Key Issues in Computer Fraud and Abuse Act (CFAA) Civil Litigation

BRENDA R. SHARTON, GABRIELLE L. GOULD, JUSTIN C. PIERCE, GOODWIN PROCTER LLP, WITH PRACTICAL LAW DATA PRIVACY ADVISOR

A Practice Note providing an overview of the Computer Fraud and Abuse Act (CFAA) and examining the key issues that counsel should consider when litigating civil actions under the CFAA. This Note focuses on CFAA provisions most commonly used to bring civil actions, the statutory requirements for bringing CFAA civil actions, and the issues that generally pose the most difficulty for litigants to maintain a CFAA claim. This Note also provides best practices for litigating claims under the CFAA.

The Computer Fraud and Abuse Act (18 U.S.C. § 1030) (CFAA) imposes criminal and civil liability for unauthorized access or damage to a protected computer. The law reaches every computer connected to the internet and non-networked computers used by the US government or financial institutions.

The CFAA covers many types of computer fraud including:

- Theft of trade secrets.
- Hacking and data breaches.
- Denial or interruptions of service.
- Anti-competitive behavior.

Organizations often use the CFAA to bring private civil lawsuits seeking injunctive relief or compensation from:

- Terminated or rogue employees.
- Competitors.
- Third-party hackers.

The CFAA's complex statutory language has generated substantial litigation. The US Supreme Court has not interpreted the CFAA and lower court decisions significantly differ in their interpretations of the CFAA. Prospective litigants must understand what the CFAA covers, how it is used, and the courts' conflicting applications of the statute.

This Note focuses on civil CFAA actions. Criminal liability is outside the scope of this Note. For more information on criminal exposure under the CFAA, see Box: Criminal Penalties Under the CFAA.

CFAA VIOLATIONS OVERVIEW

PROTECTED COMPUTERS

The term computer under the CFAA means any device for processing or storing data excluding an automated typewriter, portable handheld calculator, or other similar device (18 U.S.C. § 1030(e)(1)). In addition to desktop and laptop computers, the CFAA protects devices such as:

- Cell phones, cell towers, and stations that submit wireless signals (see *United States v. Nosal*, 844 F.3d 1024, 1050-51 n. 3 (9th Cir. 2016); *United States v. Mitra*, 405 F.3d 492, 495 (7th Cir. 2005)).
- Websites (see *United States v. Drew*, 259 F.R.D. 449, 457-58 (C.D. Cal. 2009)).
- Restricted databases (*United States v. Valle*, 807 F.3d 508, 513 (2d Cir. 2015)).
- iPads, Kindles, Nooks, and videogame systems such as Xbox (see *United States v. Nosal*, 676 F.3d 854, 861 (9th Cir. 2012)).

The term protected computer means either:

- US government computers.
- Financial institution computers.
- Computers used in interstate or foreign commerce.

(18 U.S.C. § 1030(e)(2).)

Courts have held that computers used in interstate or foreign commerce include any computer connected to the internet (see, for example, *Nosal*, 676 F.3d at 859; *United States v. Trotter,* 478 F.3d 918, 921 (8th Cir. 2007)).

PROHIBITED CONDUCT

Criminal and civil CFAA actions arise from seven categories of prohibited conduct defined in Sections 1030(a)(1)-(7). Plaintiffs commonly bring civil claims under:

- Section 1030(a)(2)(C), which prohibits intentionally accessing a protected computer, without authorization or by exceeding authorized access, and obtaining information from a protected computer.
- Section 1030(a)(4), which prohibits knowingly and with intent to defraud accessing a protected computer, without authorization or by exceeding authorized access, to obtain anything of value or further a fraud.
- Section 1030(a)(5)(A), which prohibits knowingly, intentionally, and without authorization causing the transmission of a program, information, code, or command to a protected computer, and causing damage.
- Sections 1030(a)(5)(B) and 1030(a)(5)(C), which prohibit intentionally accessing a protected computer without authorization and, as a result of such conduct, recklessly causing damage and loss.

