The Computer Fraud and Abuse Act

A Powerful Weapon vs. Unfair Competitors and Disgruntled Employees

By James M. Thomas

"Boss, Lee is gone, and you are not going to like what I have found out!"

An officer at the highest levels of your company has been lured to your top competitor. His laptop is clean as a whistle, and files from his desktop computer have been erased. You can find neither the non-compete/non-solicitation, nor the confidentiality agreements for him that you thought HR was going to have everyone sign years ago. Is your company still protected? Yes, by the Computer Fraud and Abuse Act.

"Boss, here are the quarterly sales figures, but you are not going to like what I found!"

You discover your company's sales in the last few months have plummeted, while a previously unknown competitor's sales to your now-former customers seem to have skyrocketed, with the new competitor seeming to undercut your prices again and again. One of your staff did mention they had heard a mid-level marketing person whom you had fired now works for that competitor, but that does not seem to explain how the competitor could undercut almost all your prices. Is there something out there with some punch that can protect your company? Yes, the Computer Fraud and Abuse Act.

The Birth of the CFAA

The innovative spark and drive that has brought a bountiful return to many in the course of the information and technological age in which we live has not been limited to those pioneering new approaches. Unfortunately, it has also filtered down to those who would, if left to their devices, secretly harvest the fruits of others' labors and creativity. In 1984, to combat what was described as a "growing wave of computer crime," Congress passed what was called "The Counterfeit Access Device and Computer Fraud and Abuse Act." *Pacific Aerospace & Electronics, Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1195 (E.D. Wash. 2003). The protections contained within this initial act were focused on criminal acts and were limited to "a relatively narrow class of government-operated computers," leaving the states and local authorities to deal with computer crime in their respective jurisdictions. *Id.* Under the terms of this Act, it was a felony "to knowingly access a computer without authorization in order to obtain classified defense information," and was a misdemeanor "to knowingly access a computer without authorization in order to obtain information in a financial record… or in a consumer file," if those acts detrimentally affected the government. Pub. L. No .98-473, 98 stat, 2190. As damage to companies increased due to the clandestine efforts of individuals outside those companies and disgruntled employees still inside, and states' and local government's efforts to combat those destructive actions lagged, Congress amended the Act in 1986, 1994, 1996, 2001 and again in 2002, to expand protections to computers and information systems in the private sector, adding civil remedies.

The Computer Fraud and Abuse Act (CFAA) now provides that "any person" damaged in the manner and to the extent Congress sets out, can "obtain compensatory damages and injunctive relief or other equitable relief." *See* the pertinent statutory language (18 U.S.C. §1030), next page.

■ James M. Thomas, a member in the Seattle office of Williams, Kastner & Gibbs, has 30 years of experience litigating cases in state and federal courts and is a frequent lecturer on employment law issues. Mr. Thomas has a broad litigation background in employment matters, deals with non-competition and unfair trade practices claims, Uniform Trade Secret Act and Computer Fraud and Abuse Act issues, and handles complex contract and construction disputes. He can be reached at JThomas@WilliamsKastner.com.

The question was: would anyone take an action by Congress to provide civil litigants safeguards against the invasion or corruption of computer information systems seriously if the mechanism to do so was attached as only a small subsection in a much larger criminal act? Believe it.

The Courts and the Breadth of CFAA

Who believed Congress actually intended to put some muscle behind one small subsection in that criminal act? The federal courts, for one, did.

In dealing with the civil remedy provided in the CFAA as described in 18 U.S.C. §1030(g), courts have both recognized the existence of federal question jurisdiction under the CFAA (*Miles v. America Online, Inc.*, 202 F.R.D. 297, 300 (N.D. Fla. 2001)), and recognized the exercise of that jurisdiction to be constitutional. *Peridyne Technology Solutions, LLC v. Matheson Fast Freight, Inc.*, 117 F. Supp. 2d 1366 (N.D. Ga. 2000). And, the exercise of that jurisdiction does not stop at the borders of the United States. In *United States v. Ivanov*, 175 F. Supp. 2d 367 (D. Conn. 2001), the defendant former employee argued the CFAA simply did not apply to him. In *Ivanov*, the defendant "hacked" into a Connecticut company's computer system and obtained the key passwords that controlled the company's entire computer network. The defendant then allegedly threatened the Connecticut company "with the destruction of its computer systems" unless it paid him approximately $10,000 "for his assistance in making those systems secure." *United States v. Ivanov*, *supra* at 369. With both the defendant

The Computer Fraud and Abuse Act (CFAA) 18 U.S.C. §1030

(a) Whoever—…
- (5) (A) (i) 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;
  - (ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
  - (iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and
- (B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—
  - (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 or 1 or more individuals;
  - (iii) physical injury to any person;
  - (iv) a threat to public health or safety; or
  - (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.
- (6) knowingly and with intent to defraud traffics (as defined in §1029) in any password or similar information through which a computer may be accessed without authorization, if—
  - (A) such trafficking affects interstate or foreign commerce…

(e) As used in this section—
- (1) the term "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 or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;
- (2) the term "protected computer" means a computer…
  - (B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States….
- (6) 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;…
- (8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;…
- (11) the term "loss" means 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; and
- (12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity….

