Three Threshold Questions Every Attorney Must Answer before Filing a Computer Fraud Claim

By Pierre Grosdidier

It can be tempting to file a lawsuit against a computer trespasser or wrongdoer with a claim under the Computer Fraud and Abuse Act (18 U.S.C. § 1030, the "CFAA"). A CFAA claim opens the federal courthouse doors and enjoys tangible media appeal. But like any other cause of action, a CFAA claim must be carefully considered to ensure that it is not vulnerable to a dispositive motion. The challenge awaiting counsel is not so much that the statutory language is difficult, but that the case law construing the statute is fragmented. A CFAA claim that stands in one district court might fall in another.

The CFAA is a broadly-worded criminal statute that proscribes unauthorized access to protected computers, or access that exceeds authorization. The statute's § 1030(g) grants CFAA a victim "who suffers damage or loss" the right to a civil cause of action provided that the wrongdoer violated § 1030(a) though conduct that involved one of the factors set forth in § 1030(c)(4)(A)(i). *See*, *e.g.*, *Kluber Skahan & Assocs., Inc. v. Cordogen, Clark & Assocs., Inc.*, No. 08-cv-1529, 2009 WL 466812, at *6 (N.D. Ill. Feb. 25, 2009) (mem. op.).

The CFAA's § 1030(a) bars at least seven types of activities, several of which involve government or financial institution computers and are improbable bases for claims in private civil litigation. Most civil CFAA claims between private parties arise under §§ 1030(a)(2)(C) ("obtaining information"), (a)(4) ("intending to defraud"), or (a)(5) ("causing damage").

A civil CFAA claim must also be premised on one of the five factors listed in § 1030(c)(4)(A)(i). Realistically, however, civil claims can be expected to arise only under sub-section (I), which requires "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I). Other § 1030(c)(4)(A)(i) sub-sections deal with physical injury, health and safety, and government computers—plausible but improbable topics of civil litigation in relation to unauthorized computer access.

Plaintiff's counsel must answer three threshold questions before filing a CFAA claim.

Was access unauthorized or beyond granted authority?

Much has been made of the fact that the CFAA does not define unauthorized access (it only defines "exceeds authorized access"). Naturally, courts are split on whether to construe the term

"unauthorized" broadly or narrowly. Access that circumvents a firewall or a password is almost always unauthorized. The issue is less clear when employees help themselves to their employers' digital information before resigning to start or join a competing business. Is such access unauthorized even though the employee proceeded with a legitimate password? Does it make a difference if the employee violated the express terms of a computer-use agreement? The answers to these questions depend on the court where the lawsuit is filed and on the specific CFAA claim asserted, as the following cases show.

The Ninth Circuit held in *United States v. Nosal*, a criminal case, "that the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions." 676 F.3d 854, 863 (9th Cir. 2012). In other words, an employee does not violate the CFAA by accessing information in violation of his employer's computer-use policy using an otherwise valid password. Nosal was charged with a § 1030(a)(4) violation after using information pilfered from his previous employer's database to start a competing business. The court reasoned, in part, that applying the CFAA under these conditions would also criminalize the conduct of employees who used their work computers for innocent—albeit arguably unauthorized—activities, such as "playing games, shopping or watching sports highlights."

The Fifth Circuit reached the opposing conclusion in another criminal case, *United States v. John*, 597 F.3d 263 (5th Cir. 2010). John worked in a bank and passed on computer-stored customer account information to a relative, who used the information to orchestrate frauds. John had attended bank training programs that delineated the limits of her authority to use the bank's computer systems and customer information. A trial court found her guilty of "exceeding authorized access to a protected computer in violation of 18 U.S.C. §§ 1030(a)(2)(A) and (C)." The Fifth Circuit upheld the conviction, reasoning in part that "when an employee knows that the purpose for which she is accessing information in a computer is both in violation of an employer's policies and is part of an illegal scheme, it would be 'proper' to conclude that such conduct 'exceeds authorized access' within the meaning of § 1030(a)(2)."

John was also a case of "exceeding authorized access." Suppose the plaintiff alleges a claim under §§ 1030(a)(5)(B) or (C), which only implicate conduct "without authorization," and the defendant had valid log-in credentials and arguably merely exceeded his or her authority. Will a CFAA claim stand under these facts in the Fifth Circuit in light of *John*? At least one district court hinted that it might not. In *Devon Energy Corp. v. Westacott*, which post-dates *John*, the court noted that "[c]ourts have held that the CFAA must be construed narrowly, even in civil actions." No. H-09-1689, 2011 WL 1157334, at *10 (S.D. Tex. Mar. 24, 2011) (Rosenthal, J.)

