulted in a "loss" of at least \$5,000 under Section 1030(c)(4)(A)(i)(I) before plaintiff is entitled to "damages" under Section 1030(g). Distinctions between "loss" and "damage" are discussed below.

**Note: 2008 amendments to the CFAA removed the subclauses of 1030(a)(5)(C), which previously had been designated by the statute as part of the basis of civil claims. Among the provisions removed was the requirement of a "loss" of at least \$5,000 under former 18 U.S.C. 1030(a)(5)(C).**

**However, the 2008 amendments also added substantially similar subclauses (quoted above) to subsection 1030(c)(4)(A)(i). For liability based on conduct described in 1030(c)(4)(i)(I), which appears to be the "successor" to former 1030(a)(5)(B)(i) (on which civil liability has frequently been based), contains a similar \$5,000 requirement.**

**As a result of these 2008 amendments, in analyzing prior case law, the many citations to section 1030(a)(5)(B), must now be compared with the language of 1030(c)(4)(A)(i). In addition, note that sections 1030(a)(5)(A)(i) – (iii) have been renumbered as sections 1030(a)(5)(A) – (C), and subclause (C) (formerly 1030(a)(5)(A)(iii)) now requires a showing of *both* "damage" and "loss", not just "damage," as before. (Apparently, in making these changes, Congress did not believe that the statute was complicated enough and sought to remedy the deficiency.)**

With the advent of private civil liability, the number of litigants using the law increased dramatically. Ensuing decisions have identified and highlighted open issues and undefined terms under the law. Among the most hotly litigated issues under the CFAA are: (i) whether copying or taking information from the employer's computer system for an improper purpose, by an employee who has authorized access to the computer, is accessing "without authorization", or is "exceeding authorized access" within the meaning of the statute; (ii) whether an employee who copies or disseminates confidential information from his employer's computer has violated the statute, if that information is not erased or otherwise made unavailable to the employer.

## **II. CFAA and the Conduct of Disloyal Employees.**

To state a claim under subsections 1030(a)(2) or (a)(4), plaintiff must allege that defendant accessed a protected computer either "without authorization," or that defendant "exceeded authorized access." To state a claim under subsections (a)(5)(A)(B) or (C), defendant's access must be "without authorization."

The CFAA defines “exceeds authorized access” as “access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.” Section 1030(e)(6). The statute contains no definition of access “without authorization”.

When a former employee accesses the former employer’s computer system, and removes, damages or copies nonpublic information, there is little doubt that the CFAA is triggered. However, there is a split in authority –and a great deal of litigation – over whether the CFAA applies to an employee who is authorized to access the employer’s computers system and information, but uses that access for an improper purpose, such as disloyal competitive conduct, violation of a confidentiality agreement, copying and/or erasure of competitive data, etc. Some courts have concluded that, within the meaning of the CFAA, an employee “exceeds” his authorization, or acts without authorization, whenever the employee uses authorized access to obtain and misuse the confidential or proprietary data contained in the employer’s computers, or to otherwise engage in conduct contrary to the employer’s interest. Note, however, that where such liability is found, the basis for this liability differs from court to court.

In the leading case of *Int’l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006), the Seventh Circuit held that the CFAA applied in these circumstances. Defendant Citrin, in violation of his contract with his employer, IAC, decided to quit his job and go into competition. While still employed by IAC, defendant also deleted IAC data from the employer’s computer to which he had authorized access, and introduced “scrubbing” software to hide his improper conduct. In addition to addressing defendant’s deletion of data and introduction of a scrubber program, the Seventh Circuit relied on agency principles and held that the breach by Citrin of his duty of loyalty to his employer, IAC, terminated his agency relationship with IAC, and thus, terminated his authorization to access the computer. In the process, the Seventh Circuit cited to the *Restatement (Second) of Agency*, in defining the scope of this criminal statute.