(g) 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 clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within the 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.

and the government agreeing that "when Ivanov allegedly engaged in the conduct charged in the superseding indictment, he was physically present in Russia and using a computer there at all relevant times," the defendant argued the extraterritorial application of the CFAA was not permissible. Noting that "all of the intended and actual detrimental effects" that the defendant was charged with "occurred within the United States," and that the victim's computers "were located in Vernon, Connecticut," the court rejected the defendant's jurisdictional argument, and held:

> Congress has the power to apply its statutes extraterritorially, and in the case of 18 U.S.C. §1030, it has clearly manifested its intention to do so.

United States v. Ivanov, *supra* at 375.

How long that federal question claim stays alive, however, is still being debated. In *Ashcroft v. Randel*, 391 F. Supp. 2d 1214 (N.D. Ga. 2005), the court noted that the CFAA did contain "a statute of limitations provision," where it provided: "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." 18 U.S.C. §1030(g); *Ashcroft v. Randel*, *supra* at 1220. The court noted, however, that there was no specific designation as to when that two-year period began to run. With the parties before it agreeing that "the federal discovery rule" applied, and based on the facts before it, the court refrained from defining the precise parameters of that two-year period:

> But, because the Court concludes that Plaintiff's claim is barred under the more permissive federal discovery rule whereby the statute of limitations runs from the date that Plaintiff knew or should have known of both the injury and its cause, the Court need not decide this issue here.

Ashcroft v. Randel, *supra* at 1220. The court in *Egilman v. Keller & Heckman*, 401 F. Supp. 2d 105 (D.D.C. 2005), did not feel so constrained on that statute of limitations issue. In *Egilman*, the plaintiff "discovered the damage" the defendants allegedly caused "by, at the latest, June 22, 2001," but "did not become aware of the essential facts of his CFAA claim until November 20, 2002." *Egilman v. Keller & Heckman*, *supra* at 110. Agreeing with the defendant that the complaint ultimately filed in May 2004 missed the statute of limitations, the court held:

> Egilman states that he learned by November 2002 all additional facts necessary to file his claim. By that date, the statute of limitations period still had over seven months before it expired. Egilman failed to file his complaint within those seven months; rather, he waited a year and a half. Under these facts and D.C. Circuit precedent, the court concludes that equitable tolling is not merited and Egilman's CFAA is barred by the statute of limitations.

Egilman v. Keller & Heckman, *supra* at 111–12.

> Courts have accented the belief that "Congress has, therefore, continuously broadened the scope and coverage of the CFAA since its original enactment."

Given the federal question jurisdiction and a two-year life span of a claim, how broad have the federal courts viewed the operation of the CFAA? In *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2003), *cert. denied*, 543 U.S. 813, 125 S. Ct. 48 (2004), the defendants asserted the only "civil offenses" described by the CFAA were those contained in subsection (a)(5)(A)(i)–(iii). The Ninth Circuit rejected that assertion, noted that the alleged wrongful conduct "must involve one of the five factors" set out in 18 U.S.C. §1030(a)(5)(B), which specifically include an allegation of "a loss in excess of $5,000," and held:

> But subsection (g) applies to any violation of "this section" and, while the offense must involve one of the five factors in (a)(5)(B), it need not be one of the three offenses in (a)(5)(A).

Theofel v. Farey-Jones, *supra* at 1078.

Likewise, in *I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems*, 307 F. Supp. 2d 521 (S.D.N.Y. 2004), the defendant contended a claim under §1030(a)(2)(c) should be dismissed, asserting that "§1030(g) does not provide a civil action for violations of this subsection." The court rejected defendant's assertion, and held:

> The plain text of §1030(g) does not provide or imply, and defendant offers no supporting case law for, such a restriction. Section 1030(g) affords a civil action for any CFAA violation, but requires an allegation of one of the five enumerated factors in §1030(a)(5)(B).

I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc., *supra* at 526.

Similarly, in *Southwest Airlines Co. v. Farechase, Inc.*, 318 F. Supp. 2d 435 (N.D. Tex. 2004), the court refused to restrict the application of 18 U.S.C. §1030(g). In *Southwest*, the defendant posed a dual assertion, first claiming the corporate plaintiff had no CFAA claim due to its failure to specifically allege "the statutory definition of damage in §1030(n)(8)," and second, that it did not allege " conduct described in subsection (a)(5)(A), which requires an allegation of damage." Pointing to the fact that the plaintiff had alleged a "loss aggregating at least $5,000," the court rejected the defendant's assertion and held:

> The CFAA does not require a civil plaintiff to allege damage, as defined in §1030(e)(8), if the civil plaintiff alleges loss of at least $5,000 as defined in §1030(e)(11)…. A careful reading of the statutes shows that a civil plaintiff is not required to state a cause of action pursuant to subsection (a)(5), but merely to allege one of the factors enunciated in subsection (a)(5)(B).

Southwest Airlines Co. v. Farechase, Inc., *supra* at 439; *see also Fiber Systems International, Inc. v. Roehrs*, 470 F.3d 1150, 1156–57 (5th Cir. 2006) (Fifth Circuit rejects the defense assertion that violations of §1030(a)(4) could not be brought under §1030(g), holding "[s]ection 1030(g) extends the ability to bring a civil action to any person suffering damage or loss 'under this section,' which *refers to §1030 as a whole*. Indeed, if Congress intended to limit civil actions in this manner, it could

have simply provided that civil actions may only be brought for violations of subsection (a)(5)" (emphasis added)).