Plaintiffs bringing civil claims under the CFAA must also establish one of the following factors under Section 1030(c)(4)(A)(i) for the court to have jurisdiction to hear a CFAA civil claim:

- Loss to one or more persons during any one-year period aggregating at least $5,000 in value.
- The modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals.
- Physical injury to any person.
- A threat to public health or safety.
- Damage affecting a computer used by or for an entity of the US Government in furtherance of the administration of justice, national defense, or national security.

(18 U.S.C. §§ 1030(g) and 1030(c)(4)(A)(i).)

Plaintiffs typically rely on the first factor, which requires proof that the computer fraud caused a combined loss of at least $5,000 to one or more persons during any one-year period (see $5,000 Loss Threshold).

CONSPIRACY CLAIMS

Section 1030(b) of the CFAA creates a separate offense for attempting or conspiring to violate any of the seven prohibitions in Section 1030(a). However, courts are divided on whether Section 1030(b) applies to civil liability (see, for example, *Hovanec v. Miller*, 2018 WL 1221486, at *8 (W.D. Tex. Mar. 7, 2018) (recognizing that Section 1030(g) creates a private right of action for CFAA conspiracy claims); *Welenco, Inc. v. Corbell*, 126 F. Supp. 3d 1154, 1176 (E.D. Cal. 2015) (same); but see *Coll Builders Supply, Inc. v. Velez*, 2017 WL 4158661, at *6 (M.D. Fla. Aug. 31, 2017) (stating that it is unsettled whether a civil defendant may be liable for attempting or conspiring to violate the CFAA); *Porters Bldg. Ctrs., Inc. v. Sprint Lumber*, 2017 WL 4413288, at *3 (W.D. Mo. Oct. 2, 2017) ("[I]t is doubtful the CFAA permits a civil conspiracy claim")).

STATUTE OF LIMITATIONS

Plaintiffs must bring CFAA actions within two years from either:

- The date of defendant's act.
- The date plaintiff discovers the unauthorized computer access or damage (for explanations of these terms see Unauthorized Access and Damage).

(18 U.S.C. § 1030(g).)

The key inquiry in determining when the limitation period accrues is when the plaintiff learns of the unauthorized access or damage, even if the identity of the perpetrator is not known. If a plaintiff cannot determine the perpetrator's identity within two years of discovering a violation, a court may deem the CFAA action untimely, as the Second Circuit cautioned in *Sewell v. Bernardin*, 795 F.3d 337, 342 (2d Cir. 2015). This underscores the necessity of engaging a forensic investigator promptly after the computer fraud to identify the perpetrator.

CFAA KEY LITIGATION ISSUES

To maintain a successful claim under Sections 1030(a)(2)(c) and 1030(a)(4), a plaintiff must plead that:

- The defendant:
  - accessed a protected computer without authorization (see Without Authorization); or
  - exceeded authorized access on a protected computer (see Exceeding Authorization).
- The plaintiff suffered a monetary loss of at least $5,000 (unless another factor under 18 U.S.C. 1030(c)(4)(A)(i) applies) (see $5,000 Loss Threshold).

Plaintiffs bringing a claim under Section 1030(a)(5) must plead that:

- For claims under Section 1030(a)(5)(A), the defendant knowingly transmitted a program, information, code, or command to a protected computer (see Transmission).
- The defendant caused damage to the protected computer without authorization (see Damage).
- The plaintiff suffered a monetary loss of at least $5,000 (unless another factor under 18 U.S.C. 1030(c)(4)(A)(i) applies) (see $5,000 Loss Threshold).

Courts rely uniformly on criminal and civil cases when interpreting the above requirements (see, for example, *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012) ("Where, as here, our analysis involves a statute whose provisions have both civil and criminal application, our task merits special attention because our interpretation applies uniformly in both contexts.")).

UNAUTHORIZED ACCESS

CFAA litigation typically focuses on whether the defendant accessed a protected computer without authorization or by exceeding authorized access. Cases and the CFAA legislative history suggest that:

- "Without authorization" applies to company outsiders or individuals who have no authorized access to the computer.