Other cases have similarly found liability. *E.g.*:

(i) *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582-84 (1st Cir. 2001) (former employee provided other company with nonpublic, proprietary information, in violation of confidentiality agreement, in order to mine former employer’s publicly accessible website; found to have exceeded authorization (as opposed to *Citrin*, where the employee was found to be without authorization));

(ii) *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1124-25 (W.D. Wash. 2000)(employees who had authorized access to employer’s computers, were “without authorization” when they accessed and sent proprietary information to a competitor);

(iii) *Int’l Sec. Mgmt. Group, Inc., v. Sawyer*, No. 3:06cv0456, 2006 U.S. Dist. LEXIS 37059, at \*58-59 (M.D. Tenn. June 6, 2006) (adopting *Explorica* and *Shurgard Storage* without analysis; plaintiff found likely to succeed on CFAA claim, as former employee “exceeded

authorization” when employee emailed confidential information to future partner, in violation of non-disclosure agreement);

(iv) *Sam's Wines & Liquors, Inc. v. Sean Hartig and Plinio Group, LLC*, 2008 U.S. Dist. LEXIS 76451 (N.D.Ill. 2008)(relying on *Citrin*);

(v) *Mintel International Group, Ltd. v. Meesham Neergheen*, No.: 08-CV-3939 (N.D. Ill. July 16, 2008) (*Slip Op.*), citing *YourNetDating, LLC v. Mitchell*, 88 F. Supp. 2d 870, 872 (N.D. Ill. 2000), *Charles Schwab & Co., Inc. v. Carter*, 2005 WL 351929, at \*3 (N.D. Ill. Feb. 11, 2005) and *George S. May Int'l Co. v. Hostetler*, 2004 WL 1197395, at \*3 (N.D. Ill. May 28, 2004);

(vi) *See Pacific Aerospace & Electronics, Inc. v. Taylor*, 293 F.Supp.2d 1188 (E.D. Wash. 2003).

Under these cases, even when an employee has unlimited authority to access the employer’s computers, the employee is deemed to be without authorization, or to be “exceed[ing] authorized access” within the meaning of the CFAA, when the employee engages in conduct which is, or which the employee intends to be, adverse to the interests of the principal.

Other courts have rejected this approach, finding that the CFAA addresses – and criminalizes – the unauthorized accessing of information, not its misuse after being obtained through authorized access. For example, in *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008), the court rejected *Citrin* and *Shurgard* and held that the plain language of the CFAA, its legislative history, and the rule of lenity which governs construction of this criminal statute, all require a more limited reading:

Given the plain language, legislative history, and principles of statutory construction, the restrictive view of "authorization" is adopted. "[A] violation for accessing 'without authorization' occurs only where initial access is not permitted. And a violation for 'exceeding authorized access' occurs where initial access is permitted but the access of certain information is not permitted." (*quoting Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1342, 2007 U.S. Dist. LEXIS 73032, 2007 WL 2904119, at \*13 (N.D. Ga. Oct. 1, 2007); and *Lockheed Martin Corp. v. Speed*, 2006 U.S. Dist. LEXIS 53108, 2006 WL 2683058, at \*5 (M.D. Fla. Aug. 1, 2006))

Other cases hold similarly. *E.g.*:

(i) *Black & Decker (US), Inc. v. Timothy C. Smith*, No. 07-1201 (W.D.Tenn. July 11, 2008) (*Slip Op.*):

The Court agrees with *Lockheed Martin* that the plain meaning of “exceeds authorized access” is “to go beyond the access permitted.” 2006 U.S. Dist. LEXIS 53108, at \*19. Likewise, while there is no definition for access “without

authorization,” the Court finds that its plain meaning is “no access authorization.” *Id.* The Defendant’s alleged conduct clearly does not fall under these definitions, however, as he was permitted access to B&D’s network and any information on that network. The fact that he did not have permission to subsequently misuse the data he accessed by sharing it with any of his former employer’s competitors is another matter that may be circumscribed by a different statute.

(ii) *Brett Senior & Assocs., P.C. v. Fitzgerald*, No. 06-1412, 2007 U.S. Dist. LEXIS 50833, at \*12 (E.D. Pa. July 13, 2007) (“The common thread running through [*Explorica* and cases holding that employee “exceeded authorized access”] is a focus on the employee's motive for accessing a computer and his or her intended use of the information obtained. . . . this interpretation reads section (a)(4) as if it said ‘exceeds authorized use’ instead of ‘exceeds authorized access.’”). As the court in *Brett Senior* also held:

The CFAA defines “exceeds authorized access” as accessing “a computer with authorization” and using “such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.” *Id.* §1030(e)(6). By its plain terms, this definition does not apply to Fitzgerald’s conduct. He did not obtain any information that he was not entitled to obtain or alter any information that he was not entitled to alter. As Senior testified at his deposition, Fitzgerald was allowed full access to information contained in the BSA computer system until his departure.