Moreover, courts have accented the belief that "Congress has, therefore, continuously broadened the scope and coverage of the CFAA since its original enactment," supporting the enlargement of avenues open to civil litigants attempting to enforce their rights under the CFAA, with one court stating:

> Companies frequently find themselves in litigation with former employees who depart to set up shop elsewhere in competition with their former employer. Such former employees may attempt to gain an edge for their new venture by making use of proprietary information, such as customer lists or trade secrets, obtained with ease of access from their former employer's computer database or workstations that are linked together in a network. While passwords and other electronic means can limit the unauthorized dissemination of some confidential information, an employee who has not yet announced his departure is still able to access confidential information and store it on a CD or floppy disk before he or she leaves. Computers also make it easy for employees to quickly transmit information out of the company via e-mail…. Employers, however, are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system.

Pacific Aerospace & Electronics, Inc. v. Taylor, 295 F. Supp. 2d 1188, 1197–96 (E.D. Wash. 2003).

The Courts and the Terms of CFAA

With the broad view of Congress's intent as a baseline, the examination of the application of the CFAA must start with a computer or computer system itself. Efforts to limit that application on that facet have been equally unsuccessful. In *United States v. Mitra*, 405 F.3d 492 (7th Cir. 2005), the court was faced with the allegation of a defendant that the trial court had applied the CFAA far too broadly. In *Mitra*, a student at the University of Wisconsin Graduate Business School was charged with developing and sending signals to the City of Madison's computer-based radio system for police, fire, ambulance and other emergency communications, along with the city's communication towers themselves. While the initial strategy used by the defendant was to block the city's computer-based radio system's use by having "no signal" messages appear, thereby disabling all communications, he subsequently changed tactics to keep the system open, appending "a sound, such as a woman's sexual moan," at the end of each communication. Focusing on the term "computer," the crux of the defendant's defense was to assert that "[a]ll he did was gum up a radio system," and that such actions "cannot be a federal crime… even if the radio system contains a computer." *United States v. Mitra*, *supra* at 493–95. The *Mitra* court rejected that argument. Noting first that it was the defendant's contention that the CFAA was never intended to cover one who

> did not invade a bank's system to steal financial information, or erase data on an ex-employer's system [citation omitted], or plaster a corporation's website with obscenities that drove away customers, or unleash a worm that slowed and crashed computers across the world, [citation omitted], or break into military computers to scramble a flight of interceptors to meet a nonexistent threat, or plant covert programs in computers so that they would send spam without the owner's knowledge,

and that the defendant insisted he had never affected "any radio system on the other side of a state line," the *Mitra* court then noted that there was "no constitutional obstacle to enforcing broad but clear statutes," and held:

> [T]he statute does not ask whether the person who caused the damage acted in interstate commerce; it protects computers (and computerized communication systems) used in such commerce, no matter how the harm is inflicted. Once the computer *is used in interstate commerce*, Congress has the power to protect it from a local hammer blow, or from a local data pocket that sends it haywire.

United States v. Mitra, *supra*, 495–96; *accord Shurgard Storage Centers, Inc. v. Safeguard Self-Storage, Inc.*, 119 F. Supp. 2d 1121, 1124 (W.D. Wash. 2000) ("a 'protected computer' means a computer 'which is used in interstate or foreign commerce or communication.' 18 U.S.C. §1030(e)(2)(B)").

As to who may bring a CFAA claim, courts have had no problem interpreting the CFAA broadly on this point as well. In *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2003), *cert. denied*, 543 U.S. 813, 125 S. Ct. 48 (2004), the court was faced with a trial court decision that the CFAA "does not apply to unauthorized access of a third-party computer." Focusing on Congress's use of the term "any," the Ninth Circuit reversed the trial court and held:

> The district court erred by reading an ownership or control requirement into the Act. The civil remedy extends to "*any person* who suffers damage or loss by reason of a violation of this section." 18 U.S.C. §1030(g) (emphasis in original). The word 'any' has an expansive meaning, that is, 'one or some indiscriminately of whatever kind.' [citation omitted] Nothing in the provision's language supports the district court's restriction. Individuals other than the computer's owner may be proximately harmed by unauthorized access, particularly if they have rights to data stored on it.

Theofel, *supra* at 1078.

As for access being "without authorization," the evidence need not be as blatant as the showing made by one plaintiff where a "computer systems room" door was "forcibly" opened by a group "including armed security guards" with the computer information being subsequently copied. *Four Seasons Hotels & Resorts B.V. v. Consorcio Barr*, 267 F. Supp. 2d 1268, 1279 (S. D. Fla. 2003). For even if authorization *could* have been legitimate, if that authorization is *exceeded*, the CFAA applies. In *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001), the court was faced with claims the CFAA applied to the new employer of the plaintiff's former "Vice President of Information Strategy." In *Explorica*, the former vice president believed his new company "could gain a substantial advantage" over his prior employer "by undercutting" the plaintiff's prices. Although the defendant would have been "authorized" had it proceeded to "manually" search through the plaintiff's brochures and printed materials, the defendants, instead, hired a consultant "to design a computer program called

a 'scraper' to glean all of the necessary information" from the plaintiff's website. That "scraper" designed by the consultant, and "focused solely" on the plaintiff's website, "sent more than 30,000 inquiries" to the plaintiff's website, obtaining two year's of prices, "downloaded 60,000 lines of data," and provided information to the defendants that allowed them to "systematically undercut" the plaintiff's prices. Without the "proprietary information about the structure of the website and the tour codes," the surreptitious gathering of pricing information and the subsequent undercutting of the plaintiff's prices could not have occurred. Rejecting the defendant's arguments that it could have gathered the information "manually," and that it had "authorization" to scan the plaintiff's website anyway, the court held "authorization" could be eliminated if exceeded and found the CFAA to be applicable, stating:

