

# **Computer Fraud and Abuse Act:**

## **Current Developments**

by

Robert B. Fitzpatrick, Esq.  
Robert B. Fitzpatrick, PLLC  
Universal Building South  
1825 Connecticut Ave., N.W.  
Suite 640

Washington, D.C. 20009-5728  
(202) 588-5300  
(202) 588-5023 (fax)

[fitzpatrick.law@verizon.net](mailto:fitzpatrick.law@verizon.net)

<http://www.robertbfitzpatrick.com> (website)

<http://robertbfitzpatrick.blogspot.com> (blog)

## **DISCLAIMER OF ALL LIABILITY AND RESPONSIBILITY**

THE INFORMATION CONTAINED HEREIN IS BASED UPON SOURCES BELIEVED TO BE ACCURATE AND RELIABLE – INCLUDING SECONDARY SOURCES. DILIGENT EFFORT WAS MADE TO ENSURE THE ACCURACY OF THESE MATERIALS, BUT THE AUTHOR ASSUMES NO RESPONSIBILITY FOR ANY READER’S RELIANCE ON THEM AND ENCOURAGES READERS TO VERIFY ALL ITEMS BY REVIEWING PRIMARY SOURCES WHERE APPROPRIATE AND BY USING TRADITIONAL LEGAL RESEARCH TECHNIQUES TO ENSURE THAT THE INFORMATION HAS NOT BEEN AFFECTED OR CHANGED BY RECENT DEVELOPMENTS.

THIS PAPER IS PRESENTED AS AN INFORMATIONAL SOURCE ONLY. IT IS INTENDED TO ASSIST READERS AS A LEARNING AID; IT DOES NOT CONSTITUTE LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL ADVICE. IT IS NOT WRITTEN (NOR IS IT INTENDED TO BE USED) FOR PURPOSES OF ASSISTING CLIENTS, NOR TO PROMOTE, MARKET, OR RECOMMEND ANY TRANSACTION OR MATTER ADDRESSED; AND, GIVEN THE PURPOSE OF THE PAPER, IT MAY OMIT DISCUSSION OF EXCEPTIONS, QUALIFICATIONS, OR OTHER RELEVANT INFORMATION THAT MAY AFFECT ITS UTILITY IN ANY LEGAL SITUATION. THIS PAPER DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP BETWEEN THE AUTHOR AND ANY READER. DUE TO THE RAPIDLY CHANGING NATURE OF THE LAW, INFORMATION CONTAINED IN THIS PAPER MAY BECOME OUTDATED. IN NO EVENT WILL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, OR OTHER DAMAGES RESULTING FROM AND/OR RELATED TO THE USE OF THIS MATERIAL.

# **COMPUTER FRAUD AND ABUSE ACT:**

## **Current Developments**

by Robert B. Fitzpatrick, Esq.\*

### **I. Introduction**

Originally designed as a criminal statute aimed at deterring and punishing hackers, particularly those who attack computers used for compelling federal interests (e.g., computers used by the federal government, large financial institutions, etc.), the Computer Fraud and Abuse Act (CFAA), “has been expanded through various amendments since its enactment in 1984.” *Int’l Airport Centers L.L.C. v. Citrin*, 2005 U.S. Dist. LEXIS 3905 (N.D. Ill. 2005), *rev’d on other grounds*, 2006 U.S. App. LEXIS 5772 (7<sup>th</sup> Cir. 2006). For example, in 1994 the Act began to allow for civil liability for certain types of violations. As amended in September 2008, the Act establishes civil liability for anyone who, among other things, “intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage...” involving “loss to 1 or more persons during any 1-year period... aggregating at least \$5,000 in value.” 18 U.S.C. § 1030(g) (incorporating 18 U.S.C. § 1030 (a)(5)(B) & (c)(4)(A)(i)(I)).

In recent years, employers have increasingly been using the CFAA to sue employees and former employees who make wrongful use of the employer’s computer systems or electronic devices, such as retaining, wrongfully accessing, or copying the employer’s computer systems or electronic documents without proper authorization. Such use of the CFAA in the employment context has been made possible in part by the broad definition of “protected computer” under the Act, which explicitly includes any computer “which is used in or affecting 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...” 18 U.S.C. § 1030(e)(2)(B). At the time this language was originally adopted, relatively few computers fit within this statutory definition of “protected computer”, as internet connectivity was much more primitive and less commonly used than it is today. But, given the current state of technology and the courts’ expansive definition of “interstate or foreign commerce”, it is hard to conceive of an internet-connected employer-owned computer or other device which could not arguably be considered a “protected computer”.