**Note: the *Brett Senior* court stated that it was not construing the “without authorization” language that was at issue in *Citrin and Shurgard*, and thus, the court tried not to expressly distinguish the Seventh Circuit’s approach. Similarly, the court in *Shamrock Foods* noted that *Citrin* was legally and factually distinguishable, and involved a different section of the statute from that construed in *Shamrock Foods*. But the cases in this group are generally clear in rejecting the *Citrin* approach, which they deem to be an improper expansion of a criminal law.**

(iii) *Lockheed Martin Corp. v. Speed*, 2006 U.S. Dist. LEXIS 53108, at \*19 (M.D. Fla. Aug. 1, 2006) (“In this Court's view, the plain meaning brings clarity to the picture and illuminates the straightforward intention of Congress, *ie.*, ‘without authorization’ means no access authorization and ‘exceeds authorized access’ means to go beyond the access permitted. While *Citrin* attempts to stretch ‘without authorization’ to cover those *with* access authorization (albeit those with adverse interests), Congress did not so stipulate.”).

(iv) *Am. Family Mut. Ins. Co. v. Rickman*, 2008 U.S. Dist. LEXIS 32480, at \*13 (N.D. Ohio Apr. 18, 2008) (“The statute was not meant to cover the disloyal employee who walks off with confidential information. Rather the statutory purpose is to punish trespassers and hackers.” (*Dictum*)).

Many of the cases, on both sides of the issue, are well reasoned and contain numerous citations to additional authorities and legislative history.

Influence of Criminal Liability. Among the issues influencing the courts following the more restrictive view, is the rule of lenity that governs construction of criminal statutes, and the concept that this criminal statute must have a consistent meaning and not be subject to individual contractual agreements. *See, eg., Black & Decker, supra, citing Leocal v. Ashcroft*, 543 U.S. 1, 12 n.8 (2004); *Crandon v. United States*, 494 U.S. 152, 158 (1990). Indeed, the recent prosecution under the CFAA of Lori Drew, *U.S. v. Drew, No. 08-00582* (C.D.Cal. May 15, 2008), which premised Drew's unauthorized use of MySpace on a violation of the MySpace terms of service, is being cited as a dangerous expansion of federal criminal law, and an improper consequence of permitting the interpretation of the CFAA, to vary with alleged breaches of private contractual terms. The Electronic Frontier Foundation and the Cyberlaw Clinic at Harvard Law School submitted an *amicus* brief on this issue, [http://www.eff.org/files/filenode/US\\_v\\_Drew/Drew\\_Amicus.pdf](http://www.eff.org/files/filenode/US_v_Drew/Drew_Amicus.pdf), which analyzes the case law on the application of the CFAA in this area, and makes a very strong case for the restrictive approach.

Practice Suggestions. In those jurisdictions (the Seventh Circuit and others) where the courts have adopted the more expansive view of the CFAA's reach, an employer has a strong remedy and a federal forum to pursue a disloyal employee who has accessed the employer's computer system in connection with disloyal conduct. In jurisdictions taking a more restrictive approach, the CFAA will be available only if the employee has done something more than utilize his authorized level of access.

In either case, company policies and agreements which state, expressly, that the employee is not authorized to use either the company computers, or the company email, for personal matters, or for any use other than the company's business, may provide a basis to sustain a CFAA case. Although this is the type of liability rejected in some of the "restrictive" cases, and condemned by the critics of the *Drew* prosecution, at least one court has attempted to sidestep the debate by relying on such policies and agreements to deem the employee's conduct unauthorized. *See Hewlett-Packard Company v. Byd:Sign, Inc., et al.*, No. 6:05-CV-456 (E.D.Tex. Jan. 25, 2007) (*Slip Op.*) In *Hewlett-Packard*, the court found a complaint sufficient in alleging lack of authorization, or exceeding authorization, where the disloyal employee was alleged not only to have accessed the system, but to have sent emails for personal gain, and to have introduced scrubbing software, after having agreed to refrain from such conduct.

