

**A PRACTITIONER’S GUIDE TO THE COMPUTER FRAUD AND ABUSE ACT:
FINALLY, A CAUSE OF ACTION FOR “ANYTHING WRONG” (OVER \$5000)
By: Gregory C. Cook and Will Hill Tankersley, Jr.¹**

Because of the immense explosion of computer use and the internet over the last five years, as well as certain recent amendments, the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030 now provides a powerful tool in private litigation for persons or businesses injured by, among others, former employees, hackers, spammers and perhaps many others. The CFAA generally prohibits (1) the unauthorized accessing (2) of a “protected” computer (3) with the intent either (a) to obtain information, (b) to further a fraud, or (c) to damage the computer or its data.

I. History

The CFAA began in 1984 as a criminal statute to protect classified information in government computer systems. Over the years, Congress gradually expanded its reach. In 1994, Congress added, for the first time, a private right of action (18 U.S.C. § 1030(g)), providing both compensatory damages and injunctive relief. Even more significantly, Congress amended the CFAA in 1996 to cover computers “which [are] used in interstate or foreign commerce or communications” by defining such computers as “protected” computers.² The growth of the internet has made nearly all computer use interstate in nature and thereby subject to the CFAA.³

II. Prohibited Acts Under CFAA⁴

A. Unauthorized access

The CFAA criminalizes (and provides a civil remedy for such criminal violations) a variety of acts involving computers. First, section 1030(a)(2) provides that it is a crime (1) to obtain information (2) by intentionally accessing (3) a protected computer (4)

without authorization (or “exceeds authorized access”).⁵ For instance, under section 1030(a)(2)(A), it is a crime to obtain information from the records of financial institutions, card issuers, or consumer reporting agencies. More important, however, is section 1030(a)(2)(C), which **makes it a crime to obtain information from any “protected” computer if the conduct involves interstate or international communication.**

B. “Further[.]” a “fraud”

Second, section 1030(a)(4) establishes that it is illegal (1) to intentionally further a fraud or obtain anything of value (2) by knowingly accessing a protected computer (3) without authorization (or in excess of “authorized” access). However, there is no violation if the thing obtained is only the use of the computer and that use is worth less than \$5,000 in any one-year period. Notably, at least one decision has held that “fraud” in the context of the CFAA does not necessarily require the showing of the traditional elements of common law fraud, but rather requires “wrongful action.”⁶

C. “Damage” a “protected computer”

Third, section 1030(a)(5) makes it a crime (1) to intentionally cause (2) “damage” (3) to a “protected” computer. “Damage”, defined in § 1030(e)(8) includes, among other things, (A) “loss aggregating at least \$5,000 in value during any 1-year period”, (B) modification or potential modification of medical diagnosis or treatment, (C) physical injury to any person, or (D) threatened public health or safety. For instance, under section 1030(a)(5)(A), it is unlawful to intentionally cause damage to a protected computer by knowingly transmitting a destructive program. Likewise, under section 1030(a)(5)(C), it is unlawful to cause damage to a protected computer by intentionally

accessing it without authorization. The effect of section 1030(a)(5)(C) is to create a strict liability standard for the resulting damage as long as the unauthorized access was intentional.⁷

D. “Traffic” in computer passwords

Fourth, section 1030(a)(6) makes it illegal (1) to knowingly traffic (2) in computer passwords in certain situations. Under section 1030(a)(6)(A) and (B), it is illegal to affect interstate or foreign commerce by knowingly trafficking in computer passwords with the intent to defraud or to knowingly traffic in passwords to government computers with the intent to defraud.

E. “Transmits” a threat to “damage” a “protected computer”

Finally, section 1030(a)(7) makes it unlawful (1) to transmit (2) any threat to damage (3) a “protected” computer (4) in interstate or foreign commerce (5) with the intent to extort anything of value.

III. Punishment and Enforcement

Sections 1030(b)-(c) set forth the various criminal punishment guidelines under the CFAA. These provisions vary the fines and imprisonment terms according to which provision of section 1030(a) is violated and whether it is a first offense. Section 1030(d) grants authority to the United States Secret Service to enforce the CFAA. Section 1030(f) prevents enforcement of the CFAA against the lawful activities of other law enforcement agencies.

IV. Civil Remedies

Section 1030(g) expressly provides the civil remedy (and thus federal court subject matter jurisdiction) for violation of the CFAA to any person who suffers “damage

or loss” from a violation of the CFAA. The aggrieved person may obtain compensatory damages and injunctive or other equitable relief. However, only economic damages are available for the type of aggregate financial damages specified in section 1030(e)(8)(A). The statute of limitations for civil actions under the CFAA is two years from the discovery of the damage.