However, as the CFAA is primarily a criminal statute, courts have held that its language should be narrowly construed in the context of civil liability. *See, e.g., Int’l Ass’n of Machinists & Aero. Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 499 (D. Md. 2005). Thus, understanding the language of the Act and its construction by courts is of paramount importance for any party contemplating bringing a civil suit under the Act.

---

\*This article was prepared with assistance by Ryan P. Chapline, an associate with Robert B. Fitzpatrick, PLLC. Mr. Chapline is a May 2009 graduate of George Mason University School of Law and a member of the Maryland State Bar.

## II. Scope of Employee Authorization to Access Employer's Computerized Information

Since civil liability under the CFAA hinges in part upon whether the defendant accessed the protected computer in question with or without “authorization”, the scope of an employee’s or a former employee’s authorization to access his current or former work computer is often a topic of contention in employment cases brought under the Act. According to the Act, “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...” 18 U.S.C. § 1030(e)(6). Along those lines, a circuit split has recently developed on the topic of whether the Act should be interpreted broadly or narrowly when an employer claims that an employee or former employee has acted “without authorization” or has “exceeded authorization” in accessing the employer’s computer-stored information.

The narrower and more employee-friendly view, which has garnered significant support, is illustrated by the 9th Circuit’s holding in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), where the Court rejected the employer’s argument that an employee accesses electronic documents without “authorization” when the employee acts contrary to the employer’s interest or in breach of the employee’s fiduciary obligation of loyalty to the employer. Rather, where the employee’s actions are consistent with the access previously granted to him as an employee, the Court held that the employee acts with proper “authorization” within the meaning of the Act, regardless of whether the employee breached his or her duty of loyalty to the employer. For other decisions adopting this view, see, e.g., *Clarity Servs. v. Barney*, 2010 U.S. Dist. LEXIS 32519 (M.D. Fla. 2010); *Bell Aero. Servs. v. U.S. Aero Servs.*, 2010 U.S. Dist. LEXIS 19876 (M.D. Ala. 2010); *Bridal Expo, Inc. v. Van Florestein*, 2009 U.S. Dist. Lexis 7388 (S.D. Tex. 2009); *Lasco Foods, Inc. v. Hall & Shaw Sales, Marketing, and Consulting LLC*, 600 F. Supp. 2d 1045 (E.D. Mo. 2009); *U.S. Bioservices Corp. v. Lugo*, 595 F. Supp. 2d 1189 (D. Kan. 2009); *Condux International, Inc. v. Haugum*, 2008 U.S. Dist. LEXIS 100949 (D. Minn. 2008); *Black & Decker, Inc. v. Smith*, 568 F. Supp. 2d 929, 934-37 (W.D. Tenn. 2008); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 967 (D. Ariz. 2008); *Diamond Power Int’l v. Davidson*, 540 F. Supp. 2d 1322, 1342 (N.D. Ga. 2007); *Brett Senior & Assocs., P.C. v. Fitzgerald*, 2007 U.S. Dist. LEXIS 50833 (E.D. Pa. 2007); *B&B Microscopes v. Armogida*, 532 F. Supp. 2d 744 (W.D. Pa. 2007); *Lockheed Martin Corp. v. Speed*, 2006 U.S. Dist. LEXIS 53108 (M.D. Fla. 2006); *International Ass’n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479 (D. Md. 2005).

The broader and more employer-friendly view, which has proven thus far to be the minority view, is illustrated by the 7th Circuit’s decision in *Int’l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), where the Court held that an employee can be found to have accessed a computer “without authorization” whenever he does so in breach of his duty of loyalty to the company. For other decisions adopting this view, see, e.g., *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2007); *Guest-Tek Interactive Entm’t Inc. v. Pullen*, 665 F. Supp. 2d 42 (D. Mass. 2009); *Ervin & Smith Advertising & Pub. Relations, Inc. v. Ervin*, 2009 U.S. Dist. LEXIS 8096 (D. Neb. 2009); *Nilfisk-Advance, Inc. v. Mitchell*, 2006 U.S. Dist. LEXIS 21993 (W.D. Ark. 2006).

