

**Computer Technology Law Conference
Seattle, Washington, December 13-14, 2007**

Brent Caslin
Kirkland & Ellis LLP
777 South Figueroa, Floor 37
Los Angeles, CA 90017

bcaslin@kirkland.com
Telephone: 213-680-8454
Facsimile: 213-680-8500

Introduction

This brief paper introduces the Computer Fraud & Abuse Act, contains the text of the statute, and summarizes recent case law applying the CFAA's \$5,000 damages floor and interpreting the statutory requirement that, to trigger the CFAA, conduct accessing or damaging a protected computer must be done "without authorization."

Short Summary of the CFAA and Recent Trends

The CFAA was the first federal computer crime statute in the United States. When enacted in 1984 (reportedly by a group of lawmakers unnerved by the Matthew Broderick movie *War Games*), the CFAA protected a narrow class of computers used by the federal government and interstate financial institutions from those who might access or damage those computers without authorization. The statute was expanded slightly in 1986 but remained a criminal statute until the 1990s, when Congress authorized civil remedies for violations of the CFAA. The 1996 change was the most dramatic, altering the CFAA's scope to cover "protected computers" and defining that phrase as broad as constitutionally possible to include any computer "used in interstate or foreign commerce or communication." The definition remains expansive to this day and, with the ubiquity of the Internet and on-line technology in general, covers almost every computer attached to some form of network.

The expanded CFAA sat quietly for half a decade. But, at about the turn of the century, employers began using its civil provisions against employees who had "without authorization" accessed proprietary information from the employer and, using some electronic method (email, instant messaging, snap servers, compact discs, data sticks, on-line data links), misappropriated the information, usually by delivering it to the employee's new employer. It is a surprisingly common fact pattern and the number of civil CFAA claims filed with the federal courts has increased since 2000.

Following the text of the CFAA immediately below is a series of case summaries that reflect the on-going debate among federal courts as to whether the CFAA should apply to employees and former employees who access proprietary company information on a protected computer for an improper purpose, such as copying it for use with a competing firm. One line of cases holds that the employee, under traditional rules of agency, loses authorization when he acts adverse to the interests of his employer. Without authorization, the employee's mere access of electronic data on a networked computer could trigger the CFAA. The second line of cases interprets the statute literally, finding no cause of action

where an employee with authorized access simply accesses information, even if for nefarious purpose.

There is some good news in this for employers who would like to utilize the CFAA -- the federal courts appear to agree that an employee not authorized to damage a protected computer violates the CFAA if he destroys or deletes data on a protected computer. Thus, an employee who steals information might avoid liability under the CFAA for simply accessing and copying proprietary information, but will have violated the statute if he attempted to cover his tracks by deleting electronic files evidencing his access.

The Computer Fraud & Abuse Act

18 U.S.C. § 1030

(a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the

United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;

(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 (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;

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

(iii) physical injury to any person;

(iv) a threat to public health or safety; 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 section 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; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause

damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is--

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds \$5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(4)(A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and

(5)(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and

(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.

(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014 (y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(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--

(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, 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;

(3) the term “State” includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term “financial institution” means--

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;

(5) the term “financial record” means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(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 accessor is not entitled so to obtain or alter;

(7) the term “department of the United States” means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8) the term “damage” means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term “government entity” includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10) the term “conviction” shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(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.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(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 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.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

Recent Case Law Interpreting Civil Liability Under the CFAA.

Broad Interpretations of “Without Authorization”

Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000). Shurgard alleged rival Safeguard hired away key employees to misappropriate Shurgard’s confidential business plans, contacts, and potential business locations. According to Shurgard, the employees began working for the competition while still employed by Shurgard and, key to the CFAA claims, accessed and emailed confidential information from Shurgard’s computers to Safeguard. Among others, Shurgard brought claims under CFAA Sections 1030(a)(2)(C) (accessing a computer without authorization) and 1030(a)(4) (accessing a computer with intent to defraud). Safeguard moved to dismiss the complaint but, relying on traditional agency principles, the District Court held the employees lost authorization to access Shurgard’s computers when they accessed the company’s computers for the purpose of stealing trade secrets. The court also held that the former employees’ conduct, if true, constituted “fraud” because the CFAA’s fraud provision should be read broadly to include wrongdoing by dishonest schemes or methods, in addition to classic fraud. Finally, on the issue of “damage,” the Court again interpreted the statute broadly, finding its reference to damage as “any impairment to the integrity . . . of data . . . or information” included the alleged access and disclosure of information Shurgard claimed to be trade secrets.