> Explorica's wholesale use of [plaintiff's] travel codes to facilitate gathering [plaintiff's] prices from its website reeks of use—and, indeed, abuse—of proprietary information that goes beyond any authorized use of [plaintiff's] website…. [W]hatever authorization Explorica had to navigate around [plaintiff's] site (even in a competitive vein), it exceeded that authorization by providing proprietary information and know-how to [the consultant] to create the scraper.

EF Cultural Travel BV v. Explorica, Inc., *supra* at 582–83.

Likewise, "authorization" can be lost. In *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), the court had to determine whether and under what circumstances the "authorization" of an employee to gather information could be lost. In *Citrin*, the plaintiff hired the defendant to "identify properties" the plaintiff might want to acquire, and provided the defendant "a laptop to use to record data he collected in the course of his work." At some point, however, the defendant decided to quit and go into business for himself. Prior to leaving the employer, however, and prior to returning the laptop, the defendant "loaded into the laptop a secure-erasure program, designed, by writing over the deleted files, to prevent their recovery." In so doing, the defendant not only deleted the information he had gathered for his employer, but deleted any record of any wrongdoing, if there was any on that laptop. The Seventh Circuit distinguished *Citrin* from a "without authorization" case or an "exceeding authorized access" case and held:

> Our case is different. Citrin's breach of his duty of loyalty terminated his agency relationship (more precisely, terminated any rights he might have claimed as [plaintiff]'s agent—he could not by unilaterally terminating any duties he owed his principal gain an advantage!) and with it his authority to access the laptop, because the only basis of his authority had been that relationship. "Violating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship."

International Airport Centers, LLC. v. Citrin, *supra* at 420–21; *see also Theofel v. Farey-Jones*, 341 F.3d 978, 981, 983–84 (9th Cir. 2003), *cert. denied*, 543 U.S. 813, 125 S. Ct. 48 (2004) (Ninth Circuit rejects the defense assertion of authorization as a result of a subpoena that had been issued, on the ground the subpoena "was massively overbroad," and "patently unlawful," transforming "a bona fide state-sanctioned inspection into private snooping," and that, as such, the subpoena, being "a piece of paper masquerading as legal process," could not and did not "authorize" access to the information obtained by the defendant); *accord United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991) (access gained by guessing another person's password is not "authorization" under the CFAA); *I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc.*, 307 F. Supp. 2d 521, 523–25 (S.D.N.Y. 2004) (court rejects defense assertion its access to the plaintiff's information through a third party's identification and password, after it induced the third party to provide that information in breach of its agreement with the plaintiff, was "authorization" under the CFAA, as the information, instead, was "for the exclusive use of its customers, and not for competitor appropriation."); *but see International Ass'n of Machinists & Aerospace Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 496–99 (D. Md. 2005) (the defendant, while serving in her capacity as an officer of the plaintiff, allegedly accessed confidential union membership lists to assist in contacting those same members so as to form a new union, and to "subsequently challenge [plaintiff's] representation" of those members. In dismissing the plaintiff's CFAA claim, the *Werner-Matsuda* trial court pointed to the fact that when defendant accessed the confidential membership list she was an officer of the plaintiff and had full authority to access that list (even though she had signed an agreement stating she would not use the information "for any purpose contrary" to the plaintiff's "policies and procedures"), and held that the CFAA did not "prohibit the unauthorized disclosure or use of information, but rather unauthorized access;"). In *Secureinfo Corporation v. Telos Corporation*, 387 F. Supp. 2d 593, 599–600, 608–10 (E.D. Va. 2005), the court noted that, as the plaintiff had sued defendants, but not the defendants' consultant who had violated his licensing agreement with the plaintiff by providing the defendants access to the plaintiff's confidential information, the plaintiff's CFAA claim would be dismissed, and held:

> The Court grants the defendants' motion to dismiss the CFAA claim because Plaintiff fails to allege that the CFAA defendants had "unauthorized access"… Plaintiff makes clear throughout its Amended Complaint, that [the defendants' consultant] gave various defendants permission or authorization to use [plaintiff's server] and to view what was contained therein…. consequently, the CFAA defendants were "entitled to obtain" information on the server because [defendants' consultant] explicitly allowed them access to it…

The Ninth Circuit in one recent matter refused to accept that the impersonation of an entity that had "authorization" would avoid a CFAA violation.

> In essence, the plaintiff is asking the Court to hold that every breach of a computer software license agreement allows the licensing party to recover damages against a non-party to the software license under the CFAA, even though it cites no cases that so hold. The Court declines to read the statute as broadly as suggested by the plaintiff.