As discussed below, the strongest debate in the developing CFAA caselaw appears to focus upon the \$5,000 jurisdictional limit – that is, whether a civil plaintiff must satisfy \$5,000 “damage” for all claims under the CFAA and what type of damages may satisfy this limit.

V. Application of the CFAA

The caselaw applying the CFAA in light of the key 1996 and 1994 amendments is just now beginning to emerge. The following section illustrates the application of the CFAA but should not be read as limiting the scope of its potentially large application.

A. Departing employee – loses authorization

An employee likely loses his status as an “authorized” user of a computer when he acts as an agent of a competitor. In one of the best discussions of the history of the CFAA, the court in Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F.Supp.2d 1121, 1124 – 5 (W.D.Wash. 2000), addressed just such a situation. There the key employees of plaintiff, Shurgard, were hired away by defendant, Safeguard. Plaintiff alleged that some of those key employees e-mailed trade secrets to defendant while still employed by plaintiff. The court, in rejecting a motion to dismiss, held that the employees may have ceased to be authorized users when they began acting for the benefit of another. The court relied on, among other things, the decision in United States v.

Morris, 928 F.2d 504, 510 (2nd Cir. 1991), where a computer user, who had authority to access a computer, became unauthorized when he used the computer in an unauthorized way. Likewise, the court cited United States v. Galindo, 871 F.2d 99 (9th Cir. 1989), where an employee of a jewelry store stole company mail that she was authorized to pick up. There, the employee forged a signature to conceal her receipt of the mail, and the court held that the employee was not an agent of the jewelry store when she used fraud to obtain the mail. The Shurgard court also cited Restatement (Second) of Agency §112 (1958). Presumably, there will be increased use of the CFAA for departing employees who (since almost everything in business is now computerized) often use computerized information when they leave or are preparing to leave their employer.

B. What is “exceeds authorized access” - Spammers

A key area of litigation under the CFAA appears to relate to “Unsolicited Bulk E-mail” (“UBE”), also known as “spam.”⁸ Decisions regarding spam have varied and no consensus appears to have yet emerged. For instance, in America Online, Inc. v. National Health Care Discount, Inc., 121 F.Supp.2d 1255, 1273 (N.D.Iowa 2000), a bonafide user of America Online (AOL) obtained addresses for spam in violation of AOL’s “Terms of Service” and “Rules of the Road”. The court refused to grant summary judgment to AOL on its claim under section 1030(a)(2)(C) or 1030(a)(5), noting that violations of “Terms of Service” and “Rules of the Road” agreements by an “insider,” or otherwise authorized user, may not automatically render that person’s access unauthorized under the CFAA. The National Health court was also not certain that the CFAA was intended to apply to UBE or “spam” at all. The court based this concern on Congressional reluctance to enact sweeping computer crime legislation.⁹

In addition, the court raised concerns that AOL may not have suffered sufficient damages, construing “damage” under the CFAA narrowly to mean injury to the specific computers or data, ruling that such an “impairment” must be shown to have directly caused the required \$5,000 injury (apparently recognizing a distinction between the term “damage” which is such an “impairment” and must be shown for jurisdictional purposes and the term “loss” which can be the measure of recovery). Likewise, the National Health court apparently held that the \$5,000 damage requirement applied to all portions of the CFAA, even those portions of the CFAA that do not expressly reference “damage” or mention a \$5,000 limit (such as section 1030(a)(2)). Other courts have also wrestled with these questions (generally holding that all private claims under the CFAA are subject to the \$5,000 requirement but appearing to differ on whether an “impairment” to the computer or data must be shown for every CFAA claim and what can constitute “damage” or “loss”). In general, these damage questions remain the key point of debate in most CFAA reported decisions.¹⁰

In contrast, in America Online, Inc. v. LCGM, Inc., 46 F.Supp.2d 444, 450 (E.D.Va. 1998), the court held that violations of “Terms of Service” and “Rules of the Road” agreements by spammers do render otherwise authorized access unauthorized. There, the defendants admitted to maintaining an AOL membership and using extraction software to harvest e-mail addresses of AOL members. Plaintiff, AOL, estimated that defendant sent ninety-two million UBE messages. The court granted summary judgment for AOL on claims under sections 1030(a)(2)(C) and 1030(a)(5)(C). Under section 1030(a)(2)(C), it is a crime to obtain information from any protected computer by unauthorized access if the conduct involves interstate or international communication.