(mem. op.). *Devon* unfortunately did not address the aforementioned question because the claim involved the CFAA's § 1030(a)(5)(A), which is worded differently from §§ (B) and (C). But in *Beta Tech., Inc. v. Meyers*, the same court held that the plaintiff stated a § 1030(a)(5)(C) claim where the defendant allegedly deleted files on his employer's computer. No. H-13-1282, 2013 WL 5602930, at *4 (S.D. Tex. Oct. 10, 2013) (Werlein, J.) (mem. op.). The court specifically noted that the defendant might have accessed his employer's computer "after he was no longer employed by Plaintiff," which would have been access "without authorization." The court's carefully-chosen language suggests that plaintiff's § 1030(a)(5)(C) claim might have failed had the defendant only accessed the computer before his resignation when his access was still authorized. *See id.* at *4 and n.33. In that case, the defendant would have merely exceeded authorized access, and arguably remained outside the aegis of the CFAA's § 1030(a)(5)(C), which bars unauthorized access.

These cases show that plaintiff's counsel must precisely ascertain the facts that potentially give rise to a CFAA cause of action, identify the applicable statutory claim or claims, and thoroughly check the case law in the court where the case is to be filed to see how judges have construed the statutory language. Only then will counsel appreciate the viability of a CFAA claim.

The defendant's authority to access a computer is not the only element of a CFAA claim that must be precisely ascertained before filing suit. The CFAA authorizes a cause of action to victims "who suffer[] damage *or* loss." Claims under § 1030(a)(2)(C) and (a)(4) require the plaintiff to demonstrate a loss, but claims under § 1030(5) require both damage *and* loss (assuming § 1030(c)(4)(A)(i)(I) applies). Counsel must, therefore, also assess plaintiff's loss, or both damage and loss, depending on the asserted CFAA claim.

What is the plaintiff's damage and is it actionable?

The CFAA defines "damage" to mean "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Courts have generally interpreted the term "damage" to refer to harm to data and information. *Kluber*, 2009 WL 466812, at *7. Here again the district courts are split between those that construe "damage" broadly or narrowly. File deletion obviously qualifies as damage. *Milbank v. Simons (In re Simons Broad., LP)*, No. W-11-CA-172, 2013 WL 9542015, at *19 (W.D. Tex. Nov. 19, 2013) (mem. op.). Some courts hold that mere access and copying of files does not constitute damage (narrow construction). Other courts adopt the position that accessing data or information without authorization or with ill

intent creates an uncertainty over the data that, in and of itself, qualifies as "damage" (broad construction).[1]

Two cases illustrate the case law's fragmentation with respect to the damage element of a CFAA claim. In both cases the plaintiff asserted § 1030(a)(4) claims. In *Milbank*, the defendant downloaded information from plaintiff's computer. 2013 WL 9542015, at *19. The court was "not convinced that a party can be damaged by the simple download of computer software." The court held that "even if a computer was improperly used to misappropriate a trade secret, such facts alone will be insufficient to allege" damage as the term is defined in § 1030(e)(8), and it granted the defendants judgment as a matter of law. The majority of district courts follow this narrow construction of the term "damage."[2]

In *T-Mobile USA, Inc. v. Terry*, the defendants developed an elaborate scheme to defraud the telephone operator of air time and services. 862 F. Supp. 2d 1121, 1125-26 (W.D. Wash. 2012). The court held that T-Mobile was damaged when one of the defendants accessed T-Mobile's proprietary database. Citing to prior case law, the court reiterated that someone who infiltrates a computer system and collects information thereby impairs its integrity and, therefore, causes damage as that term is construed under the CFAA. *Id*. at 1131.

One court apparently even changed its mind about what constitutes "damage" under the CFAA. In *Fidlar Techs. v. LPS Real Estate Data Solutions, Inc.*, the court denied LPS's motion to dismiss Fidlar's CFAA § 1030(a)(5)(A) claim because Fidlar detailed how LPS's web harvesting software bypassed Fidlar's user controls. No. 4:13-cv-4021-SLD-JAG, 2013 WL 5973938, at **1, 7 (C.D. Ill. Nov. 8, 2013) ("*Fidlar I*"). The court held that "[u]nder the plain language of the statute, this [wa]s sufficient to allege 'damage'." But the court reversed course after LPS filed its motion for summary judgment. *Fidlar Techs. v. LPS Real Estate Data Solutions, Inc.*, No. 4:13-cv-4021-SLD-JEH, 2015 WL 1059007, at *8 (C.D. Ill. Mar. 5, 2015) ("*Fidlar II*"). The court held that "access to or disclosure of information on remote servers is generally not understood in the Seventh Circuit as 'damage' within the meaning of the statute," and it granted LPS judgment as a matter of law as to Fidlar's § 1030(a)(5)(A) claim.