International Airport Centers v. Citrin, 440 F.3d 418 (7th Cir. 2006). This Seventh Circuit decision is a leading case for employers seeking to use the CFAA against former employees who use company computers to misappropriate information and it deserves special attention.

In Citrin, the plaintiffs alleged Citrin was a leading manager and partial owner of IAC, a real estate business focused on airport related properties. Citrin was tasked by IAC with identifying potential investment properties for the company. According to the plaintiffs, Citrin defrauded IAC by using company resources, including a laptop computer and a snap server, to purchase properties for the benefit of another company formed by Citrin. Citrin allegedly acted with the intent to misappropriate IAC’s business opportunities and trade secrets. The plaintiffs also alleged, among other things, that Citrin breached obligations to IAC by failing to carry out his ordinary employment responsibilities, such as attending company meetings and abiding by company policies.

According to the plaintiffs, after the relationship between Citrin and IAC fell apart, Citrin used a secure delete computer program to permanently erase all information from his company assigned laptop computer and the snap server. As a result, claimed the plaintiffs, IAC was unable to access information that had value to the company and could have been used to prove Citrin’s misconduct. Citrin denied the allegations of the lawsuit but admitted he had used an erase program to wipe clean the laptop computer and snap server.

In the District Court, the presiding judge was asked to dismiss the CFAA cause of action against Citrin on the grounds that his alleged deletion of materials on his individual laptop and the backup server were not a “transmission” of computer code under the CFAA.

Believing the purpose of the CFAA was to thwart computer hackers and protect data network systems, the District Court ruled Citrin's use of a computer program to delete his individual files did not violate the CFAA. The Court wrote that it would not "expand the scope of the" CFAA to cover the facts alleged against Citrin. In other words, the District Court dismissed the claim, refusing to apply the CFAA to an individual's unauthorized secure deletion of files on a company assigned laptop computer and snap server. IAC appealed the dismissal.

Transmission. Richard Posner wrote the Citrin opinion for the Seventh Circuit Court of Appeals. He focused on the precise language of the CFAA. In simple, straight forward terms, ruled the Court, that language prohibited the "transmission" of a "program, information, code, or command" that intentionally causes "damage" to a protected computer. The precise mechanics of the transmission effected by Citrin were irrelevant, held the Court - a transmission under the CFAA can be accomplished by an on-line technology but also through the use of a disk or a physically attached computer cable. Any such transmission violated the statute, decided Judge Posner. Assuming the plaintiffs' allegations as true, he ruled they had properly plead a transmission under the CFAA.

Without Authorization. The Court of Appeals also determined Citrin lost the protections of his employment contract (which gave him certain rights to delete data) and his status as an authorized employee when he breached his fiduciary obligations to IAC. As a result, according to the Court of Appeals, under the facts as plead, Citrin's access to the laptop and snap server for the purpose of misappropriating or damaging data was unauthorized by IAC. Citrin's motion should have been denied, and the case was sent back to the District Court.

ViChip Corp. v. Lee, 438 F. Supp. 2d 1087 (N.D. Cal. 2006). This decision also addressed the "without authorization" issue addressed in Citrin and is worth noting because with it the District Court granted summary judgment in favor of a CFAA claim. The facts of the case are fairly complicated and involve international trade but, generally, ViChip's Board of Directors suspected their president, Lee, was engaged in a series of improper transactions and asked him to step down. Lee apparently responded by taking ViChip files and deleting others from company computers. He was quickly fired by ViChip and, within a few weeks, Lee filed a series of patent applications claiming ownership of technology allegedly developed and owned by ViChip. ViChip and Lee then brought claims against each other, including a CFAA claim by ViChip against Lee under CFAA Sections 1030(a)(5)(A-B) (transmitting a program that damages a protected computer). Lee disputed that he could have caused damage to company computers "without authorization" when he was technically still an officer and director of ViChip. Relying on Citrin, however, the District Court had little trouble finding Lee broke his agency relationship with ViChip when he broke his duty of loyalty to the company by misappropriating and deleting information from ViChip computers. With his agency relationship gone, held the Court, Lee lost all authorization to access the files he accessed and damaged and thus his conduct was prohibited by the CFAA.