- "Exceeds authorized access" applies to company insiders or individuals whose initial access to a computer was authorized but who access unauthorized information or files.

(*Nosal,* 676 F.3d at 858; *United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007).)

However, courts often do not clearly distinguish between these two concepts, making it difficult for litigants to establish them (see, for example, *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006) (noting that the distinction between "without authorization" and "exceeding authorized access" is paper thin)).

When analyzing defendant's authorization, organizations must understand that:

- Some CFAA provisions require a showing that a defendant accessed a computer without authorization or exceeding authorization (see Sections 1030(a)(2)(C) and 1030(a)(4)).
- Other provisions require damage to a computer without authorization (see Section 1030(a)(5)).

Plaintiffs should plead both unauthorized access or exceeds authorization if appropriate because courts often blur the two concepts, particularly when considering claims against company insiders.

Without Authorization

The CFAA does not define "without authorization." Most courts interpret the term to mean accessing or damaging a computer without permission (see, for example, *United States v. Thomas*, 877 F.3d 591, 598 (5th Cir. 2017) (without authorization means intentionally damaging a computer system without permission); *Nosal,* 844 F.3d at 1028 (concluding that the plain and ordinary meaning of "without authorization" means accessing a protected computer without permission); *Tech Sys., Inc. v. Pyles*, 630 Fed. App'x 184, 186-87 (4th Cir. 2015) (holding that "authorization is a matter of permission and dependent on its scope")).

For example, courts have ruled that the defendant acts without authorization when:

- A hacker remotely accesses a computer without authorization to do so (see, for example, *Phillips*, 477 F.3d at 220-21 (student acted without authorization when he used a brute-force program to access a university's internal computer system and steal social security numbers)).
- Former employees access an organization's computers after the employer terminated their access credentials (see *Nosal,* 844 F.3d at 1035 (defendant accessed computer without authorization after plaintiff employer revoked defendant's credentials); see also *Coll Builders Supply, Inc.*, 2017 WL 4158661, at *5 (former employees accessed plaintiff's computer systems without authorization after plaintiff explicitly informed them they no longer had access to the plaintiff's systems).

Courts differ in their views of whether employees act without authorization when they have permission to access a computer but use that access in an improper manner. Courts often analyze this as a situation in which the employee exceeds authorized access (see Exceeding Authorization).

However, the Seventh Circuit Court of Appeals uses an agency analysis to consider the liability of an employee who uses permitted access to a computer for an improper purpose. In *International Airport Centers., LLC. v. Citrin*, a former employee deleted data on a laptop after quitting his position to conceal improper conduct. The court stated that once an employee acts adversely to his employer's interest, the agency relationship and authorization under the CFAA immediately terminates, establishing that an employee acts without authorization. (440 F.3d 418, 418-21 (7th Cir. 2006).)

Courts may also find that defendants who breach the terms of service on public-facing websites act without authorization under the CFAA. For example, in *Craigslist Inc. v. 3Taps Inc.*, the defendant continued to access the plaintiff's public website to repost advertisements on a copycat website after plaintiff sent cease-and-desist letters and blocked the defendant's IP addresses. The court found that, although the defendant initially had permission to access the plaintiff's website, plaintiff rescinded that permission and the defendant's continued access was "without authorization." (964 F. Supp. 2d 1178, 1183-84 (N.D. Cal. 2013); see also *Facebook, Inc. v. Power Ventures, Inc*, 844 F.3d 1058, 1068 (9th Cir. 2016), cert. denied, 138 S. Ct. 313 (2017) (finding that Facebook revoked the defendant's permission to use Facebook's messaging system by issuing a cease and desist letter and using IP blocks to thwart defendant's access to its system); but see *Ticketmaster LLC. v. Prestige Ent., Inc.*, 2018 WL 654410, at *6-7 (C.D. Cal. Jan. 31, 2018) (dismissing a CFAA claim where the plaintiff sent a cease-and-desist letter that only admonished defendants for violating website's terms of use without expressly revoking defendant's access).)

Exceeding Authorization

Under the CFAA, a defendant exceeds authorized access if the defendant:

- Accessed a computer with authorization.
- Uses access to obtain or alter information.
- Is not entitled to obtain or alter that information.

