

Protecting Trade Secrets Under The Computer Fraud and Abuse Act

**By Francis J. Burke, Jr.
Steptoe & Johnson LLP
Phoenix, Arizona
(602) 257-5227
fburke@steptoe.com**

1. A theft or misappropriation of trade secrets from a computer or website may be a violation of the Computer Fraud Act, 18 U.S.C. §1030, which provides for civil remedies in addition to criminal sanctions. “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.” 18 U.S.C. §1030(g).
2. The Federal Computer Fraud and Abuse Act is focused on the protection of the confidentiality, integrity and availability of computer systems and data. There are seven different sections, which for the most part focus on unauthorized computer access which leads to or furthers some additional criminal end. In this outline we will focus on the three sections which have been primarily used in civil actions.
3. Subsection 1030(a)(2) prohibits the obtaining without authorization or in excess of authorized access, information from financial institutions, card issuers, consumer reporting agencies, the U.S. government or protected computers if the conduct involved an interstate or foreign communication. The term “protected computer” is defined very broadly. It means a computer—“(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States government and the conduct constituting the offense affects that use by or for the financial institution or the government; or (B) which is used in interstate or foreign commerce or communication.”
4. Section 1030(a)(4) prohibits knowingly and with intent to defraud accessing a protected computer, without or exceeding authorization, thereby furthering the intended fraud and obtaining anything of value. There is an exclusion if the defendant obtains solely computer time (use of the computer) with a value less than \$5,000 in any one year period. This is the first federal computer fraud statute, and the only subsection of the statute that directly addresses fraudulent conduct.
5. Section 1030(a)(5) consists of three subsections.
 - a. Under subsection (A)(i), it is a crime to intentionally cause damage without authorization to a protected computer by “transmission of a program, information, code, or command”, whether or not one has authorization to access the computer.

- b. Under subsections (A)(ii) and (A)(iii), it is a crime to cause damage if the protected computer was intentionally accessed without authorization. If the person recklessly causes damage, it shall be a felony (A)(ii) and if a person causes damage “as a result of such conduct” (i.e., negligently or otherwise), it shall be prosecuted as a misdemeanor (A)(iii).
 - c. In reviewing this provision, it should be noted that subsection (i) can be violated whether the actor is an outsider, such as a hacker, or an insider, such as a disgruntled employee. Some have indicated that the first portion of the statute is intended to apply to both viruses and worms.
 - d. To violate Sec. 1030(a)(5)(A), the conduct must cause (or in the case of attempted conduct, 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) modification or impairment s or potential modification or impairment, the medical examination, diagnosis, treatment, or care of one or more individuals;
 - (iii) physical injury to any person; or
 - (iv) a threat to public health or safety . . .” or
 - (v) damage affecting a computer used by or for a government entity in furtherance of administration of justice, national defense or national security.”
6. “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 accessor is not entitled so to obtain or alter”. 18 U.S.C. § 1030(e)(6).
7. “Damage” means any impairment to the integrity or availability of data, a program, a system, or information. 18 U.S.C. Sec. 1030(e)(8)
8. As a jurisdictional prerequisite to a civil action, the conduct must involve one of the damage factors in Sec. 1030 (a)(5)(B), which in most cases means \$5000 in loss. “Loss” is defined as “any reasonable cost to any victim, including the cost of responding to any 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.” 18 U.S.C. Sec. 1030(e)(11)

Cases Involving Unauthorized Access to Company Computers

9. In *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000), a civil action under the Computer Fraud and Abuse Act, the plaintiff alleged that the defendant embarked on a systematic scheme to hire away key employees for the purpose of obtaining the plaintiff’s trade secrets and that some of these employees

while still working for the plaintiff used the plaintiff's computers to send trade secrets to the defendant via e-mail.

Ruling upon a motion to dismiss, the court ruled the complaint stated a claim under 18 U.S.C. § 1030(a)(2)(C) which relates to the intentional accessing of a computer without authorization or exceeding authorized access, and thereby obtaining information from any protected computer. The defendant argued that the employees all had full access to all information allegedly transferred to the defendant. However, the court found that once the employees began acting as agents for the defendant, when the employees used the plaintiff's computers and information on those computers in an improper way, they were "without authorization."

