THE COMPUTER FRAUD AND ABUSE ACT: AN UNDERUTILIZED LITIGATION WEAPON

Audra Dial and Daniel G. Schulof[1]

To combat increasingly common computer-related crimes, Congress enacted "The Counterfeit Access Device and Computer Fraud and Abuse Act" (the "CFAA") in 1984. Although the legislation originally imposed only criminal liability and provided protection only with respect to a limited group of government-operated computers, Congress amended the CFAA in 1986, 1994, 1996, 2001, and 2002, gradually adding protection for privately-maintained computers and incorporating civil remedies.

The CFAA currently prohibits any person from, among other acts: (a) "access[ing] a protected computer without authorization" so as to perpetuate a fraud and "obtain anything of value"; (b) knowingly "caus[ing] the transmission of a program, information, code or command" so as to intentionally cause damage to a protected computer; (c) accessing a protected computer without authorization, in a manner that causes "damage" to the computer; or (d) causing damage to a protected computer through the unauthorized transmission of computer passwords.[2]

A "protected computer" is broadly defined as any computer "used in interstate or foreign commerce or communication."[3] The term "damage" is defined as any act that causes "impairment to the integrity or availability of data, a program, a system or information."[4] The statute expressly recognizes a civil cause of action for compensatory damages or injunctive relief by a person who "suffers damage or loss by reason of a violation of the [Act]."[5]

Over the past thirty years, all fifty state legislatures have enacted similar computer crime statutes.[6] As with the CFAA, these state statutes are triggered where a would-be defendant improperly accesses a computer. "Access without authorization," "unauthorized access," and "exceeding authorized access" are the terms most commonly used to define the type of computer access which runs afoul of these various statutes.[7]

[1] Ms. Dial is a partner and Mr. Schulof is an associate with Kilpatrick Stockton LLP's Technology Litigation Team and are based in the firm's Atlanta office.

[2] 18 U.S.C. § 1030 ("CFAA").

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1615 (2003).

[7] *See id.*

Because courts have generally interpreted these terms very broadly, civil actions based on the CFAA and its state analogues are powerful weapons for business litigators. This article summarizes the civil actions available under these computer crime statutes, highlights why they are particularly effective tools for civil litigators, and explains how they can be utilized in conjunction with other civil causes of action.

Threshold Issues

Actions brought under the CFAA are subject to a two-year limitations period.[8] Courts have recognized that the statute's text is not clear as to whether the limitations period accrues immediately upon a plaintiff's discovery of the damage underlying its claim or upon discovery of *both* the underlying injury *and* the identity of its perpetrator.[9] At least one court has held that the CFAA limitations period accrues before a claimant has discovered all facts necessary to file its claim.[10] In light of this uncertainty, a would-be CFAA plaintiff would be wise to file its claim within two years of discovering the damage caused by a potential CFAA violation.

Because the CFAA is a federal statute, any civil action brought thereunder triggers federal question jurisdiction and may be filed in a federal district court. The jurisdictional element of the CFAA is satisfied by virtue of the requirement that any violation of the Act concern a "protected computer," defined as a computer "used in interstate or foreign commerce or communication."[11] This requirement is easily satisfied, as under this definition "virtually any computer that sends e-mail in the course of its business is a 'protected computer.'"[12]

Furthermore, the physical location of the would-be defendant is unimportant for the purpose of determining jurisdiction under the CFAA. In *U.S. v. Ivanov*, the defendant, acting from his home in Russia, hacked into a company's computer system in Connecticut, obtained various network passwords, and downloaded the passwords onto his computer in Russia.[13] The defendant moved to dismiss the CFAA charges brought against him on subject matter jurisdiction grounds, arguing that charging him under the CFAA would require an impermissible extraterritorial application of the law.[14] The court disagreed and upheld the indictment, noting that "Congress has the power to apply its statutes extraterritorially, and in the case of [the CFAA], it has clearly

[8] *See* CFAA § (g).

[9] *See Ashcroft v. Randel*, 391 F. Supp. 2d 1214, 1220 (N.D. Ga. 2005).

[10] *See Egilman v. Keller & Heckman*, 401 F. Supp. 2d 105, 111–112 (D.D.C. 2005) ("Egilman states that he learned by November 2002 all additional facts necessary to file his claim. By that date, the statute of limitations period still had over seven months until it expired . . . [T]he court concludes that equitable tolling is not merited and Egilman's CFAA claim is barred.").

[11] *See* CFAA at §§ (a)(5)(A); (e)(2).

[12] Nick Akerman, *CFAA Resembles RICO*, Nat'l L. J., Aug. 29, 2005, at 13.

[13] 175 F.Supp.2d 367, 368–69 (D. Conn. 2001).