(18 U.S.C. § 1030(e)(6).)

Courts have generally adopted one of two positions when deciding whether a defendant exceeded authorized access. Under a broader interpretation, an individual (most commonly a former employee) exceeds authorized access when the individual misuses information it has permission to access and the misuse violates a policy or agreement. The First, Fifth, and Eleventh Circuit Court of Appeals have adopted this broad approach. For instance:

- In *EF Cultural Travel BV v. Explorica, Inc.*, the First Circuit held that a defendant's use of a program to capture pricing data from his former employer's public website exceeded authorized access because:
  - the computer program relied on the defendant's inside knowledge about his former employer's tour codes; and
  - a broad confidentiality agreement prohibited the defendant from disclosing information considered contrary to his former employer's interests.

- (274 F.3d 577, 582-84 (1st Cir. 2001); but see *Wentworth–Douglass Hosp. v. Young & Novis Prof'l Ass'n,* 2012 WL 2522963, at *3 (D.N.H. June 29, 2012) (characterizing the First Circuit's broad approach as dicta and refusing to find that a defendant exceeded authorization by misusing information in violation of the employer's policy).)
- *In United States v. Rodriguez*, the Eleventh Circuit held that a government employee exceeded his authorized access by violating a policy prohibiting employees from obtaining database information without a business reason (628 F.3d 1258, 1263 (11th Cir. 2010)).
- In *United States v. John*, the Fifth Circuit held that a bank employee exceeded her authorized access and violated a company policy when she used information from a protected computer to commit a fraud (597 F.3d 263, 271-273 (5th Cir. 2010)).

By contrast, a narrower interpretation focuses only on whether technological measures prevented the defendant from accessing information and not on the defendant's misuse of the information. For example, if a company has two secure servers, X and Y, and issues an employee valid login credentials for only server X, the employee has authorized access to server X only. If the employee accesses data from server X, the court treats the access as authorized no matter how the employee uses that that information. However, if the employee accesses server Y, the employee has exceeded authorized access. (*Advanced Micro Devices, Inc. v. Feldstein*, 951 F. Supp. 2d 212, 217 (D. Mass. 2013).)

The Second, Fourth, and Ninth Circuit Court of Appeals have followed this narrow approach:

- In *Nosal,* the Ninth Circuit held that a former employee's accomplices who accessed information using their valid credentials for an improper purpose (to provide it to the former employee) did not exceed authorized access, even though the company's use restrictions prohibited the disclosure of confidential information (676 F.3d at 864).
- In *WEC Carolina Energy Sols. LLC*, the Fourth Circuit found that a departing employee did not exceed authorized access by downloading confidential information to a personal computer in violation of company policy because the employee was authorized to view the information in question (687 F.3d at 205-06).
- In *Valle,* the Second Circuit reversed the conviction of a police officer who accessed a restricted database without a law enforcement purpose because he was otherwise authorized to obtain the database information (807 F.3d at 523-28).

To establish that the defendant exceeded authorization under the narrow approach, plaintiffs must allege that:

- The defendant had the authority to access the computer system.
- The authorization was limited to particular information stored on the computer.
- The defendant bypassed technological barriers to access additional information (in other words, that the defendant is an "inside hacker").

(See *Nosal*, 676 F.3d at 857; *Wentworth–Douglass Hosp.*, 2012 WL 2522963, at *4 (explaining that a defendant who has access to limited information on a computer but uses a third party's password to access additional information has exceeded authorization).)

TRANSMISSION AND DAMAGE

Transmission

Plaintiffs bringing a claim under Section 1030(a)(5)(A) must plead that the defendant knowingly transmitted a program, information, code, or command to a protected computer. The CFAA does not define transmission. However, courts have stated that, for purposes of the CFAA, a transmission can occur over the internet or through a physical medium such as a compact disc (see *Meridian Fin. Advisors, Ltd. v. Pence*, 763 F. Supp. 2d 1046, 1061-62) (S.D. Ind. 2011)).