Bending the CFAA back to a more claim-enforcement approach, the Ninth Circuit in one recent matter refused to accept that the impersonation of an entity that had "authorization" would avoid a CFAA violation, with a California district court in another matter fully endorsing the Seventh Circuit's termination of authority approach. In *Creative Computing v. Getloaded.com, LLC*, 386 F.3d 930 (9th Cir. 2004), the court was faced with an argument by the defendants that "impersonating" a legitimate subscriber to the plaintiff's services and/or "registering a defunct company" as a current subscriber of the plaintiff's services could fall within the "authorization" guidelines of CFAA. The Ninth Circuit rejected the defense assertion and applied the CFAA.

Dealing next with the "I had authority, so there is no CFAA violation" assertion, a California federal district court had to decide whether a company was left unprotected from the acts of a soon-to-be-fired employee. In *ViChip Corporation v. Lee*, 438 F. Supp. 2d 1087 (N.D. Cal. 2006), the plaintiff, ViChip, presented uncontroverted testimony, most through the defendant, Lee, himself, showing:

- the defendant, Lee, was its former CEO, president, secretary, CFO, and sole director;
- Lee signed an "Employee Invention Agreement," a consulting agreement, and a patent assignment form, where he assigned all rights to all inventions to ViChip, and agreed to keep confidential and return to ViChip "all proprietary information… in the event of termination";
- Lee had used ViChip funds to attend a trade show on behalf of another company that he served as president;
- Lee planned to split the previously submitted patent application (that he had assigned to ViChip, so that he could be the "sole" inventor;
- Lee, just prior to being fired, removed from ViChip's offices, and "tore up" all of his signed agreements with ViChip, including the patent assignment form, and
- Lee, just prior to being fired, accessed ViChip's file server, and deleted files he generated as an employee, and deleted the contents of his ViChip issued laptop computer.

Defending against ViChip's claim he had violated the CFAA, Lee asserted the "without authorization" element of the act had not been proven, since he deleted the files from the company's server and his company lap top "while still an officer and director of ViChip." Wholeheartedly endorsing the Seventh Circuit's stand against such a betrayal in its 2006 *Citrin* decision, the *ViChip* court rejected Lee's assertion his soon-to-be terminated position with the company immunized him from his pre-departure destructive, damaging acts, and granted summary judgment to ViChip on the CFAA violation claim, holding:

> It cannot be disputed that Lee, as both employee and officer, had a duty of loyalty that he owed ViChip, and therefore an agency relationship. [citation omitted] Accordingly, when Lee decided—the night before his termination and *after* knowing that he was being asked to step down and give up his duties at ViChip—to delete all information from ViChip's server and his ViChip-issued computer, he similarly breached his duty of loyalty and terminated his agency relationship to the company. [citation omitted] In so doing, and as the *Citrin* court held, he also terminated his authorization to access files.

ViChip Corporation v. Lee, *supra* at 1091–92, 1100.

At the same time, merely connecting to a plaintiff's server, with no evidence of any files having been copied or information gathered (*Pearl Investments, LLC v. Standard I/O Inc.*, 257 F. Supp. 2d 326 (D. Me. 2003)), or merely receiving an email with no evidence the email contained trade secrets or proprietary information (*Role Models America, Inc. v. Jones*, 305 F. Supp. 2d 564 (D. Md. 2004), will not be sufficient to prove the unauthorized person was "accessing" information so as to fit within the requirements for a CFAA violation. Focusing on that same evidentiary bar a CFAA plaintiff must reach, the Third Circuit in *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504 (3d Cir. 2005), was faced with a claim that the plaintiff's former employee had "accessed [plaintiff's] computer system from his home 125 times" in a seven day period over 60 days after he left his employment with the plaintiff. In finding the requisite level of evidence of a CFAA violation had not been met, the Third Circuit held:

> It is clear that [plaintiffs] do not know, have not shown, and cannot show, what information, if any, was taken. Mr. Nasun, [plaintiff's president] stated repeatedly in his deposition that plaintiffs do not know what, if anything, was actually taken, much less information that could be deemed to be a trade secret, and this is uncontroverted….
>
> Under the CFAA, too, more is required….
>
> The [plaintiffs] urge that we draw inferences of intent and the obtaining of valuable information from the mere fact that unauthorized access has been shown, and ask defendants to rebut these inferences by demonstrating the innocence of their purpose or actions. However, the elements of the claims asserted are part of *plaintiff's* [emphasis in original] burden. That information was taken does not flow logically from mere access. Access could be accidental, and, even if access were purposeful and unauthorized, information could be viewed but not used or taken. Furthermore, without a showing of some taking, or use, of information, it is difficult to prove intent to defraud, and indeed, [plaintiffs] have not shown that they can do so….
>
> …The record contains the numerous e-mails sent by [the former employee defendant] over the relevant time period pertaining to his plans and steps he was taking with [the co-defendant] to start Celebrations, none of which contains any reference to any outside information. Nor do [plaintiffs] point to any conduct by [defendants] that might imply use of any type of information gained from [plaintiff's computer system]… This does not satisfy the proof necessary…

P.C. Yonkers Inc. v. Celebrations the Party and Seasonal Superstore, LLC, *supra* at 509–10.