### **III. "Loss" and "Damage" under the CFAA**

- A. There is also a split of authority regarding whether the CFAA applies to cases involving the theft of information.
  1. If the information is deleted or erased, or otherwise made unavailable to the plaintiff, courts have an easier time applying the CFAA.
    - *B&B Microscopes v. Armogida*, 2007 WL 2814595 (W.D.Pa., September 25, 2007), held that Defendant's intentional deletion of

customer lists and other business information from his work laptop caused damage to that data since that data is no longer available to B&B and B&B cannot retrieve it.

2. If the information is not destroyed, but rather is copied, transmitted, and/or accessed e.g., for later competitive use, the courts disagree as to the application of the CFAA.

- *Garelli Wong & Associates, Inc. v. Nichols*, 2008 WL 161790 (N.D.Ill. January 16, 2008), held that Defendant’s copying of confidential and proprietary information (which Defendant later used for competitive purposes with his new employer) did not amount to damage under the CFAA because Plaintiff could not show “impairment to the integrity or availability” of the data.
  - The court noted that merely arguing in a conclusory manner that copying data constitutes damage under the CFAA is insufficient. However, one could interpret this holding to imply that Plaintiff’s argument could hold more water if Plaintiff could set forth facts to indicate that the copying of the trade secret somehow compromised the “integrity” of the data.
- *Therapeutic Research Faculty v NBTY, Inc.*, 2007 WL 214595 (E.D. Cal., January 25, 2007), held that unauthorized access to online subscription may constitute “impairment to the integrity” of the data even if “no data was physically changed or erased.”
- Some courts have said that the CFAA applies if the company had clear policies prohibiting the employee from the actions in question (see e.g., *Hewlett-Packard Co. v. BYD:Sign, Inc.*, 2007 WL 275476 (E.D. Teas., Jan. 25. 2007), where HP had a policy not to use computers/network for personal purposes and employee had used HP computers/network for personal, competitive purposes.

B. The statutory provisions that most commonly provide the ammunition for this battle are those regarding “loss” and “damage.” The “loss” and “damage” provisions of the CFAA can be somewhat confusing, however, and the case law applying them has become a muddle of contradictions and inconsistency.

1. “Loss” under the CFAA

- a. Statutory definition: §1030(e)(11) defines “loss” as: “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the

offense, and any revenue lost, cost incurred or other consequential damages incurred because of interruption of service.”

- b. When does the CFAA require a “loss”? The CFAA requires a loss for most civil claims. The loss must be to one or more persons during any one-year period aggregating at least \$5,000.00. For criminal cases, no loss is required. *Sidebar*: in a criminal case, of course, the elements must be proven beyond a reasonable doubt; in a civil case, the elements need to pass the preponderance of the evidence test.
- c. What types of losses have the courts deemed to be a “loss” under the statute?
  - Cost of investigating damage to computer system (*Nexans Wires S.S. v. Sark-USA, Inc.*, 319 F.Supp.2d 468 (S.D.N.Y. 2004)).
  - Cost of forensic investigation (e.g. to discover the identity of the offender or the method the offender used to improperly access information). *Successfactors, Inc. v. Softscape, Inc.*, 2008 WL 906420 (N.D.Cal., April 1, 2008).
  - Does NOT include cost of assisting government (e.g., employees traveling to meet with FBI) *U.S. v Shuster*, 2006 WL 3041074.
  - Does NOT include loss of exclusive use of data or information. Copying and unauthorized use of information does not constitute “loss” under the CFAA. (*Nexans Wires S.S. v. Sark-USA, Inc.*, 319 F.Supp.2d 468 (S.D.N.Y. 2004), *aff’d*, 166 Fed. Appx. 559, 2006 WL 328292, held that lost revenue as a result of competitor’s misappropriation of information in files does not constitute “loss” under the CFAA).

## 2. “Damage” under the CFAA

- a. Statutory definition: §1030(e)(8) means “any impairment to the integrity or availability of data, a program, a system, or information.”
- b. Which CFAA sections require “damage”?
  - §1030(a)(5)(A) states: “knowingly causes the transmission of a program, information, code, or command, and as a result of

such conduct, **intentionally causes damage** without authorization, to a protected computer.”