Examples of transmissions under the CFAA include:

- Code or programs containing viruses, including spyware (see, for example, *Becker v. Toca*, 2008 WL 4443050, at *1 (E.D. La. Sept. 26, 2008)).
- Phone calls and text messages (see, for example, *Czech v. Wall St. on Demand, Inc.*, 674 F. Supp. 2d 1102, 1114 (D. Minn. 2009)).
- Bulk emails (see, for example, *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 301 (6th Cir. 2011)).
- A program that deletes files from the plaintiff's computer (*Citrin*, 440 F.3d at 419–20).

DAMAGE

Liability under Section 1030(a)(5) also requires the plaintiff to show damage to a protected computer. The CFAA defines the requisite damage to mean any impairment to the integrity or availability of:

- Data.
- A program.
- A system.
- Information.

(18 USC. § 1030(e)(8).)

The CFAA does not define impairment, integrity, or availability. However, courts have found damage when the defendant's conduct diminishes a plaintiff's ability to use computer data or systems. For example, plaintiffs have successfully asserted damage when:

- A barrage of calls and emails impeded access to voicemail and email, prevented customers from reaching plaintiff's sales offices and representatives, and forced an employee to turn off her cell phone (see *Pulte Homes, Inc.,* 648 F.3d at 301).
- The permanent deletion of employee emails caused an impairment to the integrity or availability of data (see *Meridian Fin. Advisors,* 763 F. Supp. 2d at 1062).
- A defendant sent thousands of emails to one inbox and impaired the user's ability to access his other "good" emails (see *United States v. Carlson*, 209 Fed. App'x 181, 185 (3d Cir. 2006)).
- A defendant impaired the availability of an emergency communication system by transmitting data that interfered with the way the computer allocated communications to other channels (see *Mitra*, 405 F.3d at 494).
- A program that deleted files impaired the integrity or availability of data, programs, or information on the computer (*Citrin*, 440 F.3d at 419–20).

In contrast, courts have rejected damage allegations based on:

- The loss of memory space in a protected computer (*In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1066-1067 (N.D. Cal. 2012)).
- The plaintiff's receipt of unwanted text messages, in the absence of allegations that the defendant's text messages stopped the plaintiff from receiving or sending calls or messages (*Czech*, 674 F. Supp. 2d at 1117–18).

$5,000 LOSS THRESHOLD

The CFAA allows plaintiffs to aggregate the following two categories of loss to reach the $5,000 jurisdictional threshold under Section 1030(c)(4)(A)(i)(I):

- The costs of responding to an offense including:
  - conducting a damage assessment; and
  - restoring the data, program, system, or information to its condition prior to the offense.
- (See Costs.)
- Lost revenues or other consequential damages resulting from an interruption of service (see Lost Revenue and Consequential Damages).

(18 U.S.C. § 1030(e)(11).)

The $5,000 loss may comprise solely "costs" under the first category, solely "lost revenues or consequential damages" from the second category, or a combination of both (*Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*, 774 F.3d 1065, 1073 (6th Cir. 2014)).

Costs

To qualify as a cost for purposes of meeting the $5,000 loss threshold, plaintiffs must show a nexus between the expense and the affected computer. For example, in *Nexans Wires S.A. v. Sark–USA, Inc.*, the plaintiffs alleged that the travel expenses of two executives to conduct a damage assessment and respond to the misappropriation of information from computer constituted a cost under Section 1030(e)(11). The court affirmed the district court's dismissal of the complaint, stating that the costs did not relate in any way to the investigation or repair of affected computers. (166 Fed. App'x at 563.)