---

[1] *See generally*, Pierre Grosdidier & Mike Stewart, *When Employees Leave with Electronic Files: The CFAA's Eclectic Damage and Loss Case Law Illustrated*, Bloomberg BNA Electronic Commerce & Law Report, June 2, 2014.

[2] The CFAA's "damage" case law is comprehensively reviewed in *NetApp, Inc. v. Nimble Storage, Inc.*, No. 5:13-CV-05058-LHK (HRL), 2015 WL 400251, at *14 (N.D. Cal. Jan. 29, 2015) (adopting a narrow construction of the term "damage" in the case of a § 1030(a)(5) claim).

What is the plaintiff's loss, and is it actionable?

The CFAA defines "loss" as

> 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.

18 U.S.C. § 1030(e)(11). Courts are also split over the construction of this deceptively simple definition. The issue is whether the final "clause 'because of interruption of service' modifies the entire provision or just 'revenue lost, cost incurred, or other consequential damages.'" *Lyon v. Can. Nat'l Ry. Co.*, No. 4:10CV185DPJ-FKB, at *5 (S.D. Miss. Apr. 10, 2012) (available at Fastcase.com and Loislaw.com).

Many courts have followed the Southern District of New York's narrow statutory construction and held that "[t]he term 'loss' encompasses only two types of harm: costs to investigate and respond to an offense," i.e., damage to data or information, "and costs incurred because of a service interruption." *Alliantgroup, L.P. v. Feingold*, 803 F. Supp. 2d 610, 630 (S.D. Tex. 2011) (Rosenthal, J.) (mem. op.) (citing *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 474‑76 (S.D.N.Y. 2004), aff'd, 166 F. App'x 559, 562‑63 (2d Cir. 2006)). Under these conditions, pleadings that do not allege an interruption of service, or costs incurred to investigate or respond to same, risk being struck. In *Rajaee v. Design Tech Homes, Ltd.*, for example, Rajaee alleged that his employer remotely wiped his iPhone shortly after he resigned, ostensibly deleting all data residing on the iPhone. No. H-13-2517, 2014 WL 5878477 (S.D. Tex. Nov. 11, 2014) (mem. op.) (motion for new trial denied, Dkt. No. 47, Jan. 27, 2015) (disclosure: the author was one of the defense attorneys). The court dismissed Rajaee's claim because he "produced [no] evidence of any costs he incurred to investigate or respond to the deletion of his data, nor do the losses and damages for which he does produce evidence arise from an 'interruption of service.'"

Other courts have adopted a broader construction of the definition of "loss." As the court held in *Fidlar I*, the problem with a narrow reading of the term "loss" "is that it ignores the opening clause of § 1030(e)(11), which broadly defines loss as *any* reasonable cost to any victims." *Fidlar I*, 2013 WL 5973938, at *8. In *Costar Realty Info., Inc. v. Field*, for example, the court held that plaintiff adequately pled a loss under the CFAA when it alleged lost license fee revenue caused by defendants' unauthorized use of plaintiff's database. 612 F. Supp. 2d 660, 675 (D. Md. 2009) (mem. op.).

The case law shows that CFAA civil claims are not easily asserted, despite the Act's strong and broad language. Counsel pondering filing a CFAA claim must carefully analyze the underlying facts and confirm that the claim will stand in light of the local case law. In the event the relevant case law is sparse, a court's disposition of one CFAA issue discussed in this article might be a harbinger of its disposition of another. Judge Rosenthal in the Southern District of Texas, for example, narrowly construed the term "loss" in *Alliantgroup* on the same day she noted in *Devon*, in relation to unauthorized access, that "[c]ourts have held that the CFAA must be construed narrowly."

About the Author

Pierre Grosdidier is an Associate in Haynes and Boone, LLP's Business Litigation practice group in Houston, Texas. His practice focuses on complex commercial litigation, especially lawsuits and arbitrations with strong technical elements. He has litigated cases involving construction, oil and gas, software copyright, Computer Fraud and Abuse Act, Stored Communications Act, and trade secret claims. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas and is a registered Texas P.E. (inactive).