The court also found that the pleading stated a claim under 18 U.S.C. § 1030(a)(4) for knowingly and with intent to defraud accessing a protected computer without authorization or exceeding authorized access, and by means of such conduct, furthering the intended fraud and obtaining anything of value. The court held that the claim need not state the common law elements of fraud, but need only allege that the defendant participated in dishonest methods to obtain the plaintiff's secret information.

Finally, the court found that the complaint stated a claim under 18 U.S.C. § 1030(a)(5)(C), which relates to persons who intentionally access a protected computer without authorization and as a result of such conduct, cause damage. The court rejected a defense claim that this section of the CFAA only applies to outsiders and not employees. The court also rejected a defense argument that the alleged loss of information by the plaintiff was not damage under the statute. The court noted that damage is "any impairment to the integrity . . . of data . . . or information." 18 U.S.C. § 1030(a)(8)(A), finding that "integrity" in the context of data necessarily contemplates maintaining the data in a protected state. By infiltrating the plaintiff's computer network and collecting and disseminating confidential information, the court found that there was an impairment of the data's integrity, and thus, damage within the meaning of the statute.

10. *Credentials Plus LLC v. Calderone*, 230 F. Supp. 2d 890 (N.D. Ind. 2002). Plaintiff alleged that defendant, a former co-owner and officer of plaintiff, had intentionally accessed plaintiff's computer and obtained information on clients and potential clients residing out of state by re-routing client e-mail originally sent to plaintiff. Plaintiff's computer was used to send and receive e-mail to customers throughout the country and qualified as a protected computer under the CFAA. Because of disputed evidence as to who had set up the alternative e-mail address, the Court denied defendant's Motion for Summary Judgment.
11. *U.S. Greenfiber v. Brooks*, No. CIV. A. 02-2215, 2002 WL 31834009 (W.D. La. Oct. 25, 2002). Defendant was quality control manager of plaintiff, responsible for overseeing quality control for 10 plants of plaintiff. Up to her termination at plaintiff's corporate headquarters, she copied documents belonging to plaintiff and took them with her. She later threatened to provide confidential information to adverse parties in litigation and to competitors. On plaintiff's Application for Preliminary Injunction, the Court found it likely plaintiff could prove a violation of the Computer Fraud and Abuse Act because she

had a company computer at home which was used to communicate with corporate headquarters and customers in interstate and foreign commerce. Although she was not authorized to access the company's communication system after her termination, she accessed the internal e-mail system and sent messages to employees and also removed all documents, e-mail files and computer files from the computer without authorization. The Court found it likely that plaintiff would establish a violation of the Louisiana Trade Secret Act because of defendant's possession of sensitive quality control and business records, including prior compliance records, e-mails, monthly reports, customer complaints, strategic plans, sales reports and customer pricing lists. In addition, she took further documents from the company computer system and was threatening to provide such information to adverse parties in civil litigation and to competitors.