Courts have found that a plaintiff can satisfy the $5,000 loss requirement based on the expense of:

- Conducting a forensic investigation after a defendant accessed confidential and proprietary information stored on a plaintiff's laptop (see *Lapp Insulators LLC v. Gemignani,* 2011 WL 1198648, at *8 (W.D.N.Y. Mar. 9, 2011)).
- Diagnostic measures to assess the physical damage to a plaintiff's website caused by a defendant's intrusion into the protected computer, even if the organization subsequently learns there was no actual physical damage (see *EF Cultural Travel BV*, 274 F.3d at 584).
- Hiring consultants and contractors to investigate a defendant's unauthorized access to employee email accounts (see *Brown Jordan Int'l, Inc. v. Carmicle*, 846 F.3d 1167, 1173-74 (11th Cir. 2017)).
- Investigating network intrusions (see *Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887, 895 (N.D. Cal. 2010)).
- Security enhancements to a plaintiff's computer systems following defendant's cyber-attack (see *Integrated Waste Solutions, Inc. v. Goverdhanam,* 2010 WL 4910176, at *9 (E.D. Pa. Nov. 30, 2010)).
- The value of employee time to investigate a defendant's unauthorized access to a plaintiff's web portal (see *Gen. Linen Serv., Inc. v. Gen. Linen Serv. Co.*, Inc., 2015 WL 6158888, at *6 (D.N.H. Oct. 20, 2015)).
- Identifying evidence of the breach, assessing any damage it may have caused, and implementing any necessary remedial measures to preserve the network (see *Univ. Sports Pub. Co. v. Playmakers Media Co.,* 725 F. Supp. 2d 378, 388 (S.D.N.Y. 2010)).
- Identifying the identity of the perpetrator (see *AssociationVoice, Inc. v. AtHomeNet, Inc.,* 2011 WL 63508, at *7 (D. Colo. Jan. 6, 2011); *SuccessFactors, Inc. v. Softscape, Inc.*, 544 F. Supp. 2d 975, 980–81 (N.D. Cal. 2008); but see *Mintz v. Mark Bartelstein & Assocs. Inc.*, 906 F. Supp. 2d 1017, 1030-31 (C.D. Cal. 2012) (distinguishing *SuccessFactors* and finding that expenses associated with identifying the perpetrator's identity were not essential to remedying harm and did not qualify as a loss)).

However, counsel should be mindful that interpretations of "costs" under the CFAA are evolving, highly unsettled, and often conflicting (see, for example, *Jarosch v. Am. Family Mut. Ins. Co.*, 837 F. Supp. 2d 980, 1022 (E.D. Wis. 2011) (holding that investigation costs did not qualify as losses because they did not relate directly to the impairment or damage of a computer system); *Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int'l, Inc.*, 616 F. Supp. 2d 805, 811–13 (N.D. Ill. 2009) (holding that the cost of damage assessment based on an employee's misappropriation of confidential information did not constitute a loss)).

To ensure their alleged costs satisfy the $5,000 loss threshold, plaintiffs should:

- Review case law in their governing jurisdiction to understand potential conflicting interpretations of costs.
- Avoid boilerplate allegations of "loss" and "costs" in their pleadings.
- Describe costs with specificity and clearly allege a nexus between the cost incurred and the affected computer or system.

Lost Revenue and Consequential Damages

Successful claims of loss resulting from lost revenue and consequential damages are less common. Unlike costs, lost revenues and consequential damages only qualify toward the $5,000 threshold when the plaintiff experiences an interruption of service (see, for example, *Teva Pharm. USA, Inc. v. Sandu*, 291 F. Supp. 3d 659, 674 (E.D. Pa. 2018) (holding that, absent an interruption of service, plaintiff's lost revenue caused by a misappropriation of confidential information did not constitute a loss); *Simmonds Equip., LLC v. GGR Int'l, Inc.*, 126 F. Supp. 3d 855, 865 (S.D. Tex. 2015) (consequential damages constituted a loss because defendant's deactivation of website cost plaintiff a lucrative business opportunity). To establish a service interruption, plaintiffs must show that defendant's conduct rendered the

protected computer system or information unavailable (see, for example, *EquipmentFacts, LLC*, 774 F.3d at 1073-74; *Nexans Wires S.A. v. Sark–USA, Inc.*, 166 Fed. App'x 559, 563 (2d Cir. 2006)).