Under section 1030(a)(5)(C), it is unlawful to cause damage to a protected computer by intentionally accessing it without authorization. The court held defendants' actions were unauthorized because they violated the "Terms of Service" agreements.

Several other courts have awarded both monetary damages and preliminary injunctions against producers of UBE or spam. In America Online, Inc. v. Prime Data Sys., Inc., 1998 U.S. Dist. LEXIS 20226 (E.D. Va.), the court accepted a Magistrate's recommendation to award \$101,400 in compensatory damages to AOL against a spammer based upon a computation of 130 million UBE messages multiplied by an estimated cost per message of \$.00078. Likewise, in HotMail Corp. v. Van Money Pie, Inc., 1998 U.S. Dist. LEXIS 10729 (N.D. Cal.), the court granted preliminary injunctions against the defendant based on the substantial likelihood that HotMail would prevail on its CFAA claims.

C. Hackers

Courts have demonstrated a willingness to issue injunctions under the CFAA to prevent damage to computer systems by hackers. For instance, in YourNetDating, LLC v. Mitchell, 88 F.Supp.2d 870 (N.D.Ill, 2000), a former employee of an online dating service hacked into plaintiff's website and created a "blind link" to another site. A "blind link" is a link that does not allow the viewer to return to the original site. The court granted an injunction against the defendant because of the potential for damage to the goodwill of plaintiff's services.

D. "Cookies"

"Cookies" are files planted on a user's computer – typically by a visit to a website. At least two CFAA actions have attacked this practice. In In re Intuit Privacy

Litig., 138 F.Supp. 2d 1272 (C.D.Cal. 2001), computer users alleged damage from “cookies” implanted on their computers by Intuit, Corp. The court dismissed plaintiffs’ claims without prejudice because they did not allege sufficiently economic damage.

Likewise, in In re Doubleclick, Inc. Privacy Litig., 2001 U.S. Dist. LEXIS 3598 (S.D.N.Y. 2001), defendant, Doubleclick, installed “cookies” on consumers’ computer systems to gain information about their internet habits for use in advertising. Although the court held that plaintiffs’ remedial expenses could be included in losses under the CFAA, the court still granted defendant’s motion to dismiss based on the holding that expenses could only be aggregated for a single act. The court explained that installing cookies on millions of computers is not a single act. Therefore, the plaintiff had the burden of alleging that Doubleclick’s cookies caused a loss of more than \$5,000 in a one-year period to a single, “particular computer.”

E. Robotic Attacks On Plaintiff’s Computers

In Register.Com, Inc. v. Verio, Inc., 126 F.Supp. 2d 238, 241 (S.D.N.Y. 2000), defendant “spammer” used automated or robotic software to search Register.Com’s WHOIS database to gather contact information such as e-mail and postal addresses. The WHOIS database contains contact information for each customer that registers a domain name with Register.Com. Register.Com did not authorize the use of robotic searches in its WHOIS database. The court found that robotic searches could diminish response time, increase repair costs, cause a loss in good will from customers, and encourage other robotic searches. The court held that these damages were sufficient to sustain a CFAA claim and granted a preliminary injunction against such practices.

F. Harmful Programming Installed by Manufacturers on Plaintiff's Computers

In Shaw v. Toshiba Am. Info. Sys., Inc., 91 F.Supp.2d 926 (E.D. Tex. 1999), purchasers of allegedly defective laptops sued the manufacturer under the CFAA. The manufacturers argued that the CFAA was not meant to include actions against manufacturers. On the manufacturers' motion for summary judgment, the court held that a manufacturer could be liable for the "design, manufacture, creation, distribution, sale, transmission, and marketing" of computer programming that is known to be defective, citing North Texas Preventive Imaging v. Eisenberg, 1996 U.S. Dist. LEXIS 19990 (C.D. Cal. 1996). In that case, a software manufacturer installed "time bomb" code into the program to disable the computer system at the end of the contract period, and the North Texas court found that the inclusion of this disabling code in the system's programming constituted a "transmission" under section 1030(a)(5)(A), and defendant manufacturer could be held liable.

In In re America Online, Inc. Version 5.0 Software Litig., 2001 U.S. Dist. LEXIS 6595 (S.D.Fla.), consumers alleged that installation of AOL 5.0 software caused damage to their computer systems. Specifically, their systems were allegedly damaged by denying non-AOL internet access, disrupting Local Area Networks (LANs), and causing system crashes. The court held that these losses could be aggregated to reach the \$5,000 minimum required by section 1030(e)(8)(A) for an action under section 1030(a)(5)(A), rejecting In re Doubleclick, Inc. Privacy Litig. Despite this holding, however, the court dismissed plaintiffs' claims because they had still failed to plead sufficiently in detail the required damage.