- §1030(a)(5)(B) states: “intentionally accesses a protected computer without authorization, and as a result of such conduct, **recklessly causes damage.**”
- §1030(a)(5)(C) states: “intentionally accesses a protected computer without authorization, and as a result of such conduct, **causes damage and loss.**”
- §1030(a)(7) deals with threats of damage.

c. What types of losses have the courts deemed to be “damage” under the statute?

- The information is deleted or erased, or otherwise made unavailable to the plaintiff (*B&B Microscopes v. Armogida*, 2007 WL 2814595 (W.D.Pa., September 25, 2007), held that Defendant’s intentional deletion of customer lists and other business information from his work laptop caused damage to that data since that data is no longer available to B&B and B&B cannot retrieve it.
- Copying and unauthorized use of information was deemed NOT to constitute or give rise to “damage” under the CFAA in *Garelli Wong & Associates, Inc. v. Nichols*, 2008 WL 161790 (N.D.Ill. January 16, 2008). (See discussion of this case, supra.)
- Copying and unauthorized use of the information was deemed to constitute “damage” under the CFAA in *Therapeutic Research Faculty v NBTY, Inc.*, 2007 WL 214595 (E.D. Cal., January 25, 2007, in which the court held that unauthorized access to online subscription may constitute “impairment to the integrity” of the data even if “no data was physically changed or erased.” Also, *HUB Group, Inc. v. Clancy*, No 05-2046, 2006 WL 208684 at \*3-\*4 (E.D. Pa., Jan. 25. 2006) held that unauthorized access to confidential information compromised the integrity of plaintiff’s computer database which was therefore “damaged” under the CFAA).

3. “Damage” vs. “Damages” under the CFAA

- a. The case law evidences some confusion about the concepts of “loss,” “damage,” and “damages.”

- *Cohen v. Gulfstean Training Academy, Inc.*, 2008 WL 961472 (S.D. Fla., April 9, 2008) – confuses “loss” with “damages.”
  - *Bansal v. Russ*, 2007 WL 1030941 (E.D.Pa., April 5, 2007) says that “losses” (as opposed to compensatory damages) are limited to economic damages. Court erroneously held plaintiff had not alleged that he suffered \$5000 in economic damages (as opposed to “losses”).
- b. One example of a court applying the terms correctly: *Frees, Inc. v. McMillian*, 2007 WL 2264457 (W.D.La. 2007), which held that “loss” is merely a jurisdictional threshold, leaving no limit on “compensatory damages,” other than limiting such damages to “economic damages.”

#### IV. Remedies & Penalties

##### A. Generally:

1. Both criminal penalties and civil remedies are available.
2. Apply to attempted offenses and to conspiracies to commit an offense. 18 U.S.C. § 1030(b).

##### B. Criminal Penalties

1. Generally speaking, the CFAA’s penalties include fines, imprisonment, and forfeiture. The statutory scheme setting forth the specific penalties is complex, and those penalties depend upon which section of the Act is violated, as well as whether the defendant is a repeat offender.
2. More specifically, the penalties and punishments under the CFAA are:

<b>Violation of CFAA Section:</b>	<b>First Offense:</b>	<b>Repeat Offense:</b>
(a)(1)	Fine and/or prison ≤ 10 yrs (c)(1)(A)	Fine and/or imprisonment ≤ 20 yrs (c)(1)(B)
(a)(2)	Fine and/or prison ≤ 1 year (if purpose was NOT commercial advantage, private	Fine and/or prison ≤ 10 yrs (c)(2)(C)