[14] *See id.* at 370.

manifested its intention to do so."[15] Thus, the CFAA's jurisdictional requirements are met where the targeted computer regularly transmits interstate e-mails, regardless of the defendant's physical location while committing his culpable acts.

A third and final threshold requirement of civil claims filed under the CFAA is that a plaintiff plead and prove at least $5,000 in "loss."[16] The CFAA defines "loss" to include "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."[17] This broad definition and relatively low value threshold ensure that most CFAA claimants can generally meet this requirement with "ease."[18]

Nevertheless, not every conceivable form of injury necessarily constitutes a "loss" under CFAA. While the statutory definition clearly encompasses remedial expenses, these expenses must be "related to fixing a computer."[19] Because travel expenses and lost revenues related solely to the use of improperly acquired information are insufficiently linked to the offended computer, such expenses do not constitute "loss" for CFAA purposes.[20] Similarly, neither loss of goodwill nor loss of business opportunities and revenue resulting from the use of improperly acquired information constitute "loss" as contemplated by the CFAA.[21] Furthermore, even where remedial expenses are computer-related, plaintiffs must plead facts explaining the type of investigation performed or the type of damages remedied. In *Chas. S. Winner, Inc. v. Polistina*, the court held that the plaintiff failed to allege facts satisfying the CFAA loss requirement where the plaintiff merely stated that it spent in excess of $5,000 "to hire a computer expert to conduct an assessment and investigation."[22]

Factual Grounds for CFAA Claims

The various civil causes of action contemplated by the CFAA can be grouped into three prominent categories: (1) using unauthorized access to fraudulently acquire valuable information from a computer; (2) causing damage through the unauthorized transmission of computer passwords; and (3) causing unauthorized damage to computer data or causing damage to computer

[15] *Id.* at 375.

[16] *See* CFAA § (a)(5)(B)(i).

[17] *Id.* at § (e)(11).

[18] *Pac. Aerospace & Elec., Inc. v. Taylor*, 295 F.Supp.2d 1188, 1197 (E.D. Wash 2003).

[19] *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F.Supp.2d 468, 475 (S.D.N.Y. 2004), *aff'd*, 166 Fed. App. 559 (2d. Cir. 2006).

[20] *See id.* at 477.

[21] *See id.* at 475–478.

[22] 2007 WL 1652292, No. 06-4865, at *4 (D.N.J. June 4, 2007),

data through unauthorized access.[23] Taken together, these categories cover a wide variety of computer-related activity. Lack of authorization is a common element of each.[24]

Prior to 2000, all reported civil actions brought under the CFAA involved claims of unauthorized damage to computer data under sections (a)(5)(A)(ii) or (a)(5)(A)(iii) of the Act.[25] Several of these cases were brought against software manufacturers whose programs allegedly damaged host computers after customer installation.[26] Counsel should thus understand that a software manufacturer whose product damages a customer's existing computer data may be liable to the customer under CFAA for any damage caused to the customer's computer.

Several cases decided in 2000 demonstrated that the CFAA also may be used by businesses to safeguard their computerized data from competitors. In *Register.com, Inc. v. Verio, Inc.*, the defendant used several robotic devices to download customer information from a competing domain name registry's web site.[27] The defendant used the data to solicit customers in direct competition with the plaintiff-registry.[28] Importantly, the plaintiff's customer data was publicly available from the plaintiff's website.[29] Nevertheless, the court concluded that the defendant's actions violated section 1030(a)(2)(C) of the CFAA.[30]

The CFAA is also commonly used to redress the destruction of company data by disgruntled employees.[31] In *International Airport Centers, LLC v. Citrin*, an employee of a real estate developer decided to quit and go into business for himself.[32] Before leaving, he deleted all the data on his company laptop using a secure-erasure program designed to prevent the recovery of data.[33] While a district court dismissed the plaintiff-developer's CFAA-based claim, the

[23] *See* Nick Akerman & Patricia Finnegan, *Civil Relief Under CFAA*, NAT'L. L. J., Dec. 24–31, 2001, at A19.

[24] *See* CFAA at §§ (a)(4); (a)(5)(A).

[25] *See* Ackerman & Finnegan, *supra* note 23, at A19.

[26] *See, e.g.*, *In re America Online, Inc.*, 168 F.Supp.2d 1359 (S.D. Fla. 2001) (although class of customers failed to satisfy damages element, "§1030(a)(5)(A) applie[d] to the facts of the case"); *Shaw v. Toshiba Am. Info. Sys., Inc.*, 91 F. Supp. 2d 926 (E.D. Tex. 1999) (defendant's motion for summary judgment denied on 1030(a)(5)(A) claim where defendants' floppy disk controllers destroyed data and stored corrupted data); *North Texas Preventive Imaging, L.L.C. v. Eisenberg*, 1996 WL 1359212, No. 96-71AHS (C.D. Cal Aug. 19, 1996) (plaintiff stated a §1030(a)(5)(A) claim where disk manufacturer provided customers with disks designed to render software inoperable on a specific date).