United States v. Phillips, 477 F.3d 215 (5th Cir. 2007). The defendant in this case was a student at the University of Texas. Like all UT students, Phillips signed a "terms of use"

agreement with the University in which he promised not to use the school's network to perform port scans. Nevertheless, shortly after arriving at UT, Phillips began using his UT account to scan and steal information from unprotected computers on and off the UT network. Phillips accumulated a database of credit card numbers, bank account information, social security numbers. His efforts crashed the UT network several times. After the Secret Services was called to help UT, an investigation led to Phillips and he was charged with a series of crimes, including violations of CFAA Section 1030(a)(5)(A)(ii) (intentionally accessing a protected computer without authorization and recklessly causing damage). After he was convicted, Phillips appealed to the Fifth Circuit on the grounds, among several others, that he did not access the UT server "without authorization", but the Circuit Court affirmed the conviction because Phillips' access was in no way related to the intended function of his authorization. The Court found no reasonable user could believe they were permitted to access, view, and use areas of the network Phillips used and thus Phillips did not have authorization for his access. The CFAA conviction was affirmed.

Forge Industrial Staffing, Inc. v. De La Fuente, 2006 WL 2982139 (N.D. Ill. 2006). De La Fuente, the defendant in this case, was employed by Forge but demoted and then placed under investigation by the company. When Forge asked De La Fuente for his company issued laptop computer, he refused to turn it over initially. The next day, when De La Fuente returned his laptop, a forensics expert was hired to examine the laptop and allegedly learned from files found on the laptop that De La Fuente was setting up a competing business using Forge's confidential information. Much of the data on the laptop, according to the expert, was impaired, altered, and destroyed. Forge brought claims against De La Fuente, among them claims under the CFAA. De La Fuente moved to dismiss the CFAA claims with two arguments (i) that Forge had not satisfied the \$5,000 floor; and (ii) De La Fuente had not acted without authorization because he was authorized to access the data he allegedly accessed. The District Court easily found that Forge had satisfied the \$5,000 damage requirement with its pleading that the forensic examination of De La Fuente's computer cost more than \$5,000. On the second issue, relying on Citrin, the District Court ruled that De La Fuente had acted without authorization because his authorization to delete data from the company's laptop computer ended when he began engaging in misconduct in violation of his duty of loyalty to Forge. The Court expressly decided not to follow Lockheed, discussed below, on the ground that it was bound by the Seventh Circuit's decision in Citrin.

Hewlett-Packard Company v. Byd:Sign, Inc., 2007 WL 275476 (E.D. Tex. 2007). HP alleged that a group of former employees, who had agreed to keep HP's information confidential and not work for personal gain or an HP competitor, utilized HP computers, email, and instant messaging technology to misappropriate confidential HP information and set up competing business ventures. The employees also allegedly "scrubbed" HP computers clean of incriminating evidence. After discovering the employees' acts, HP brought a series of claims against them and their new firms, including claims under the CFAA. The defendants moved to dismiss HP's CFAA claims on the ground the employees did not act without authorization when they accessed HP data. The Court addressed the division between Citrin / Shurgard and the Lockheed case discussed below, but avoided the Lockheed decision by pointing to the employees' agreements not to access or use HP information for

personal gain or to support a competing firm. Because the employees had made these promises, ruled the court, the employees had acted in breach of contract and without authorization. The Court also noted that the scrubbing allegations constituted damage to HP's computers, according to the pleadings, and there was no claim the defendants were authorized to damage HP's computers. The defendants' motion to dismiss the CFAA claims was denied.