Most cases based on lost revenue and consequential damages involve alleged violations of Section 1030(a)(5)(A) (see Transmission and Damage). For example, in *B&B Microscopes v. Armogida*, the plaintiff alleged that defendant permanently deleted files relating to the plaintiff's proprietary algorithm stored exclusively on the defendant's laptop in violation of Section 1030(a)(5)(A)(i). The court held that:

- The deletion of the algorithm constituted an interruption of service because the plaintiff had no other way of accessing that algorithm.
- The plaintiff's inability to sell software based on the deleted algorithm and a resulting loss of $10,000 in revenue satisfied the $5,000 loss threshold.

(532 F. Supp. 2d 744, 758-59 (E.D. Pa. 2012).)

Interruptions of service also occur when the damage is only temporary. In *Simmonds Equipment, LLC v. GGR International*, the court held that:

- The temporary deactivation of the plaintiff's website sufficiently established damage within the meaning of Section 1030(e)(8).
- The plaintiff's inability to make a sales presentation while the website was unavailable and resulting loss of $1,000,000 in revenue satisfied the $5,000 loss threshold.

(126 F. Supp. 3d at 865.)

RECOVERY OF ECONOMIC DAMAGES

Once plaintiffs satisfy the $5,000 jurisdiction threshold, any damages they seek to recover in the lawsuit must be economic damages (18 U.S.C. § 1030(g)).

This limitation precludes recovery for non-monetary damages such as:

- Death.
- Personal injury.
- Mental distress.

(See, for example *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir. 2004) ("When an individual or firm's money or property are impaired in value, or money or property is lost, or money must be spent to restore or maintain some aspect of a business affected by a violation, those are 'economic damages.'").)

PRACTICAL CONSIDERATIONS FOR CFAA LITIGANTS

Organizations seeking to bring a CFAA claim can take actions before and after an incident to help them maintain their claim including:

- Having procedures in place to terminate computer access immediately after employment ends or a user violates website terms and conditions (see Terminate and Limit Access).
- Implementing technical barriers to limit computer access only to what is strictly necessary (see Terminate and Limit Access).
- Developing policies that describe permitted computer access and use (see Describe Permitted Access and Use in Policies and Employment Agreements).
- Documenting the date they learn of any fraud (See Document Date of Discovery of Computer Fraud).
- Documenting all costs associated with the computer damage or service interruption to meet the $5,000 threshold (see Document all Costs Associated with the Computer Fraud).

TERMINATE AND LIMIT ACCESS

Many courts assessing whether a defendant acted without authorization or exceeded authorized access focus only on whether technological barriers prevented the defendant from accessing information. If defendants misused information that they had access to, these courts reject any argument that the defendants acted without authorization or exceeded authorized access.

Organizations should therefore implement measures to:

- Terminate computer access under appropriate circumstances. For example:
  - in the employment context, organizations should have procedures to cut off an employee's computer access immediately after their termination; and
  - for websites and mobile apps, organizations must unequivocally revoke or restrict a user's access if necessary through cease and desist notices and other technological measures.
- Limit employees' computer access to only what is strictly necessary to perform their roles. However, even in these circumstances, many courts will not support a CFAA claim if the employee misuses information to which he had access.

DESCRIBE PERMITTED ACCESS AND USE IN POLICIES AND EMPLOYMENT AGREEMENTS

In considering whether an individual exceeded authorized access under the CFAA, certain courts focus on whether the misuse of information that the company permitted the individual to access violates of an employment agreement or company policy (see, for example, *EF Cultural BV*, 274 F.3d at 581-82 and Exceeding Authorization).

Organizations should carefully review internal policies, such as employee acceptable use policies, and public-facing terms of service. These documents should include:

- Language addressing what the individual has access to on the computer or website and an explicit statement on the website restricting access.
- In the employment context:
  - a broad confidentiality agreement prohibiting the disclosure of any information that is contrary to the interests of the employer; and
  - an Acceptable Use Policy addressing proper use of employer IT resources and electronic communications systems.
- In the commercial context, a terms of use agreement that defines prohibited uses of public-facing websites or applications.

For guidance on drafting confidentiality agreements, acceptable use policies, and terms of service agreements, see:

- Drafting an Employee Confidentiality Agreement: Best Practices Checklist (0-523-2392).