For a number of cases decided before this circuit split arose on the scope of “access” and “authorization” under the Act, *see United States v. Phillips*, 477 F.3d 215; 2007 U.S. App. LEXIS 1632 (5th Cir. 2007) (A user's authorization to access a protected computer is based on the expected norms of intended use or the nature of the relationship established between the computer owner and the user); *Expert Business Systems, LLC v. BI4CE, Inc. d/b/a Business Intelligence Forces*, 233 Fed. Appx. 251; 2007 U.S. App. LEXIS 11002 (4th Cir. 2007) (upholding the district court’s ruling that an employer had failed to present sufficient evidence to support its claims under the CFAA, which centered in part on whether the defendants had remotely accessed the employer’s computers without authorization); *Triad Consultants Inc. v. Wiggins*, 249 Fed. Appx. 38; 2007 U.S. App. LEXIS 22226 (10th Cir. 2007) (upholding district court’s dismissal of corporation’s claims under the CFAA, in part because the corporation alleged no facts showing that former employee / defendant accessed the information in question); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001) (upholding district court’s award of preliminary injunction to plaintiff, because plaintiff showed it would likely succeed on the merits of its CFAA claim, which turned largely in part on whether the defendant had “exceeded authorized access” to the plaintiff’s website); *Worldspan, L.P. v. Orbitz, LLC*, 2006 U.S. Dist. LEXIS 26153 (N.D. Ill. Apr. 19, 2006) (“Moreover, it is clear from the language of the CFAA that accessing a computer ‘without authorization’ does not include ‘exceed[ing] authorized access.’ Because Worldspan has not adequately alleged that Orbitz accessed its computers “without authorization,” Count I must be dismissed”); *SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 209; 2005 U.S. Dist. LEXIS 21228 (E.D. Va. Sept. 9, 2005) (“Furthermore, Plaintiff’s Amended Complaint does not allege facts that the defendants “exceeded authorized access” within the meaning of the statute. Mr. Berman gave the CFAA defendants access to BAI’s server and to the information on the server; consequently, the CFAA defendants were “entitled to obtain” information on the server because Mr. Berman explicitly allowed them access to it. *See* § 1030(e)(6). Even if Mr. Berman allowed the defendants access to the BAI server and SecureInfo’s materials in violation of the license agreements, under his grant of authority to the defendants, they were entitled to obtain the information on the server”) (Corporation’s wholesale use of the tour company’s travel codes to facilitate gathering tour company’s prices from its website was abuse of proprietary information that went beyond any authorized use of appellee’s website); *Business Information Systems v. Professional Governmental Research*, 2003 U.S. Dist. LEXIS 27363 (W.D. Va. Dec. 16, 2003) (“Progress’s actions did not result in impairment of the availability of data, a program, a system, or information because it did not shut down BIS’s server. In addition, Progress’s actions did not result in an impairment to the integrity of the system because Progress’s program utilized Snyder’s username and password to access BIS’s system on behalf of others. It was the same as if Snyder had communicated his username and password to the remote user and told him or her that they were free to use it; Progress’s program just automated this process. As a result, there is no violation of the Computer Fraud and Abuse Act”); *Four Seasons Hotel & Resorts B.V. v. Consorcio Barr, S.A.*, 267 F. Supp. 2d 1268, 2003 U.S. Dist. LEXIS 8717 (S.D. Fla. May 9, 2003) (e-mail messages are considered to access every computer they pass through on their way to their intended recipients); *In re America Online, Inc. Version 5.0 Software Litigation*, 168 F.Supp.2d 1359, 1370-71 (S.D. Fla. 2001) (Citing legislative history of subsections 1030(a)(5)(B) and (C) for the proposition that these provisions “are intended to apply to outsiders who access a computer,” not to “insiders” who access individuals’ computers with their

permission to do so); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000) (Use of search robots to harvest information from Plaintiff's database is "access" under the CFAA).