12. *Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A.*, 267 F. Supp. 2d 1268 (S.D. Fla. 2003). The Court found that the defendant, a licensee of the plaintiff, violated Sec. 1030 (a)(5)(A)(i) by accessing without authorization Four Seasons protected computers by spoofing the IP addresses of Four Seasons, thereby causing damage to the computer system. The Court also found that defendant had violated Subsections (a)(5)(A)(ii) and (iii) by accessing remote computers within the Four Seasons's protected network through e-mail transmissions which damaged the network computers by impairing the availability of the computers to other systems and the network. The Court also found that defendant violated Subsections (a)(5)(A)(ii) and (iii) by accessing Four Seasons's protected computers and downloading confidential customer and financial data from its reservations database. A hotel industry expert testified that the value of the information obtained from the downloads was \$2,090,000 which plaintiff was awarded in damages. The Court also found that Four Seasons suffered "loss" in the amount of \$28,000 in expenses incurred in investigating and responding to the offenses which occurred within a one-year period.
13. *Pacific Aerospace & Electronics, Inc. v. Taylor*, 295 F. Supp. 2d 1188 (E.D. Wash. 2003). Plaintiff had a specialized business designing and manufacturing hermetically sealed connectors and housings for highly sensitive electronic circuitry. It had a limited market consisting of highly selected engineers. Defendant had employees who had signed confidentiality and employment agreements requiring them to maintain the secrecy of plaintiff's confidential information, including its customer information. Plaintiff alleged that defendants had stolen its customer information from its computer systems prior to leaving the company to form a competitor. The Court found that these allegations were sufficient to establish Federal Court jurisdiction under the CFAA. The Court noted that "Employers . . . 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" (at 1196).
14. *George S. May International Co. v. Hostetler*, No. 04 C 1606, 2004 WL 1197395 (N.D. Ill May 28, 2004). Plaintiff was a consulting firm, and defendant formed his own consulting firm to compete with plaintiff. Prior to being in plaintiff's employ, he used his access to plaintiff's computer system to take several copyrighted documents with him when he left. Although plaintiff did not specify the subsections under which it was suing,

the Court found that there were sufficient allegations to support claims under Sections 1030 (a)(2), 1030 (a)(4) and 1030 (a)(5). The defendant also claimed that at the time of his offense, he had authorized access to the computer. The Court held that under no stretch of the imagination did his authorization extend to removing copyrighted material from the computer system for his personal benefit or that of the competitor. Defendant also alleged that the loss alleged within the Complaint could not satisfy the statutory requirement of damages. The Court found that plaintiff had been damaged due to impairment of the integrity of the copyrighted information.

15. *Charles Schwab & Co., Inc. v. Carter*, No. 04 C 7071, 2005 WL 2369815 (N.D. Ill. Sept. 27, 2005). The Director of Information Technology for one of Schwab's divisions left to work for one of its institutional clients. While employed at Schwab, the Director had access to proprietary information but agreed to keep this information confidential. On the weekend prior to his departure, the Director accessed approximately 15,000 Schwab computer files and e-mailed confidential information to his new employer relating to certain of the data sources used in proprietary business models. The e-mails attached documents that would facilitate access to information databases licensed by Schwab used in connection with the models. Schwab's computer records also indicated that the Director had copied huge volumes of the 15,000 files. Shortly before copying the information, the Director had acquired a laptop with a high-speed DVD burner and told his colleagues that he planned to copy and keep the models. Schwab sued under Sections 1030 (a)(2) and (a)(4). The Court denied defendant's claim that private actions under the CFAA are limited to Section 1030 (a)(5), and also found that Director's new employer and its limited partners could be held vicariously liable for the Director's activities by urging the Director to access Schwab's computer system beyond his authorization for their benefit. The Court further found that Schwab is a financial institution and that the records accessed were financial records within the meaning of Sec. 1030 (a)(2). The Defendant also moved to dismiss because the director had not accessed the computers using an interstate communication. The Court held that because the Complaint alleges that Schwab maintains an interstate computer network as part of its nationwide business operations, it would be reasonable to infer that when the Director accessed the network, his conduct involved interstate communication.
16. *P.C. Yonkers, Inc. v. Celebrations The Party and Seasonal Superstore, LLC*, 428 F. 3d 504 (3d Cir. 2005). Plaintiffs were retail party goods and related products stores which sued two former managers who formed a competing business. Plaintiffs proved that defendants accessed their computer system from their home computers 125 times over 7 days after their departure but had no proof as to what information was stolen. The Court found the Complaint stated a cognizable claim under Section 1030 (a)(4), but affirmed the District Court's denial of a preliminary injunction based on lack of evidence that they had taken any information.
17. *C.H. Robinson Worldwide, Inc. v. Command Transportation, LLC*, No. OSC 3401, 2005 WL 3077998 (N.D. Ill. Nov. 16, 2005). In this case plaintiff, which provides computerized commercial logistic services to truckers, sued two of its former employees and a new competitor after the competitor developed a new software program identical to the express software used by the plaintiff. The Court denied challenges to the Complaint

which alleged claims under Sections 1030 (a)(2) and 1030 (a)(5). Defendants alleged that plaintiff failed to allege that they had intercepted interstate or foreign communications. Following the Schwab decision, the Court found it reasonable to infer that the defendants' involved interstate commerce.