[27] 126 F.Supp.2d 238, 243 (S.D.N.Y. 2000),

[28] *See id.*

[29] *See id.* at 242.

[30] *See id*. at 253 (enjoining defendant's actions).

[31] *See, e.g., Int'l. Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *see also Four Seasons Hotels and Resorts, B.V. v. Consocio Barr*, 267 F. Supp. 2d 1268, 1322–23 (S.D. Fla. 2003).

[32] *See id.* at 419.

[33] *See id.*

Seventh Circuit Court of Appeals reversed, noting that use of the erasure program constituted a "transmission" as used in section 1030(a)(5)(A)(i).[34]

Unauthorized Access

With few exceptions, a claimant under the CFAA or one of its state analogues must demonstrate either "unauthorized access," "access without authorization," or "exceeding authorized access" to a protected computer.[35] Courts have struggled to interpret these key terms consistently, with several recent decisions defining unauthorized access in a "remarkably expansive" manner, according to one commentator.[36]

The CFAA does not include a definition of the word "access." Most courts have used a "virtual reality approach" to determine what constitutes access under the CFAA.[37] Under this approach, a user accesses a computer only by getting "inside" the device and interfacing with its data.[38]

Other courts, however, have interpreted the word "access" more broadly. In *America Online v. National Health Care Discount, Inc.*, the court reasoned:

> [f]or purposes of the CFAA, when someone sends an e-mail message from his or her own computer, and the message then is transmitted through a number of other computers until it reaches its destination, the sender is making use of all of those computers, and is therefore "accessing" them.[39]

Moreover, unlike the CFAA, some state computer crime statutes do define the term "access." Often these definitions are far broader than any common understanding of the word. The Washington statute, for example, defines "access" as "to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resource of a computer, directly or by electronic means."[40] The Washington Supreme Court has held that, under this

[34] *See id.* at 420.

[35] *See, e.g.*, CFAA at §1030(a)(4) (a violation occurs where a person "accesses a protected computer without authorization, or exceeds authorized access").

[36] *See* Kerr, *supra* note 6, at 1617.

[37] *See id.* at 1625.

[38] *See State v. Allen*, 917 P.2d 848 (Kan. 1996) (defendant did not access a computer for the purposes of Kansas' computer crime statute where he never bypassed a password prompt); *Moulton v. VC3*, No. 1:00CV434-TWT, 2000 WL 33310901 (N.D. Ga. Nov. 7, 2000) (defendant did not access a computer for CFAA purposes where defendant merely executed a "port scan" [a common network security test that queries a target computer for open network ports] of plaintiff's computer network).

[39] 121 F. Supp. 2d 1259, 1272–73.

[40] Wash. Rev. Code Ann. § 9A.52.010(6) (West 2008).

definition, a user accesses a computer even where he is rebuffed by a password prompt and never interacts with protected data.[41]

Courts also have struggled to interpret "authorization" for purposes of computer crime statutes. Their opinions on this matter generally fall into three categories: so-called "intended function" cases, employee misuse cases, and breach of contract cases.[42]

Under the intended function test, first announced by the Second Circuit in *U.S. v. Morris*, access is unauthorized where it is not "in any way related to [a program's] intended function."[43] As such, use is unauthorized "when a user exploits weaknesses in a program and uses a function in an unintended way to access a computer."[44]

When presented with the proper facts, several courts have alternatively tied authorization to employee misconduct.[45] For example, in *Shurgard Storage Centers v. Safeguard Self Storage*, the defendant corporation lured away several of the plaintiff's employees.[46] Before leaving, one of the employees accessed the plaintiff's proprietary information and e-mailed it to the defendant.[47] The court, noting that "the authorization for [the plaintiff's] . . . employees ended when the employees began acting as agents for the defendants," concluded that the employees "lost their authorization and were 'without authorization' when they allegedly obtained and sent the proprietary information to the defendant via e-mail."[48] Thus, under *Shurgard*, an employee is seemingly without authorization for purposes of the CFAA whenever the employee uses a computer for any reason that is against an employer's interests. Not surprisingly, at least one commentator has called the *Shurgard* theory of authorization "strikingly broad."[49]

Furthermore, in some civil cases courts have held that, where a contract regulates an individual's access to a computer, any actions in breach of the contract constitute unauthorized access for purposes of the CFAA.[50] For example, in *America Online v. LCGM, Inc.*, a spammer purchased an AOL e-mail account to collect the addresses of AOL users.[51] AOL's Terms of Service

[41] *See State v. Riley*, 846 P. 2d 1365 (Wash. 1993) (en banc).