### III. Proving Loss / Damage

As noted above, in order for civil liability to attach under the Act, the employer has the burden to show that the employee's unauthorized access "recklessly cause[d] damage..." involving "loss to 1 or more persons during any 1-year period... aggregating at least \$5,000 in value." 18 U.S.C. § 1030(g) (incorporating 18 U.S.C. § 1030 (a)(5)(B) & (c)(4)(A)(i)(I)). The Act specifically defines "loss" to mean "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 defines "damage" to mean "any impairment to the integrity or availability of data, a program, a system, or information..." 18 U.S.C. § 1030(e)(8) & (11).

A number of courts have strictly construed this damage/loss prerequisite and the Act's definition of cognizable "loss", and have granted summary judgment for defendant employees sued under the Act where the employer fails to introduce sufficient evidence to show \$5,000 in aggregate losses as defined under the Act. *See, e.g., Global Policy Partners, LLC v. Yessin*, 2010 U.S. Dist. LEXIS 14838 at \*11 (E.D. Va. February 18, 2010) (holding that plaintiffs in CFAA cases "must show that the losses they claim were the reasonably foreseeable result of the alleged CFAA violations, and that any costs incurred as a result of the measures undertaken to restore and resecure the [computer] system were reasonably necessary in the circumstances") (*citing A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009)); *B.U.S.A. Corp. v. Ecogloves, Inc.*, 2009 U.S. Dist. LEXIS 89035 (S.D.N.Y. Sept. 28, 2009) (dismissing plaintiffs' CFAA claim, in part for failing "to marshal admissible evidence that would show that they have met the jurisdictional threshold for damages under the CFAA").

In *Global Policy Partners*, it was largely undisputed that the defendant had broken into the plaintiff's computer system and read the plaintiff's emails without authority. The "loss" claimed by the plaintiff consisted of (i) nearly \$6,500 paid to a web designer and to ISPs "in order to register, configure, and design new web sites and e-mail accounts"; (ii) \$27,500 in the plaintiff's lost billable time spent investigating and responding to the offense; and (iii) "millions of dollars" in lost revenue from failing to win a project that was the subject of the emails in question. While the court conceded that many of these claimed losses were arguably spent in "responding to and addressing an offense and costs of restoring the system to its condition prior to the offense", the court held that the damages were nevertheless not recoverable under the Act because, *inter alia*, the plaintiff failed to show that the expenditures "were a reasonably necessary response to the alleged CFAA violations". As stated by Lee E. Berlik in a blog post written about this opinion, *Proving Loss Under the Computer Fraud and Abuse Act*, Virginia Business Litigation Lawyer Blog (May 24, 2010), the decision stands for the proposition that losses from a violation of the Act are not necessarily recoverable "simply because money was spent subsequent to the violations"; and even where a violation occurs, "that would not give the plaintiff a blank check to

perform system updates that were not reasonably necessary to restore and re-secure the system”. The blog post can be accessed here:

[http://www.virginiabusinesslitigationlawyer.com/2010/05/proving-loss-under-the-compute.html?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%3A+VirginiaBusinessLitigationLawyerBlog+%28Virginia+Business+Litigation+Lawyer+Blog%29](http://www.virginiabusinesslitigationlawyer.com/2010/05/proving-loss-under-the-compute.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+VirginiaBusinessLitigationLawyerBlog+%28Virginia+Business+Litigation+Lawyer+Blog%29).

Some courts have further limited the scope of cognizable losses under the Act by holding that the Act permits recovery of lost revenue only where the violation of the statute leads to an “interruption in service” and/or some type of inoperability of the computer systems in question. *See, e.g., Nexans Wires S.A. v. Sark-USA, Inc.*, 166 Fed. Appx. 559 (2nd Cir. 2006) (affirming dismissal of a CFAA case, holding that plaintiff failed to establish the requisite amount of loss required under the Act, partially due to the fact that while plaintiff company incurred lost profits from violation of the Act, it did not suffer an interruption in service); *Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760 (N.D. Ill. 2009) (holding that the Act’s definition of damage is limited to impairment of integrity or availability of data and information, as the plain language of the statutory definition referred to situations in which data was lost or impaired because, for example, it was erased or because defendant had physically destroyed the computer equipment); *Civic Center Motors, Ltd. v. Mason Street Import Cars, Ltd.*, 387 F. Supp. 2d 378 (S.D.N.Y. 2005) (holding that because lost profits resulting from defendant’s unauthorized access did not result from computer impairment or damage, they were not compensable losses under the CFAA).