	<p>financial gain, or the furtherance of unlawful act) (c)(2)(A)</p> <p>Fine &amp; prison ≤ 5 years (if purpose WAS commercial advantage, private financial gain, or the furtherance of unlawful act) (c)(2)(B)</p>	
(a)(3)	Fine and/or prison ≤ 1 year (c)(2)(A)	Fine and/or prison ≤ 10 yrs (c)(2)(C)
(a)(4)	Fine and/or prison ≤ 5 yrs (c)(3)(A)	Fine and/or prison ≤ 10 yrs (c)(3)(B)
(a)(5)(A)	<p>Fine and/or prison of ≤ 1 yr (if none of the exacerbating factors is present) (c)(4)(G)</p> <p>Fine and/or prison ≤ 10 yrs (if one of the exacerbating factors is present) (c)(4)(B)</p> <p>Fine and/or prison ≤ 20 yrs (if offender attempts to cause or knowingly or recklessly causes serious bodily injury) (c)(4)(E)</p> <p>Fine and/or prison ≤ life (if offender attempts to cause or knowingly or recklessly causes death) (c)(4)(F)</p>	Fine and/or prison ≤ 20 yrs (c)(4)(C)
(a)(5)(B)	Fine and/or prison of ≤ 1 yr (if none of the exacerbating factors is present)	Fine and/or prison ≤ 20 yrs (c)(4)(C)

	(c)(4)(G)  Fine and/or prison ≤ 5 yrs (if one of the exacerbating factors is present) (c)(4)(A)	
(a)(5)(C)	Fine and/or prison ≤ 1 yr (c)(4)(G)	Fine and/or prison ≤ 10 yrs (a)(4)(D)
(a)(6)	Fine and/or prison ≤ 1 yr (c)(2)(A)	Fine and/or prison ≤ 10 yrs (c)(2)(C)
(a)(7)	Fine and/or prison ≤ 5 yrs (c)(3)(A)	Fine and/or prison ≤ 10 yrs (c)(3)(B)

3. Forfeiture provision §1030(i)(1) covering:
  - a. personal property that was “used or intended to be used to facilitate or commit a violation, and
  - b. personal or real property constituting or derived from proceeds of violation.

## B. Civil Remedies

1. CFAA allows for a civil action if one of following factors is present:

- “loss” ≥ \$5,000,
- Impact on medical care
- Physical injury
- Threat to public health / safety
- Damage affecting a government computer

“Loss” ≥ \$5,000 will be the most common basis for a civil claim.

2. Specific remedies available to civil plaintiffs under the CFAA:

- a. Compensatory damages

- i. Section 1030(g) -- If basis of civil claim is a loss  $\geq$  \$5,000, damages are limited to “economic loss.”
- ii. Economic damages includes a broad range of recoverable losses.

*Creative Computing v. GetLoaded.com LLC*, 386 F. 3d 930, 935 (9th Cir. 2004) (Kleinfeld, J.)

Damages for lost business and business goodwill are “economic damages.”

“When an individual or firm’s money or property are impaired in value, or money or property is lost, or money must be spent to restore or maintain some aspect of a business affected by a violation, those are ‘economic damages.’”

*Contract Associates Office Interiors, Inc. v. Ruiters*, 2008 WL 3286798 (E.D.Cal., August 6, 2008) (“any loss of business and business goodwill constitutes recoverable damages under the CFAA.”)

- iii. “Economic damages” does not include damages for death, personal injury, mental distress, and the like.
- iv. Beware case law confusing the concept of recoverable damages with – and limiting recoverable damages to – “loss” as defined by the CFAA. *See, e.g., Cohen v. Gulfstream Training Academy, Inc.*, 2008 WL 961472 (S.D. Fla., April 9, 2008); *Cenveo Corp. v. Celumsolutions Software GmbH & Co KG*, 2007 WL 951550 (D. Minn., Mar. 27, 2007).

b. Injunctions

- i. Some cases in which an injunction was granted:
  - (a) Injunction requiring the destruction of all computer files belonging to plaintiff (paper or electronic format) that the defendants still possess. *KEG Technologies, Inc. v. Laimer*, 2006 WL 1789012 (N.D. Ga., June 8, 2006)
  - (b) Injunction prohibiting the defendant from doing business with any of the customers whose information he deleted from his company-issued

laptop. *Hub International of California Insurance Services, Inc. v. Kilzer*, 2006 WL 2619360 (N.D. Cal., September 12, 2006)

ii. Case denying injunctive relief:

- (a) Court would **not** issue injunction requiring former employees to return any information that they deleted from employers' servers, barring them from using or disclosing employer's trade secrets and enjoining them from continuing to work for any direct competitor. *Maxpower Corp. v. Abraham*, 557 F. Supp. 2d 955 (W.D. Wis. 2008)

c. "Other equitable relief"

It is unclear what this provision will afford to civil plaintiffs. Most, if not all, of the case law addresses damages and injunctive relief. Presumably, we will see cases filed seeking other equitable remedies, such as an accounting and/or the imposition of a constructive trust.