[42] *See* Kerr, *supra* note 6, at 1628.

[43] 928 F.2d 504, 510 (2d. Cir. 1991).

[44] *See* Kerr, *supra* note 6, at 1632.

[45] *See, e.g., Shurgard Storage Centers, Inc. v.. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

[46] *See id.* at 1123.

[47] *See id.*

[48] *See id.* at 1124–25.

[49] *See* Kerr, *supra* note 6, at 1633.

[50] *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001).

[51] 46 F. Supp. 2d 444, 448 (E.D. Va. 1998).

expressly prohibited this kind of activity.[52] The court pithily reasoned that "Defendant's actions violated AOL's Terms of Service, and as such was [sic.] unauthorized."[53]

The Benefits of the CFAA Over Similar Causes of Action

The CFAA is drafted broadly enough that conduct otherwise supporting other causes of action may also form the basis of a CFAA claim.[54] Because the CFAA offers claimants several distinct advantages over some of these other causes of actions, counsel should consider supplementing their civil complaints with CFAA-based claims whenever possible.

First, since the CFAA is a federal statute, claims filed thereunder will always support federal jurisdiction.[55] The CFAA thus provides an avenue to federal court when the only other claims available are state law-based and do not support diversity jurisdiction. Furthermore, because the CFAA includes both civil and criminal components, CFAA defendants are necessarily faced with the implicit threat of criminal sanctions.

CFAA claims also are often easier to prove than other similar causes of action. Trade secrets claims, for example, are commonly used to address instances of misappropriation or misuse of trade secrets and other confidential information. To demonstrating a viable trade secret claim, however, a claimant must establish the reasonableness of the steps taken to safeguard the protected information.[56] This can be a fact-intensive and expensive endeavor, often requiring proof of a company's business practices over many years. Furthermore, with every trade secrets action comes the risk that a court will conclude that the subject information does not qualify for trade secret protection.

These risks and concerns are obviated by pursuing a claim predicated on the CFAA. To the extent that a company's confidential information is stored electronically, an outsider's misappropriation of the data should fall squarely within even narrow definitions of "access without authorization." As discussed above, the CFAA is commonly used to address the misappropriation of company data by recently-terminated employees.[57] The CFAA can thus be used to protect the same interests as trade secrets cases, but at lower cost and risk.

[52] *See id.*

[53] *Id.* at 450.

[54] *See* Akerman & Finnegan, *supra* note 23, at A19.

[55] *See id.*

[56] *See, e.g.*, *Othentec Ltd. v. Phelan*, 526 F.3d 135, 141 (4th Cir. 2008) (Virginia Uniform Trade Secrets Act, Va. Code Ann. § 59.1-336, requires that a "trade secret" be, *inter alia*, "subject to efforts that are reasonable under the circumstances to maintain its secrecy.")

[57] *See, e.g., Shurgard*, 119 F. Supp. 2d at 1121.

As with trade secrets actions, civil RICO claims also can be complex and difficult to prove.[58] Nevertheless because the federal RICO statute provides the implied threat of criminal sanctions, punitive damages, and attorney fees, victims of fraudulent activity often couch their grievances as RICO claims.[59]

The CFAA also prohibits certain computer-related schemes to defraud.[60] Moreover, like RICO actions, claims based on the CFAA carry with them the implicit threat of criminal sanctions.[61] Thus, if an alleged fraud involves the use of a computer, CFAA claims may constitute a worthy substitute or supplement for a civil RICO claim (although, unlike with civil RICO claims, neither treble damages nor attorney fees are available under the CFAA).[62]

In sum, the CFAA constitutes a potent yet under-utilized weapon in the business litigator's arsenal. It offers unique advantages that can impact significantly the likelihood of an early settlement of a dispute, the expense of litigation, and even its outcome. Because computers increasingly permeate virtually every aspect of modern business transactions, the potential applicability of the CFAA to a dispute with a former employee or competitor accused of misappropriating confidential information or otherwise engaging in unfair competition through the misuse of sensitive data should be examined.

[58] *See* Akerman, *supra* note 12, at 13 ("Without the 'pattern' and 'enterprise' elements essential to prove a RICO violation, the CFAA provides a basis to bring a civil action predicated on a scheme to defraud . . . .").

[59] *See* 18 U.S.C. § 1961 *et seq.* ("RICO"). For example, both mail fraud and wire fraud are federal RICO predicate acts. *See id.* § 1961(1)(B).

[60] *See* CFAA at § 1030(a)(4).

[61] *See id.* at § 1030(c).

[62] *See generally id.*