But what of the term "transmission"? The courts have also given a broad definition to that term contained within the CFAA. In *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), the defendant, who had inserted "a secure-erasure program" into his employer's laptop causing the erasing of files, claimed that act was "not a 'transmission'" under the terms of the CFAA, thereby excusing his actions. The Seventh Circuit disagreed. In finding a "transmission" had occurred and that the CFAA applied, the Seventh Circuit held:

> W]e don't see what difference the precise mode of transmission can make. In either the Internet download or the disk insertion, a program intended to cause damage… is transmitted to the computer electronically. The only difference, so far as the mechanics of transmission are concerned, is that the disk is inserted manually before the program on it is transmitted electronically to the computer. The difference vanishes if the disk drive into which the disk is inserted is an external drive, connected to the computer by a wire, just as the computer is connected to the Internet by a telephone cable or a broadband cable or wirelessly…. Congress was concerned with both types of attack: attacks by virus and worm writers, on the one hand, which come mainly from the outside, and attacks by disgruntled programmers who decide to trash the employer's data system on the way out (or threaten to do so in order to extort payments), on the other. If the statute is to reach the disgruntled programmer… it can't make any difference that the destructive programs comes on a physical medium, such as a floppy disk or CD.

International Airport Centers, LLC v. Citron, *supra* at 419–20; *see also Four Seasons Hotels and Resorts B.V. v. Consorcio Barr*, 267 F. Supp. 2d 1268, 1322–23 (S.D. Fla. 2003) ("Spoofing," which is "analogous to forgery," of addresses of entities with legitimate access to the computer system, "constitutes the unlawful, intentional transmission of a program, code or command that causes damage," bringing it within the CFAA).

Once allegations are made, or the evidence shows a "protected computer" or the information contained therein tied to "any person" has been accessed without authorization, or a transmission was made affecting that "protected computer," what must the "damage" or "loss" be before the CFAA applies? The answer lies within 18 U.S.C. 1030(g).

One of the most contested facets of the CFAA, if not *the* most contested, is "damage" under the statute. Pursuant to 18 U.S.C. 1030(g), Congress provided that a person suffering "damage or loss" and bringing a CFAA claim could seek "compensatory damages and injunctive relief or other equitable relief," so long as any non-personal injury "compensatory damages" are "limited to economic damages." Once again, courts have provided a broad avenue to relief for CFAA claimants on this issue.

In *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001), the court emphasized the breadth of recovery that it perceived Congress intended:

> Congress's use of the disjunctive, "damage or loss," confirms that it anticipated recovery in cases involving other than purely physical damage…. To parse the words in any other way would not only impair Congress's intended scope of the Act, but would also serve to reward sophisticated intruders. As we move into an increasingly electronic world, the instances of physical damage will likely be fewer while the value to the victim of what has been stolen and the victim's costs in shoring up its security features undoubtedly will loom ever-larger.

EF Cultural Travel BV v. Explorica, Inc., *supra* at 584–85; *accord Pacific Aerospace & Electronics, Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1196–97 (E.D. Wash. 2003) (court acknowledges CFAA covers "more than the losses directly caused by the unauthorized accessing of a computer system, such as actual physical damage to a computer hard drive holding a company's proprietary information").

Nevertheless, a CFAA claimant must allege and be able to prove the "$5,000" damage floor to be successful. Failure to allege, and ultimately successfully prove, monetary damage in that minimal amount will be fatal. In *Pearl Investments, LLC v. Standard I/O, Inc.*, 257 F. Supp. 2d 326 (D. Me. 2003), one or more of the defendants had connected to the plaintiff's server. The plaintiff, however, had "not authorized the connection of any additional servers" to its network, and alleged its entire system "is extremely dependent upon operating on maximum speed and efficiency," which the connections of additional servers could detrimentally affect. Nevertheless, when faced with a dispositive motion, the plaintiff's expert had to concede that no evidence was found that any files had been copied from the plaintiff's system onto the defendants' hard drive. Rejecting the plaintiff's bald assertion that the defendants' "wrongful connection" to its computer system had "adversely affected the system's speed and operation, thereby causing damages," the court held:

> However, while Pearl adduces evidence that speed was important to the operation of its ATS, it sets forth no cognizable evidence that the Defendants' alleged conduct damaged its system in any quantifiable amount, let alone in an amount approximately more than $5,000 in one year. This is fatal to its CFAA cause of action.

Pearl Investments, LLC v. Standard I/O, Inc., *supra* at 349. *See also Role Models America, Inc. v. Jones*, 305 F. Supp. 2d. 564 (D. Md. 2004), where the plaintiff alleged its former academy principal violated the CFAA when he included information concerning the plaintiff in his dissertation submitted to complete his doctoral program offered by the co-defendant university. With no indication the co-defendant university had done anything more than permit the plaintiff's former academy principal to complete his dissertation, and no evidence that the co-defendant university had damaged the plaintiff by receiving anything of value from the plaintiff's former academy principal other than email and the completed dissertation, the court held there was insufficient evidence to support a CFAA claim, even though the dissertation contained "information" about the plaintiff, and held:

> It would be a different case if Dr. Jones had acted as NSU's agent in accessing information on [plaintiff's] computers. For example, if NSU had told Dr. Jones to send "emails to the defendant containing various trade secrets and proprietary information belonging to the plaintiff"… then the fact that the information was transferred first to Dr. Jone's computer might not insulate NSU from

> liability.... There is no claim that NSU directed or even encouraged Dr. Jones to access [plaintiff's] computers, nor any factual allegations supporting an agency relationship.