- d. No punitive damages. *See, e.g., Garland-Sash v. Lewis*, 2007 WL 935013 (S.D.N.Y., Mar. 26, 2007)

## V. Miscellaneous Topics

### A. Federal Jurisdiction

1. A plaintiff will have federal subject matter jurisdiction for CFAA claims under 28 U.S.C. §1331
2. and "supplemental jurisdiction" over the complaint's other (state law) claims under 28 U.S.C. §1367(a), if those claims "are so related to [the CFAA claims . . . ] that they form part of the same case or controversy under Article III of the United States Constitution."
3. Generally, supplemental jurisdiction may be declined by the court if (a) the claim raises a novel or complex issue of State law, (b) the state law claims "predominate," or (c) the CFAA claim is dismissed. 28 U.S.C. §1367(c).
4. Generally, a district court will find substantial predominance where "it appears that a state claim constitutes the real body of a case, to which the

federal claim is only an appendage.” *United Mine Workers v. Gibbs*, 383 U.S. 715, 86 S. Ct. 1130, 16 L.Ed.2d 218 (1966).

5. Cases in which the federal court declined to exercise its jurisdiction:
  - a. *Contemporary Services Corp. v. Hartman*, 2008 WL 3049891 (C.D.Cal., Aug. 4, 2008) (state claims predominate and are remanded)
  - b. *H&R Block Tax Services, Inc. v. Rivera-Alicea*, 570 F.Supp.2d 255 (D.P.R., July 7, 2008) (claims dismissed under Colorado River abstention doctrine due to parallel state court proceeding and the state court’s interest in deciding important state law issues, such as non-compete questions)

## B. Vicarious Liability

1. There is no concept of pure “vicarious liability” under the CFAA by which an employer may be held liable for its agents conduct, simply by virtue of the agency relationship.

Cases in which claims against an employer were rejected:

*Calence, LLC v. Dimension Data Holdings*, 2007 WL 1549495 (W.D.Wash., May 24, 2007) (Martinez, J.) (summary judgment is granted to corporate defendants on CFAA claim, because “plaintiff points to no evidence in the record that corporate defendants directed either of those individuals to take any of the alleged improper actions.”)

*Role Models Am., Inc. v. Jones*, 305 F.Supp.2d 564 (D. Md. 2004) (rejecting CFAA claim where plaintiff did not allege that the employer had directed or encouraged its employee to violate the CFAA)

*Butera & Andrews v. International Business Machines Corp.*, 456 F. Supp. 2d 104, 2006 WL 2971107 (D.D.C., October 18, 2006) (Both IBM and one of its employees named as defendants in hacking case. No claim stated against IBM.)

2. However, claims against employers have been sustained where the employer directed or participated in the violation. *See, e.g., Binary Semantics, Ltd. v. Minitab, Inc.*, No. 4:07-cv-1750, 2008 U.S. Dist. LEXIS 28602, at \*14-15 (M.D.Fla. Mar. 20, 2008) (allegation that defendant directed plaintiff’s employee to e-mail proprietary information belonging to plaintiff properly alleges CFAA violation).

3. At least one case suggests that an employer may be liable if it knew about (or should have known about) a violation, did nothing to “disaffirm” it, and thereby “ratified” it. *See Contract Associates Office Interiors, Inc. v. Ruitter*, 2008 WL 2225702 (E.D.Cal., May 29, 2008) (“There is a genuine issue of material fact as to whether Ruitter was an agent of Workspace Solutions and whether Workspace Solutions was aware that its new sales representative--fresh from the employ of a competing company that had worked on similar E\*trade projects--had immediately arrived with considerable outside work product substantiating several lucrative E\*Trade projects. From this, a reasonable jury could readily infer that Workspace Solutions had acquired the requisite knowledge of Ruitter's illicit conduct, effectively triggering its duty to disaffirm her acts. Accordingly, because there is a genuine issue of material fact whether Workspace Solutions ratified Ruitter's alleged violation of the CFAA, the court will deny Workspace Solutions' motion for summary judgment with respect to Contract Associates' CFAA claim.”)