For other cases along these same lines, *see also SKF USA, Inc. v. Bjerckness*, 636 F. Supp. 2d 696 (N.D. Ill. 2009) (employer failed to state claim under the CFAA against former employees because the employer did not plead that it suffered any costs related to its computers or that it suffered any service interruptions); *Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int’l Inc.*, 616 F. Supp. 2d 805 (N.D. Ill. 2009) (former employee who e-mailed customer files to herself when she left her employer was entitled to summary judgment dismissing former employer’s claim alleging violation of the CFAA because the employer suffered no damage or loss to its data, computers, or network from this conduct); *A.V. v. iParadigms*, 544 F. Supp. 2d 473 (E.D. Va. 2008) (granting summary judgment to defendant in CFAA claim, partly due to the fact that the plaintiff failed to produce any evidence of actual or economic damages resulting from the defendant’s alleged violation of the Act); *Chas. S. Winner, Inc. v. Polistina*, 2007 U.S. Dist. LEXIS 40741 (D.N.J. 2007) (dismissing for lack of federal subject matter jurisdiction because the plaintiffs failed to allege facts that show that they suffer they suffered a “loss” as defined under the Act); *L-3 Communications Westwood Corp v. Joseph Emile Robichaux, Jr. et al*, 2007 U.S. Dist. LEXIS 16789 (E.D. La. Mar. 8, 2007) (“Because L-3 has not asserted that there was damage to their computers or an interruption of service, it has not alleged a cognizable loss under the CFAA. Accordingly, L-3 has not demonstrated a likelihood of success on the merits of the CFAA claim.”); *Spangler, Jennings & Dougherty, P.C. v. Mysliwy*, 2006 U.S. Dist. LEXIS 39602 (N.D. Ind. 2006) (denying plaintiff’s motion for summary judgment on its claim under the Act, because the plaintiff failed to provide any proof that it had been damaged by the defendant’s alleged violation of the Act); *Worldspan, L.P. v. Orbitz, LLC.*, 2006 U.S. Dist. LEXIS 26153 (N.D. Ill. Apr. 19, 2006) (“Worldspan's failure to adequately allege damage is an alternative ground for dismissal of the complaint. We need not reach Orbitz's remaining argument.”); *Resdev, LLC v. Lot Builders Assoc., Inc.*, 2005 U.S. Dist. LEXIS 19099 (M.D. Fla.

Aug. 10, 2005) (Revenues from a trade secret were, in this case, neither a "but-for" nor a proximate consequence of "damage" and also did not fit within the grouping of "loss" in the CFAA.); *Civic Ctr. Motors, Ltd. v. Mason St. Imp. Cars, Ltd.*, 387 F. Supp. 2d 378, 382; 2005 U.S. Dist. LEXIS 19941 (S.D.N.Y. Sep. 6, 2005) (case dismissed because Plaintiffs failed to plead losses resulting from data corruption, the cost of responding to and repairing the computer problems, and exposure to liability to customers for breach of privacy in their complaint which resulted in a failure to state proper grounds for relief under the CFAA); *Nexans v. Sark-S.A.*, 319 F. Supp. 2d 468; 2004 U.S. Dist. LEXIS 9712 (S.D.N.Y., May 27, 2004) ("Under the Computer Fraud and Abuse Act, 18 U.S.C.S. § 1030, the meaning of 'loss,' both before and after the term was defined by statute, has consistently meant a cost of investigating or remedying damage to a computer, or a cost incurred because the computer's service was interrupted."); "The 'revenue lost' which constitutes 'loss' under 18 U.S.C.S. § 1030(e)(11) appears from the plain language of the statute to be revenue lost because of an interruption of service. Revenue lost because the information was used by a defendant to unfairly compete after extraction from a computer does not appear to be the type of 'loss' contemplated by the Computer Fraud and Abuse Act, 18 U.S.C.S. § 1030."); *Pearl Invs. LLC v. Standard I/O, Inc.*, 257 F. Supp. 2d 326, 2003 U.S. Dist. LEXIS 6890 (D. Me. 2003) (magistrate judge recommends that defendants be granted summary judgment as to plaintiff's claim under the Act, as the plaintiff showed no cognizable evidence that defendant's alleged conduct damaged plaintiff's computer system in any quantifiable amount); *Tyco Int'l Inc. v. Does*, 2003 U.S. Dist. LEXIS 11800 (S.D.N.Y. 2003) (discussing compensatory damages under the Act for plaintiff's costs associated with assessing the damage to its computer system and restoring its system after plaintiff's attack); *Motorola Credit Corp. v. Uzan*, 2002 U.S. Dist. LEXIS 19632 (S.D.N.Y., Oct. 16, 2002) ("With regard to plaintiffs' 'computer hacking' claims... Defendants properly note that plaintiffs' complaint fails to allege the requisite \$ 5,000 in damages required to maintain a civil action under § 1030(a)(5)(B)(i) and, accordingly, this claim must be dismissed, without prejudice."); *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 524-25 (S.D.N.Y. 2001) (recognizing only costs in remedying damage as recoverable under CFAA).