Role Models America, Inc. v. Jones, *supra* at 566–68; *see also Davies v. Afilias Limited*, 293 F. Supp.2d 1265, 1273 (M.D. Fla. 2003) (the plaintiff utilized authorization codes provided by the World Intellectual Property Organization to register domain names, and challenged a number of domain names for not owning the trademarks for those names, even though it did not own the trademarks to those names either. Pointing to the fact there was "no evidence that Plaintiff directly accessed Defendant's computer system," and noting that all the plaintiff did with the authorization codes it received was register domain names, the trial court ruled the fact some domain names were unavailable to the defendant, was just not the sort of "impairment... contemplated by the CFAA.").

Likewise, in *Expert Business Systems, LLC v. BI4CE, Inc.*, 411 F. Supp. 2d. 601 (D. Md. 2006), the plaintiff sought relief under the CFAA, claiming the defendants had "intercepted" two emails that had been sent to the plaintiffs, then allegedly sent a "Trojan Horse" to one of the plaintiff's computers "in order to destroy the evidence of defendants' unauthorized access." Noting the "utter lack of any expert opinion evidence to support damage to the plaintiff's computer 'through the delivery of a Trojan Horse,'" the court proceeded to dismiss the remaining CFAA claims, holding:

> I am constrained to agree with defendants that the utter lack of any substantial probative evidence that defendants wrongfully "intercepted" the disputed emails fatally undercuts plaintiffs' interception claim.

Expert Business Systems, LLC v. B14CE, Inc., *supra* at 604–06.

But what must the evidence show with regard to that $5,000 floor? Must each intrusion be shown to have damaged a CFAA claimant in the amount of $5,000? The Ninth Circuit soundly answered no.

In *Creative Computing v. Getloaded.com, LLC*, 386 F.3d. 930 (9th Cir. 2004), the court was faced with facts showing Getloaded had impersonated one company to get into the plaintiff's computer system, registered "a defunct company" as a subscriber to the plaintiff's website to gain additional access, then also hired away one of the plaintiff's employees who then proceeded to feed "confidential information to Getloaded" even before he left the plaintiff's company to go to Getloaded. Asserting that the CFAA required "a $5,000 floor for damages from each unauthorized access," the defendant asserted the court should dismiss the plaintiff's CFAA claim on the ground that it failed to produce any evidence to show "that the floor was reached on any single unauthorized access." Rejecting that assertion, and upholding the CFAA jury verdict against the defendants, the Ninth Circuit held:

> [T]he $5,000 floor applies to how much damages or loss there is to the victim over a one-year period, not from a particular intrusion. Getloaded argues that "impairment" is singular, so the floor has to be met by a single intrusion. The premise does not lead to the conclusion. The statute (both the earlier and the current versions) says "damage" means "any impairment to the integrity or availability of data [etc.]... that causes loss aggregating at least $5,000." Multiple intrusions can cause a single impairment, and multiple corruptions of data can be described as a single "impairment" to the data. The statute does not say that an "impairment" has to result from a single intrusion, or has to be a single corrupted byte.... The damage floor in the Computer Fraud and Abuse Act contains no "single act" requirement.

Creative Computing v. Getloaded.com, LLC, *supra* at 933–35.

> One of the most contested facets of the CFAA, if not *the* most contested, is "damage" under the statute.

Nor will the lack of sophistication on the part of the victim or the availability of a "patch" to prevent intrusion break the causal chain between the intrusion and the $5,000 floor requirement. The Ninth Circuit disposed of such a claim in *Creative Computing v. Getloaded.com, LLC*, 386 F.3d 930 (9th Cir. 2004). Arguing that "Microsoft had distributed a patch to prevent a hack" before the defendant's officers had hacked into the plaintiff's system, the defendant asserted the plaintiff has caused its own damage by not being more attentive and installing that patch. The argument was to no avail. The Ninth Circuit rejected that argument and held:

> Both the old version of the statute and the new one require that the impairment "causes" a $5,000 aggregate loss in a year. Damages are indeed limited to those caused by the impairment, which may not be the same thing as the expenses of the victim subsequent to the impairment.... Getloaded's argument that [plaintiff] could have prevented some of the harm by installing the patch is analogous to a thief arguing that 'I would not have been able to steal your television if you had installed deadbolts instead of that silly lock I could open with a credit card." A causal chain from the thief to the victim is not broken by a vulnerability that the victim negligently leaves open to the thief.

Creative Computing v. Getloaded.com, LLC, *supra* at 935.

Although the "at least $5,000" damage floor in 18 U.S.C. §1030(a)(5)(B)(i) was "limited to economic damages" (18 U.S.C. §1030(g)) by Congress, the courts have pushed out the definition of that "economic" boundary. In examining this statutory term, the Ninth Circuit in *Creative Computing v. Getloaded.com, LLC*, 386 F.3d 930 (9th Cir. 2004) held:

> The statutory restriction, "limited to economic damages," precludes damages for death, personal injury, mental distress and the like. 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."