Narrow Interpretations of "Without Authorization"

Lockheed Martin Corp. v. Speed, 2006 WL 2683058 (M.D. Fla. 2006). In this case, a Lockheed program manager named Speed managed a billion dollar military contract. As the first phase of the contract ended, and the second was about to be awarded, Speed and two other Lockheed employees left Lockheed to work for a competitor, L-3 Communications. Before they left Lockheed, the three employees allegedly downloaded a large number of confidential files to hundreds of compact discs. Lockheed brought several claims against the employees, including some under the CFAA. With a motion to dismiss, the defendants argued (i) Lockheed had not suffered an injury as required by CFAA Section 1030(g); (ii) the employees had not acted without authorization or in excess of their authorization; (iii) Lockheed had not alleged "damage" as required by Section 1030(a)(5)(A)(i); and (iv) Lockheed's Section 1030(a)(5)(A)(ii) claim was improper because the employees did not act without authorization and did not cause damage.

Loss. The District Court noted the loss of trade secrets alone is not a damage or loss under the CFAA, but ruled that Lockheed alleged it incurred costs responding to the offenses and conducting damages assessments, satisfying the Section 1030(g)'s "loss" requirement.

Without Authorization. On the authorization issue, the District Court expressly declined to follow the Shurgard and Citrin line of cases, reasoning that those courts improperly relied on extrinsic evidence (rules of agency) to interpret the CFAA. The Lockheed court held that, because the accused employees were authorized by Lockheed to access the information they accessed when they accessed the information, they in fact had authorization to access the information. The Lockheed decision went to great lengths to explain the errors of Citrin and Shurgard but, at bottom, simply disagreed with the agency logic in Citrin and Shurgard that an employee who begins to act adversely to his employer acts without authorization for purposes of the CFAA.

Damage. Addressing Lockheed's claim under Section 1030(a)(5)(A)(ii), the Court found that, while Lockheed had alleged a loss, it had not alleged "damage" because the mere copying of files from its computers did not result in any actual damage to Lockheed's computers. The defendants motions to dismiss were granted.

Lockheed v. L-3 Communications Corp., 2007 WL 560004 (M.D. Fla. 2007). Lockheed moved for reconsideration of the order dismissing its CFAA claims against Speed and L-3 in light of the Fifth Circuit's decision in Phillips (discussed above). The District Court denied the motion, however, finding the facts of Phillips much different from the situation before the District Court in Florida. In its decision, the District Court returned to its plain interpretation

of the CFAA, reiterating that Lockheed's former employees were in fact authorized to access the information they accessed and thus they could not have violated the CFAA, which requires unauthorized access.

Brett Senior & Associates v. Fitzgerald, 2007 WL 2043377 (E.D. Penn. 2007). In this case, a law firm employee named Fitzgerald responsible for certain tax, accounting, and financial services left his firm to work for an accounting firm. As Fitzgerald left, he allegedly used his computer to copy several client files and engagement letters. The former employer, BSA, brought claims against Fitzgerald for violations of the CFAA and various state laws, including trade secret misappropriation. Fitzgerald eventually brought a motion for summary judgment and, ruling on that motion, the District Court decided an employee authorized to access certain files does not violate the CFAA if he or she accesses them for an improper purpose. In other words, the court sided with Lockheed not Citrin.

B&B Microscopes v. Armogida, 2007 WL 2814595 (W.D. Penn. 2007). In this case, Armogida was an imaging specialist for high-end microscope manufacturer B&B. At some point in time, Armogida was asked with all other employees to submit his company-issued laptop for an upgrade, but delayed for more than a day to delete a large number of files from the computer. Armogida soon left B&B and allegedly began selling one of its more sophisticated products on his own. He sold a few models and created new sales materials that did not mention B&B. After discovering Armogida's misconduct, B&B sued Armogida for various legal violations, including claims under the CFAA. Armogida raised the "without authorized" issue addressed in Lockheed, claiming he could not be liable for unauthorized access under CFAA Section 1030(a)(5)(A)(ii) because he was in fact authorized to access the information he allegedly accessed while employed by B&B (even if he had an improper motive for that access). On this point, the District Court agreed with Armogida and Lockheed, and disagreed with Citrin. The unauthorized access precluded a CFAA claim under CFAA Sections 1030(a)(5)(A)(ii) or (iii). The District Court went one step further, however, agreeing with B&B's claim that Armogida had caused damage without authorization when he deleted several files from that computer. As a result, the CFAA Section (a)(5)(A)(i) claim against Armogida was found appropriate.