18. In *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), Mr. Citrin had resigned to compete against his employer. His job had been to identify properties that IAC might want to acquire and assist in any ensuing acquisition. Before returning his laptop computer, he deleted all of the data contained on the laptop. This included not only data he had collected in pursuit of former employer's real estate business, but also data that would have revealed that he had engaged in improper conduct before he decided to resign. To do so he had used a special eraser software that made the data unrecoverable. IAC sued Citrin under both § 1030(a)(5)(A)(i) and (ii). In deciding whether Citrin had accessed the computer without authorization or had exceeded authorized access, the court followed the Shurgard test, holding that when an employee violates his duty of loyalty, he voids his agency relationship with his employer and terminates his authority to access the employer's computer. The court found that his authorization terminated when he resolved to destroy files that incriminated himself and other files that were the property of his employer, thereby breaching his duty of loyalty. The breach of loyalty was premised not only under the destruction of data that identified prospective real estate IAC might want to buy, but also the files that incriminated him in improper conduct in which he had engaged before he decided to quit.
19. In *Lockheed Martin Corp. v. Speed*, 2006 WL 2683058 (M.D. Fla., Aug. 1, 2006), the court ruled that employees who use their access to corporate computers to download trade secrets and then share them with the companies competitors cannot be said to have accessed this proprietary information "without authorization" or in excess of their authorization for purposes of the CFAA. Lockheed had sued the employees under §1030(a)(4) and under §1030(a)(5)(A)(i) and (a)(5)(A)(ii). Unlike prior decisions, in determining whether the employees had acted either without authorization or had exceeded authorized access, the court declined to review the Restatement of Agency, holding that the plain language of the statute was clear. The court concluded that because Lockheed had permitted the employees to access the company computer, they were not without authorization, and because Lockheed permitted the employees to access the precise information at issue, the employees did not exceed authorized access.
20. In *Nilfisk-Advance, Inc. v. Kevin Mitchell*, 2006 WL 827073 (W.D. Ark., 2006), the plaintiff alleged that a former employee had transferred confidential information and trade secrets to his home computer just before he was terminated, intending to give them to competitors. The court correctly noted that the company was alleging not that Mitchell had no authorization but that he had exceed his authorization when he gained access to confidential information and emailed it to his home computer with the alleged purpose of misappropriating it.
21. In *United States v. Philips*, 477 F.3d 215 (5th Cir. 2007), the court interpreted the meaning of the words "without authorization." Defendant was a student in the department of computer sciences at the University of Texas and signed an acceptable use

computer policy in which he agreed not to perform certain scans on the university computer account that would permit him to search for vulnerabilities and hack in to attack the network. In fact, Philips did hack into the computer and gained access to information about 45,000 current and prospective students. He was convicted of violating §1030(a)(5)(A)(ii) for knowingly accessing the University of Texas network without authorization and recklessly causing damage to the network. The Fifth Circuit held that the scope of a user's authorization to access a protected computer under the CFAA may be determined based on the expected norms of intended use of the computer. The court found that Philips' activities were not authorized by the acceptable use computer policy that he had signed, and that his hacking was not an intended use of the University of Texas network within the understanding of any reasonable computer user and constituted a method of obtaining unauthorized access to computerized information that he was not permitted to view or use.

Cases Involving Unauthorized Access To Websites

22. *E. F. Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001). Several employees of plaintiff moved to defendant and hired an internet consultant to design a computer program called a scraper which functions like a robot to seek information from a website through the internet. The scraper utilized tour codes provided by the individual defendants, to access plaintiff's website repeatedly and easily obtained pricing information for those specific tours. The scraper sent more than 30,000 inquiries to plaintiff's website and recorded the pricing information into a spreadsheet. The scraper downloaded 60,000 lines of data, the equivalent of eight telephone directories of information. It compiled the data into a spreadsheet and provided it to the defendant corporation which then systematically undercut plaintiff's prices.