Creative Computing v. Getloaded.com, LLC, *supra* at 935.

Accordingly, courts have expanded that definitional boundary of "economic damages" to include detrimental effects on a

computer system, expenses incurred, together with damage to tangible and intangible property. In so doing, it has been held that (1) an unauthorized intrusion that "caused congestion" on a plaintiff's computer system or an intrusion that resulted in "impairing the availability of that computer to other systems in the network," (*Four Seasons Hotels and Resorts B.V. v. Consorcio Barr*, 267 F. Supp. 2d 1268, 1322–23 (S.D. Fla. 2003)), (2) "diagnostic measures" utilized to inspect or protect a computer system (*EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 584 (1st Cir. 2001)), (3) efforts to "devote resources to resecuring the system" (*Shurgard Storage Centers, Inc. v. Safegard Self Storage, Inc.*, 119 F. Supp. 2d. 1121, 1126 (W.D. Wash. 2000)), (4) costs to make a system "more 'hacker proof'" (*Pacific Aerospace & Electronics, Inc. v. Taylor*, 295 F. Supp. 2d. 1188, 1197 (E.D. Wash. 2003)), (5) "any impairment to the integrity or availability of data," (*Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 934 (9th Cir. 2004)), together with (6) costs incurred in "damage assessment and remedial measures," (*I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc.*, 307 F. Supp. 2d. 521, 525–26 (S.D.N.Y. 2004)), are all well within the damage definition and requirements of the CFAA. *But see Wilson v. Moreau*, 440 F. Supp.2d 81, 109–10 (D.R.I. 2006) ("litigation expenses… are not economic damages" under the CFAA and do not meet the §1030(a)(5)(B)(i) jurisdictional floor of $5,000).

Raising an objection that before the CFAA applies there must be some damage to something tangible rather than intangible will not carry the day, as it has already been held that any time "something of value" has been taken, the CFAA has been met even if all that was affected was "data," for it has also been held that "data is intangible property." *United States v. Ivanov*, 175 F. Supp. 2d 367, 371 (D. Conn. 2001); *see also Carpenter v. United States*, 484 U.S. 19, 25, 108 S. Ct. 316 (1987) (noting that the "intangible nature [of confidential business information] does not make it any less 'property' protected").

In line with those determinations, "lost profits" together with "loss of business and business goodwill" have been determined to fit the CFAA "economic damages" definition. *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir. 2004). *But see Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 475–78 (S.D. N.Y. 2004) where the trial court held neither "loss of business or goodwill," nor "lost revenue due to lost business opportunity," nor "revenue lost because the information was used by the defendant to unfairly compete after extraction," were damages of "the type of 'loss' contemplated by the statute."

> "Lost profits" together with "loss of business and business goodwill" have been determined to fit the CFAA "economic damages" definition.

Indeed, with the determination that "customer information has previously been held to constitute a property interest sufficient to satisfy the damage requirement of the CFAA" (*Four Seasons Hotels and Resorts B.V. v. Consorcio Barr*, 267 F. Supp. 2d 1268, 1324 (S.D. Fla. 2003)), one must question whether a court faced with a substantial amount of customer information or data on customers being taken, yet without any expert testimony, might hold that the "loss" of that information, itself, may satisfy the "$5,000" damage limit.

Thrust into the middle of a technological revolution, where it is doubtful a single one of the federal judges dealing with these issues would have had a computer in any of their classrooms when *they* were in high school, the foresight and flexibility of the courts faced with problems and claims of damage, unimaginable 40 years ago, is laudatory indeed. The message to the public, to businesses, to those bent on competing unfairly, and to disgruntled present or former employees is that these courts are ready, willing and able to expand the parameters of protection afforded by the broad terms within the CFAA, even as the medium of information technology itself evolves. As the First Circuit stated in *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 585 (1st Cir. 2001), "If we were to restrict the statute as appellants urge, we would flout Congress's intent by effectively permitting the CFAA to languish in the twentieth century, as violators of the Act move into the twenty-first century and beyond."

Conclusion

So, if someone from *inside* your company, or from *outside* your company:

1) intentionally accesses
2) an interstate computer/computer system you protect within the last two years,
3) either without authorization, or by far exceeding any actual authorization, and
4) as a result of that unauthorized access
5) that person or entity has intentionally, recklessly or otherwise caused
6) economic damage of over $5,000 to your company during any one-year period
   - — by impairing the value of your company's property
   - — by the loss of your company's money or property
   - — by the loss of your company's customer information or data on customers
   - — by requiring your company to expend funds
     - — to initiate diagnostic measures
     - — to restore, protect or maintain some aspect or asset of your company, or
     - — to conduct damage assessment or any remedial measures, or
     - — through lost profits, the loss of business and/or the loss of company goodwill,

the CFAA is there to protect you.

As a result, are those who aim either to strike out at former employers, or who feel they can come up with a parasitic mechanism, not thought of yet, to sap the creative attributes of a competitor's processes or business plans contained in computer information systems surreptitiously (yet unprotected against this new threat), to believe the broad protections in a congressional act, first passed as long ago as 1984, will really be enforced against them? Count on it.