Diamond Power Int'l, Inc. v. Davidson, 2007 WL 2904119 (N.D. Ga. 2007). Diamond Power and Bergemann, Inc. are the two leading manufacturers of soot blowers, which are large machines designed to clean massive industrial coal-fire boilers. The case began when Bergemann hired Davidson away from Diamond Power. As he left Diamond Power for its chief competitor, Davidson allegedly used his high-level access to Diamond Power's computer networks to download significant financial and product data, which he subsequently provided to Bergemann. Diamond Power brought substantial claims against Bergemann and Davidson, including CFAA claims and trade secret misappropriation claims. On summary judgment, the District Court recounted significant misconduct by Davidson and confirmed the viability of the trade secret claims against him and Bergemann, but dismissed Diamond Power's CFAA claim on the ground that Bergemann had authorization to access the information he alleged accessed (and allegedly misappropriated). Recognizing the split in authority on this point, the Court decided to follow the Lockheed line of cases over Citrin

and Shurgard. The CFAA claim was dismissed as improper in light of Davidson's access authorization.

The CFAA's \$5,000 Damages Floor

United States v. Middleton, 231 F.3d 1207 (9th Cir. 2000). The defendant in this case worked for Slip.net but, after leaving the firm, used his knowledge of its computers to hack into Slip.net's network. The defendant accessed email accounts, altered the company's registry, changed administrative passwords, and deleted a billing system as well as two other databases. The defendant argued the statute did not protect corporations, only individuals, and that the government did not prove damages meeting the statute's \$5,000 damages floor. In a thorough analysis of the CFAA, the Ninth Circuit confirmed it covers business entities as well as individuals. It also held the statute's \$5,000 damages threshold was met because the government introduced evidence that Slip.net employees had spent significant time investigating and repairing the damage caused by the defendant and taking measures to prevent future break-ins. The case confirms that internal employees' time can be considered (not just vendors who charge a specific price) when aggregating damages under the CFAA and that the figure may include the cost of repairing the injury caused by the defendant as well as preventing future similar attacks.

United States v. Millot, 433 F.3d 1057 (8th Cir. 2006). The defendant here was a systems analyst for Aventis. He left the company when his job was outsourced to IBM but retained, apparently without authorization, a SecureID remote access card and later used that access device to break into the company's network and delete at least one individual's email account. IBM and Aventis introduced evidence that their employees spent considerable time repairing the network but the defendant challenged the prosecution's use of the company employees' time to satisfy the CFAA's \$5,000 damages requirement. As with Middleton, the District Court and the Court of Appeal confirmed the use of internal employee time is appropriate to satisfy the floor and that the employees' time may include the cost of assessing the damage, restoring the system, and verifying the security of the system.

Forge Industrial Staffing, Inc. v. De La Fuente, 2006 WL 2982139 (N.D. Ill. 2006). De La Fuente, the defendant in this case, was employed by Forge but demoted and then placed under investigation by the company. When Forge asked De La Fuente for his company issued laptop computer, he refused to turn it over initially. The next day, when De La Fuente returned his laptop, an expert was hired to examine the laptop and allegedly learned from files found on the laptop that De La Fuente was setting up a competing business using Forge's confidential information. Much of the data on the laptop, according to the expert, was impaired, altered, and destroyed. Forge brought claims against De La Fuente, among them claims under the CFAA. De La Fuente moved to dismiss the CFAA claims on the ground, among others, that Forge had not satisfied the \$5,000 floor. The District Court easily found that Forge had satisfied the \$5,000 damage requirement with its pleading that the forensic examination of De La Fuente's computer cost more than \$5,000.