The Court focused on a confidentiality agreement between one of the individual defendants and the plaintiff which prohibited the use of confidential information "for the employees' own benefit or for the benefit of any other person or business entity." When the defendants provided the tour and gateway codes to the internet consultant, the scraper was able to correlate the tour codes to actual tours and destination points whereas to the general public they would have been gibberish. The court concluded that because of the broad confidentiality agreement, the defendants' actions "exceeded authorized access" for purposes of 18 USC §1030(a)(4).

With regard to whether plaintiff had suffered "damage" or "loss" within the meaning of 18 USC §1030(g), the District Court had held that "loss" would encompass a loss of business, good will and the cost of diagnostic measures that plaintiff took after it learned of defendants' access to its website. The defendants' challenged whether diagnostic measures could be included within the minimum damage requirement of \$5,000.00. The court concluded that expenses of at least \$5,000.00 resulting from a party's intrusion are "losses" for purposes of the "damage or loss" requirement of the CFAA.

23. *E.F. Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003). Later, the Court of Appeals declined to vacate the injunction "as against Zefer," although it found an insufficient basis to support an independent preliminary injunction against Zefer, because it had not signed a confidentiality agreement. The appellate court declined to affirm the district court's "reasonable expectations" test which was predicated upon the copyright notice on plaintiff's home page, the other defendants' provision to Zefer of confidential information obtained in breach of their confidentiality agreements, and the fact that the website was configured to allow ordinary visitors to the site to view only one page at a time.
24. *Physicians Interactive v. Lathian Systems, Inc.*, No. CA 03-1193-A, 2003 WL 23018270 (E.D. Va. Dec. 5, 2003). Lathian maintains a website for medical professionals which may be accessed only by password and personal identification number supplied by plaintiff. The website contains confidential customer lists and other proprietary information. Plaintiffs alleged that defendants, through their information technology employee, launched a series of three attacks on their website using software robots or extraction software programs and successfully accessed and downloaded a significant

amount of plaintiff's proprietary medical professional information. Two of the attacks were traced back to defendant's and their employees internet protocol addresses. The Court ruled that the plaintiff had adequately alleged violations of Section 1030 (a)(2), 1030 (a)(4), and 1030 (a)(5) of the Computer Fraud and Abuse Statute and issued a preliminary injunction.

25. *Theofel v. Farey Jones*, 341 F. 3d 978 (9th Cir. 2003), on rehearing 359 F.3d. 1066 (9th Cir. 2004). In one civil action, defendants sent a subpoena without notice to a third party ISP requesting e-mails of the plaintiffs. The subpoena was overbroad and led to the release of much personal confidential information. The plaintiffs then filed a separate suit against the defendants alleging, among other things, a violation of the Computer Fraud and Abuse Act, Sec. 1030 (a)(2). The Ninth Circuit overturned the District Court's dismissal of the action, holding that a person may maintain a cause of action against another for improperly accessing confidential information on a computer owned by a third party, holding that individuals other than the computer's owner may be proximately harmed by unauthorized access particularly if that have erased data stored on it.
26. *Creative Computing v. GetLoaded.Com LLC*, 386 F.3d 930 (9th Cir. 2004). Plaintiff had developed a successful internet site which enabled truckers to find backloads. Defendant entered the site using a stolen login name and password to copy confidential information, later also hacked into the code, exploiting a hole in Microsoft software, and later induced one of the plaintiff's employees to access confidential information regarding several thousand customers. He downloaded and sent to his home e-mail account a confidential address to plaintiff's server, so that he could access the server from home and retrieve the customer lists. The Ninth Circuit sustained a damage award for violation of the CFAA, and rejected defendant's argument that each intrusion must cause \$5,000 of loss or damage.
27. *International Association of Machinists and Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479 (D. MD 2005). Plaintiff's union sued its secretary-treasurer who had authorized access to a secure proprietary website from which she could access the confidential membership list. She had signed an agreement stipulating not to use the information for any purpose that would be contrary to the policy and procedures set forth in the union constitution. Plaintiffs alleged that she had accessed the server approximately 10,000 times to secure the names and addresses of every member in four different union locals, and that she had provided the information to a competitor union which was seeking to separately organize the workers. The Court dismissed the CFAA claim on the grounds that she had authorized access to the database and therefore could not be sued.