- Standard Document, Employee Confidentiality and Proprietary Rights Agreement (6-501-1547).
- Standard Document, IT Resources and Communications Systems Policy (8-500-5003).
- Standard Document, Website Terms of Use (3-501-3816).

DOCUMENT DATE OF DISCOVERY OF COMPUTER FRAUD

Plaintiffs must bring CFAA actions within two years from the date of either:

- The defendant's act.
- The plaintiff's discovery of the unauthorized computer access or damage.

(18 U.S.C. § 1030(g).)

To ensure that their CFAA claims are timely, organizations should:

- Carefully document the date on which they discovered the unauthorized access or computer damage.
- Promptly retain a forensic investor to learn to scope of the damage and the identity of the perpetrator if not known.

DOCUMENT ALL LOSSES ASSOCIATED WITH THE COMPUTER FRAUD

In most civil CFAA actions, plaintiffs must allege facts that they suffered a loss of $5,000 during any one-year period related to either or both:

- The costs of responding to the event such as investigating or remedying damage to the computer (see Costs).
- Revenue lost, cost incurred, or other consequential damages incurred because of an interruption of service (see Lost Revenue and Consequential Damages).

Organizations may combine response and interruption costs to meet the $5,000 threshold. However, they should separately document those costs because organizations can recover lost revenue and consequential damages only if they stem from an interruption of service (*M-I LLC v. Stelly*, 733 F. Supp. 2d 759, 779-780 (S.D. Tex. 2010) (noting that case law has consistently interpreted the loss provision to encompass only the costs incurred as a result of investigating or remedying damage, or costs incurred because the computer's service was interrupted)).

Costs

The types of response costs that typically qualify for the $5,000 loss are those necessary to assess the damage caused to the computer or to restore the system following an attack. Organizations should fully document all costs incurred to respond to the computer fraud including:

- Costs for engaging forensic and investigative services after an incident involving unauthorized access or damage.
- Value of the time of employees who investigate the event and remedy any computer damage.
- Diagnostic measures performed.
- Costs to repair damages to a computer.

Courts may reject unsupported allegations that the organization hired a computer expert without a description of the type of investigation conducted or how the computer system was interrupted, damaged, or restored (see, for example, *Chas. S. Winner, Inc. v. Polistina*, 2007 WL 1652292, at *4 (D.N.J. June 4, 2007)). Organizations should therefore provide as much detail as possible about the costs and their connection to the computer investigation and repair.

Lost Revenue and Consequential Damages

Organizations that suffer an interruption of service must promptly assess and document any lost revenue and consequential damages to ensure these losses qualify toward the $5,000 threshold requirement. Specifically, organizations should document:

- All computers and systems affected by the interruption of service.
- The start and end time of the interruption.
- The business divisions impacted.
- Potential lost profits, including:
  - inability to fulfill customer orders; or
  - lost value of prospective customers.

CRIMINAL PENALTIES UNDER THE COMPUTER FRAUD AND ABUSE ACT

Violation	Imprisonment
Section 1030(a)(1)	First offense: not more than 10 years. Prior offense: not more than 20 years.
Section 1030(a)(2)	First offense where fraud is less or equal to $5,000: not more than one year. First offense where fraud is greater than $5,000: not more than 5 years. Prior offense: not more than 10 years.
Section 1030(a)(3)	First offense: not more than one year. Prior offense: not more than 10 years.
Section 1030(a)(4)	First offense: not more than 5 years. Prior offense: not more than 10 years.
Section 1030(a)(5)	First offense where fraud is less than or equal to $5,000: not more than one year. Prior offense where fraud is less than or equal to $5,000: not more than 10 years. Prior offense where fraud is less than or equal to $5,000 and defendant acts intentionally or recklessly: not more than 20 years. First offense where fraud is greater than $5,000: not more than 10 years. Prior offense where fraud is greater than $5,000: not more than 20 years.
Section 1030(a)(6)	First offense: not more than one year. Prior offense: not more than 10 years.
Section 1030(a)(7)	First offense: not more than 5 years. Prior offense: not more than 10 years.

09-18