Thus, in bringing a claim against an employee or former employee under the CFAA, an employer must be careful to ensure that the it has incurred, within the span of no more than one year, at least \$5,000 in losses which would qualify as losses as defined under both the Act itself and case law in the relevant jurisdiction construing such claimed losses. Along those same lines, counsel for employees sued under the Act should always consider the propriety of filing a motion to dismiss or summary judgment motion, challenging the adequacy of the employer's claim for CFAA losses.

#### IV. Potential Supplement to Trade Secret and Non-Compete Claims

One common context in which CFAA claims arise in the employment context is where an employer is suing an employee or former employee for unlawful use of company trade secrets or for violation of a non-compete clause, because such claims often involve allegations that the employee has made an unauthorized use of electronic data such as customer lists, proprietary company information, and the like. Furthermore, adding a CFAA claim in such cases may be attractive to an employer for a number of reasons. For one thing, where a departing employee is

actively interfering with or damaging the employer's business by the unauthorized use of electronic data, particularly where that data has been altered or damaged, "loss" arising from a CFAA violation may be somewhat easier for the employer to establish. *See, e.g., Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (The CFAA is designed to encompass situations where Plaintiff's employees, while still working for plaintiff, used plaintiff's computers to send trade secrets to defendant via e-mail). Also, bringing a CFAA claim may give the employer the option of bringing its claims in federal court, in a case where federal jurisdiction may have otherwise been unavailable, due to lack of diversity between the parties and claims which otherwise would have been entirely governed by state law (such as a claim under a contractual non-compete clause).

On the other hand, a number of courts have questioned whether improper use of trade secrets or violation of a non-compete clause constitute the type of "loss" or "damage" contemplated by the CFAA. *See, e.g., Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760 (N.D. Ill. 2009) (claims for dissemination of trade secrets and confidential information to competitor were not covered by CFAA's definition of damage; rather, damage under the Act was limited to impairment of integrity or availability of data and information, as plain language of statutory definition referred to situations in which data was lost or impaired because, for example, it was erased or because defendant had physically destroyed the computer equipment); *SKF USA, Inc. v. Bjerkness*, 636 F. Supp. 2d 696 (N.D. Ill. 2009) (employer failed to state claim under the CFAA against former employees who allegedly transferred confidential information from their work computers to storage devices and took information with them when they went to work for a competitor, because the employer did not plead that it suffered any costs related to its computers or that it suffered any service interruptions); *Garelli Wong v. Nichols*, 2008 U.S. Dist. Lexis 3288 (N.D. Ill. Jan. 16, 2008) ("Though Garelli Wong would like us to believe that recent amendments to the CFAA are intended to expand the use of the CFAA to cases where a trade secret has been misappropriated through the use of a computer, we do not believe that such conduct alone can show "impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Therefore, we conclude that Garelli Wong has failed to sufficiently plead damage under the CFAA."); *Am. Family Mut. Ins. Co. v. Rickman*, 554 F. Supp. 2d 766 (N.D. Ohio 2008) (granting motion to dismiss CFAA claim because CFAA was not meant to cover disloyal employee who walked off with confidential information; rather the CFAA punished trespassers and hackers; the employer had not alleged the type of loss that came within the scope of the Act); *Lockheed Martin v Kevin Speed*, 2006 U.S. Dist. LEXIS 53108 (M.D. Fla. Aug. 1, 2006) (taking of trade secrets does not, by itself, fit within the grouping of "damage" or "loss"); *Civic Ctr. Motors, Ltd. v. Mason St. Imp. Cars, Ltd.*, 387 F. Supp. 2d 378, 382; 2005 U.S. Dist. LEXIS 19941 (S.D.N.Y. Sep. 6, 2005) ("In the instant case, Plaintiffs are seeking compensation for lost profits resulting from Defendant's unfair competitive edge and for their now wasted investment in the development and compilation of the database information. However, neither of these kinds of losses are the result of computer impairment or computer damage. Therefore, they are not compensable "losses" under the CFAA.").