G. Credit Reports

In Letscher v. Swiss Bank Corp., 1997 U.S. Dist. LEXIS 7909 (S.D.N.Y.), plaintiff sued his former employer for accessing his credit record without permission. Evidence was introduced to show that defendant erroneously obtained plaintiff's credit report with the belief that plaintiff was a current employee and that a consent form signed by plaintiff while he was an employee was still valid. The court held that a claim under the CFAA requires intent to access information without authorization and "is not designed to reach 'mistaken, inadvertent, or careless acts of unauthorized access.'"

Likewise, in LeBlanc v. Allstate Ins. Co., 2000 U.S. Dist. LEXIS 9351 (E.D. La.) the court, granting defendant's motion for summary judgment, held that the defendant insurance company was not liable for accessing plaintiffs' credit reports for use in litigation where the written authorizations signed by plaintiffs used expansive language. The court held that the authorization was sufficiently broad, and there was no evidence that defendants intended to access the credit reports without authorization.

CONCLUSION

The CFAA provides a powerful new tool in private litigation for claims that may be difficult to fit within traditional common law torts, and which otherwise would not create federal court jurisdiction. How broad the CFAA will eventually be applied is still unclear, and the debate over the require \$5,000 of "damage" may determine how broad that reach becomes.

¹ The authors wish to thank Ryan M. Spitzer, in his second year at Vanderbilt University Law School, for his invaluable assistance in the researching and writing of this article.

² In addition to computers used in interstate or foreign commerce or communications, a “protected” computer also includes (1) a computer that is exclusively accessed by the federal government or a financial institution, and (2) a computer that is accessed nonexclusively by the federal government or a financial institution if such access is affected by the offending conduct.

³ See generally Stephen R. Buckingham, Court Gives New Use to 1994 Law: Trade Secrets, 2 ILB 498 (2001); America Online, Inc. v. Nat’l Health Care Discount, Inc., 121 F. Supp. 2d 1255, 1275 (N.D. Iowa 2000) (citing S. Rep. No. 104-357 (1996) and H.R. Conf. Rep. No. 103-711 (1994)) (discussing general legislative history).

⁴ This Article will focus on the portions of the CFAA applicable to private rights of action. Thus, it will generally not cover certain portions of the CFAA which criminalize certain acts done to computers associated with the federal government and national defense.

⁵ Section 1030(e)(6) defines “exceeds authorized access” as when a person with authorization “obtains or alter[s] information . . . that the accesser is not entitled so to obtain or alter.”

⁶ Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F.Supp.2d 1121, 1126 (W.D.Wash. 2000).

⁷ Compare 18 U.S.C.S. § 1030(a)(5)(C) with 18 U.S.C.S. § 1030(a)(5)(B); see also America Online, Inc. v. National Health Care Discount, Inc., 121 F. Supp. 2d 1255, 1272 (N.D. Iowa 2000).

⁸ The FTC has dubbed spam “Unsolicited Commercial E-mail” or “UCE.” Complaints regarding such can be made to uce@ftc.gov.

⁹ National Health, 121 F.Supp.2d at 1275 (citing S. Rep. No. 99-432, at § I (1986 WL 31918) (discussing the 1986 amendment to CFAA)).

¹⁰ Compare Moulton v. VC3, 2000 U.S. Dist. LEXIS 19916 (N.D.Ga.) (expenses incurred by defendant to investigate plaintiff’s actions could not be included in the computation of damages towards \$5,000 requirement); In re Doubleclick, Inc. Privacy Litigation, 2001 U.S. Dist. LEXIS 3498 (S.D.N.Y.) (\$5,000 requirement applies to all private claims; cost to remedy computers and data can be considered; loss of privacy and value of advertising gained by plaintiff cannot be recovered; aggregation to meet \$5,000 requirement is only allowed for multiple victims based upon a single act to a single computer); Hotmail Corp. v. Van Money Pie, Inc., 1998 U.S. Dist. LEXIS 10729 (N.D.Cal.) (holding that delay in rendering computer services could constitute “damage”); In re Intuit Privacy Litigation, 138 F.Supp.2d 1272 (C.D.Cal. 2001) (holding that a private plaintiff could allege noneconomic damage as long as it fit within the alternative definitions of damage in section 1030(e)(8)(B), (C) or (D)); In re America Online, Inc. Version 5.0 Software Litigation, 2001 U.S. Dist. LEXIS 6595 (S.D.Fla.) (allowing aggregation of multiple acts and rejecting Doubleclick).