Cases Discussing Whether Loss or Damage Exceeds \$5000

28. *Pearl Investments, LLC v. Standard I/O, Inc.*, 257 F.Supp. 2d 326 (D. Me. 2003). Plaintiff's CFAA claim failed because plaintiff argued that defendant's alleged wrongful connection to its system adversely affected the system's speed and operation thereby causing damages. However, it did not set forth cognizable evidence that the conduct damaged its system in any quantifiable amount let alone an amount approximating more

than \$5,000 in one year. Additionally, a claim under the DMCA was sustained based on an allegation that defendant had circumvented the protections of plaintiff's encrypted password-protected virtual private network to gain unauthorized access to data that included plaintiff's copyrighted software.

29. In *United States v. Middleton*, 231 F.3d 1207 (9th Cir. 2000), defendant was prosecuted for intentionally causing damage to a protected computer without authorization, in violation of 18 U.S.C. § 1030(a)(5)(A). After quitting his job as a computer administrator, he accessed his e-mail account and switched to another user's account where he created and deleted accounts and added features to existing accounts. Later, his e-mail account was closed, he logged on to a test account and entered the main computer where he changed passwords, altered the computer's registry, deleted the entire billing system, including programs that ran the billing software and deleted two internal databases. His former employer used two company employees to repair the damage to the system. The Computer Fraud and Abuse Act defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information, that causes loss aggregating at least \$5,000.00 in value during any one-year period to one or more individuals." 18 U.S.C. § 1030(e)(8)(A). The court rejected Mr. Middleton's argument that Congress intended the phrase "one or more individuals" to exclude corporations. The court rejected his instruction on the definition of "damage", finding that the term includes any impairment to the computer system that caused the loss of at least \$5,000.00, including any monetary loss sustained as a result of any damage to the computer system, which should include any measures reasonably necessary to restore the data, program, system or information that was damaged or to re-secure the data program system or information from further damage. The court also rejected defendant's argument that by using salaried employees to repair the system, that the victim had suffered no loss. The court reasoned that calculation of the loss could include the amount of time spent by the employees at their imputed hourly rates since the company would have had to hire outside contractors to repair the damage had it not used its own employees.
30. *United States v. Wiest*, No. ACM33964, 2002 WL 31235026 (A.F. Ct. Crim. App. Sept. 24, 2002). Prosecution under 18 U.S.C. § 1030(a)(5)(B). The Court found that the unauthorized access need not be intentional because 1030(a)(5)(B) is a lesser included offense. With regard to defendant's alleged mistake of fact, the Court affirmed the trial court's instruction that the mistake of fact had to be reasonable instead of merely honest. The Court affirmed the verdict finding that any reasonable juror would have concluded that appellant did not have an authorized belief that access to a particular computer system was authorized. The sluggishness of the computer system, jerkiness of the display and presence of two unauthorized programs was sufficient to find damage and the repair and securing of the system was found to constitute damage in excess of \$5,000. The Court properly rejected a defense instruction that would have said that damages should not include expenses for making a computer system more secure than it was before the breach. In fact, damages might include "measures . . . reasonably necessary to re-secure the data, program, system or information from further damage."