For more information on CFAA claims in the context of trade secret cases, *see* Peter J. Toren, *CFAA Can Protect Trade Secrets*, New York Law Journal (May 24, 2010), <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202458635753>.

## V. Upshot / Takeaway

Counsel on both sides of the employment relationship would do well to keep several things in mind when working on matters that may potentially involve liability under the CFAA. For example:

- Attorneys counseling recently terminated employees, or employees who are for any other reason departing their employer, should take care to ensure that the client does not take any actions which may potentially lead to a claim being brought against the client under the CFAA. For instance, the client should be closely advised about the dangers of erasing valuable computer files, copying or printing files which they do not have authorization to take with them, accessing email accounts or databases which they do not have the right to view, viewing or copying sensitive proprietary information such as trade secrets or customer lists, sabotaging the employer's computer equipment or systems, etc.
- Counsel for employers should consider their client's rights to bring a civil action under the CFAA when an employee or departing employee has accessed, used, copied, printed, or deleted computer files without authorization. Such claims should particularly be considered in trade secret or non-compete claims brought against employees or former employees, and/or as potential counterclaims where such employees have sued the employer – for example, in a lawsuit challenging the circumstances surrounding the employee's termination.
- One must also always keep in mind the employer's burden to show the requisite amount of "loss" as defined under the Act. Unauthorized access of company computers or systems may not be actionable under the Act where the access was innocuous or largely harmless from an economic perspective, where the loss was not reasonably incurred in response to the unauthorized access, or where the access did not cause the computers or systems to be inoperable or out of service for any significant amount of time.

## VI. More Resources

For more information on CFAA claims brought in the employment context and related topics, see the following sources (keeping in mind that the most recent amendments to the CFAA went into effect in September 2008, making any articles before that date potentially outdated):

- Orin Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561 (2010), [http://www.minnesotalawreview.org/sites/default/files/Kerr\\_MLR\\_0.pdf](http://www.minnesotalawreview.org/sites/default/files/Kerr_MLR_0.pdf).
- Peter J. Toren, *CFAA Can Protect Trade Secrets*, New York Law Journal (May 24, 2010), <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202458635753>.