31. In *L-3 Communications Westwood Corp. v. Robichaux*, 2007 WL 756528 (E.D. La., March 8, 2007), the court concluded that loss of trade secrets and lost profits did not constitute “loss” within the meaning of § 1030 unless the loss stemmed from damage to or inoperability of a computer system. In dicta it implied the costs incurred while investigating the loss of trade secrets might not be compensable. The plaintiff had alleged that two of its former employees had inappropriately copied proprietary information from their laptops to an external hard drive and used the information to establish a competing venture. The court found that the loss of trade secrets and related profits would not constitute loss, reasoning that lost revenue is recoverable only where connected to an interruption of service. It added that costs not related to computer impairment or computer damages are not compensable under the CFAA.
32. *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393 (2d Cir. 2004). Plaintiff is a Register of domain names in the world wide web and for this purpose maintains a website maintaining domain name information. Defendant competes with plaintiff in the business of website design and development. To facilitate its pursuit of customers, it undertook to obtain daily updates of database information relating to newly registered domain names on the plaintiff’s website. It devised an automated software program or robot which each day submitted multiple successive queries through lawful authorized accesses of various registrars. The Court denied the plaintiff’s CFAA claim, finding that it could not establish the requisite \$5,000 loss since the only evidence was that plaintiff had demonstrated a slight diminishment in capacity, the possibility of diminishment and response time to customer’s queries, and the high probability that other entities not party to the suit would engage in similar conduct if the conduct were permitted.
33. *Nexans Wires, S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468 (S.D.N.Y. 2004). In this case, plaintiff Wiring Cable Industry Company alleged that its defendant competitor induced two of its employees to access computers owned by one of plaintiff’s customers, steal the plaintiff’s proprietary information and download it to their homes. The Court dismissed the Complaint for failure to establish the requisite “loss” under the statute. The only loss plaintiff proved was two trips from Europe to the United States by plaintiff’s sales representatives and could not prove that the trips were sufficiently connected to repair or remediation of the computers.
34. *Resdev LLC v. Lot Builders Association, Inc.*, No. 6:04-CV-1374 ORL 310AB, 2005 WL 1924743 (M.D. Fla. Aug. 10, 2005). Two principals of defendant acknowledged that after leaving plaintiff’s employ, they visited its website and were able to access information that was not password protected. Plaintiff sued, and alleged a loss of \$150,000 as a result of defendant’s access to its database. The Court ruled that the alleged evidence related to “damages,” but there was not real effort to establish “loss” within the meaning of the statute, and therefore the claim was dismissed.
35. *In re Pharmatrak, Inc. Privacy Litigation*, 220 F. Supp. 2d 4 (D. Mass. 2002). Internet users brought class action against web monitoring company and pharmaceutical companies, alleging that defendants secretly intercepted and accessed their personal information through the use of “cookies” and other devices in violation of state and federal law. The Court rejected a wiretap claim because the pharmaceutical defendants

had contracted with the monitoring company to obtain data regarding their websites and had the code placed on their websites, thereby bringing the web monitoring company into the statutory exception for consent. The Court rejected a Stored Communications Act claim because plaintiff's computers were not facilities which provided electronic communication services. The Court rejected the CFAA claim because plaintiffs did not allege that their computers were physically damaged in any way or that they suffered any damage resulting from the repair or replacement of their computer system.

36. *In re America Online, Inc. Version 5.0 Software Litigation*, 168 F. Supp. 2d 1359 (S.D. Fla. 2001). The court found that a complaint stated a claim under 18 USC §1030(a)(5)(A) when AOL exceeded authorized access by transmitting damaging information through its 5.0 program. Consumers could aggregate their damages for purposes of the \$5,000.00 damage requirement in 18 USC §1030(e)(8). An ISP competitor had standing to sue for damages based on AOL's interference with its relationships with existing and prospective subscribers and the increased time spent by the competitor technical support personnel in dealing with AOL 5.0 problems. The court also found that the competitor had lost a "thing of value" for purposes of 18 USC §1030(a)(4) based upon the alienation of its existing or potential customers and for damages to its good will and reputation.
37. *Thurmand v. Compaq Computer Corp.*, 171 F. Supp. 2d 667 (E.D. Tex. 2001). A plaintiff class sought damages from Compaq under the Computer Fraud and Abuse Act for manufacturing and installing faulty floppy diskette controllers on their computers. In determining whether plaintiffs could establish "damage" within the meaning of 18 U.S.C. §§1030(a)(5)(A) and 1030(e)(8). The court held that plaintiffs would be required to establish \$5,000.00 of damage to each computer owned by a class member and that class members could not aggregate their damages.