- Jon Hyman, *Do You Know? 12% of Employees Knowingly Violate IT Policies*, Ohio Employer's Law Blog (March 16, 2010), <http://ohioemploymentlaw.blogspot.com/search?q=12%25+IT&x=0&y=0>.
- Dale C. Campbell and David Muradyan, *The Seventh and Ninth Circuits Split on What Constitutes "Without Authorization" Within the Meaning of the Computer Fraud and Abuse Act*, The IP Law Blog (February 19, 2010), <http://www.theiplawblog.com/archives/-webtech-the-seventh-and-ninth-circuits-split-on-what-constitutes-without-authorization-within-the-meaning-of-the-computer-fraud-and-abuse-act.html>.
- David Johnson, *Update on CFAA Circuit Split: District Courts in 8th Circuit Adopt Minority View, Permitting Claims Where Defendant Exceeds His Authority to Access Computer*, Digital Media Lawyer Blog (November 16, 2009), [http://www.digitalmedialawyerblog.com/2009/11/update\\_on\\_cfaa\\_circuit\\_split\\_d.html](http://www.digitalmedialawyerblog.com/2009/11/update_on_cfaa_circuit_split_d.html).
- David Conforto, *Employees Beware: Computer Fraud & Abuse May Restrict Ability to Retain Documents*, Boston Employment Lawyer Blog (November 5, 2009), [http://www.bostonemploymentlawyerblog.com/2009/11/computer\\_fraud\\_and\\_abuse\\_act\\_b.html](http://www.bostonemploymentlawyerblog.com/2009/11/computer_fraud_and_abuse_act_b.html).
- Amy E. Bivins, *Attorneys Advise Employers to Revisit Data Misuse Policies After Brekka Ruling*, Bureau of National Affairs Daily Labor Report (November 4, 2009), <http://www.tradesecretslaw.com/uploads/file/110409%20DailyLaborReport.pdf>.
- Kenneth J. Vanko, *Two Views of the Computer Fraud and Abuse Act (Brekka and Pullen)*, Legal Developments in Non-Competition Agreements (October 30, 2009), <http://www.non-competes.com/2009/10/two-views-of-computer-fraud-and-abuse.html>.
- Robert B. Milligan and Carolyn E. Sieve, *Establishing CFAA Violations by Former Employees*, Law 360 (October 27, 2009), <http://www.tradesecretslaw.com/uploads/file/Establishing%20CFAA%20Violations%20-%20Law%20360.pdf>.
- David Johnson, *LVRC v. Brekka: 9th Circuit Decision Creates Circuit Split on Whether CFAA Applies to an Employee Who Misuses His Authority to Access His Employer's Computer Files*, Digital Media Lawyer Blog (October 1, 2009), [http://www.digitalmedialawyerblog.com/2009/10/lvrc\\_v\\_brekka\\_9th\\_circuit\\_dec.html](http://www.digitalmedialawyerblog.com/2009/10/lvrc_v_brekka_9th_circuit_dec.html).
- Lori Bauman, *Ninth Circuit Narrowly Interprets Computer Fraud and Abuse Act*, Ater Wynne LLP Northwest Business Litigation Blog (September 24, 2009), [http://www.aterwynneblog.com/oregon\\_business\\_litigation/2009/09/ninth-circuit-narrowly-interprets-computer-fraud-and-abuse-act.html](http://www.aterwynneblog.com/oregon_business_litigation/2009/09/ninth-circuit-narrowly-interprets-computer-fraud-and-abuse-act.html).

- David Johnson, *ES&H v. Allied Safety: Court Sidesteps Split in Authority over Whether CFAA Applies to an Employee Who Misuses His Authority to Access His Employer's Computer Files*, Digital Media Lawyer Blog (September 24, 2009), [http://www.digitalmedialawyerblog.com/2009/09/esh\\_v\\_allied\\_safety\\_court\\_side\\_1.html](http://www.digitalmedialawyerblog.com/2009/09/esh_v_allied_safety_court_side_1.html).
- Amy E. Bivins, *Brekka Case Shows Need for Comprehensive Strategy to Shield Data from Insider Misuse*, Bureau of National Affairs Electronic Commerce & Law Report (September 20, 2009), <http://www.tradesecretslaw.com/uploads/file/Sieve.pdf>.
- Nick Akerman, *When Workers Steal Data to Use at New Jobs*, The National Law Journal (July 7, 2009), <http://www.law.com/jsp/article.jsp?id=1202432036948>.
- Katherine Mesenbring Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 Mich. L. Rev. 819 (March 2009), <http://www.michiganlawreview.org/assets/pdfs/107/5/field.pdf>.
- Richard Warner, *Symposium: The Electronic Workplace: The Employer's New Weapon: Employee Liability Under the Computer Fraud and Abuse Act*, 12 Empl. Rts. & Employ. Pol'y J. 11 (2008), <https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&crawlid=1&doctype=cite&docid=12+Empl.+Rts.+%26+Employ.+Pol%27y+J.+11&srctype=smi&srcid=3B15&key=5af00d2a6ee82f58f5d3e2de9c20b24f>.
- Shari Claire Lewis, *Can the CFAA Protect Your Firm's Data?*, New York Law Journal (July 25, 2008), <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202423247330>.
- Brian H. Corcoran, *The Computer Fraud and Abuse Act: "Hacker Repellent" That Works Great on Ex-Employees, Too*, Cyberspace Lawyer Vol. 7, No. 1 (March 2002) at page 2, <http://www.kattenlaw.com/files/Publication/8bb06409-a2bc-4f76-b594-02d9c2c77078/Presentation/PublicationAttachment/a654e6e5-30f5-4bfb-96a0-f174d49f1c45/Technology%20Winter%202001%20PDF.pdf>.