Strategies for Businesses Protecting Electronic Data within California: Part One

06.10.2015

**Updated June 2019.*

PART ONE: The Computer Fraud And Abuse Act (18 U.S.C. § 1030 Et Seq.)

Data security is top-of-mind in today's corporate world. According to The Ponemon Institute's 2015 Cost of Data Breach Study, the **average** total cost of a data breach for the 350 participating organizations increased 23 percent during the past two years to $3.79 million. Businesses in California are equipped with a number of tools to help battle unauthorized intrusions into their electronic data, whether by employees, former employees, disreputable competitors or random hackers. Knowledge of these tools is essential for counsel to advise clients on preventive and remedial measures.

Data security is top-of-mind in today's corporate world. According to The Ponemon Institute's 2015 Cost of Data Breach Study, the total cost of a data breach for the 350 participating organizations increased 23 percent during the past two years to $3.79 million. Businesses in California are equipped with a number of tools to help battle unauthorized intrusions into their electronic data, whether by employees, former employees, disreputable competitors or random hackers. Knowledge of these tools is essential for counsel to advise clients on preventive and remedial measures.

This e-alert is the first of three spanning the next three weeks that together should constitute a primer on three key statutes that can help businesses deal with breaches of electronic security. The statutes include the federal Computer Fraud And Abuse Act, 18 U.S.C. § 1030 et seq.; the California Computer Data Access And Fraud Act, Cal. Pen. Code, § 502; and the federal Stored Communications Act, 18 U.S.C. § 2701 et seq. This first alert addresses the Computer Fraud and Abuse Act, while the final alert will include best practices to help businesses preserve the integrity of their electronic data.

1. Summary of Prohibitions

The Computer Fraud And Abuse Act (CFAA), 18 U.S.C. § 1030 et seq., applies to a protected computer which the statute defines as one which is used in or affecting interstate or foreign commerce or communication. (*Id.* § 1030(e)(2); see generally, 1 Serwin, *Information Security and Privacy - A Guide To Federal And State Law And Compliance* (2017) Ch. 5, pp. 171 et seq.) The CFAA prohibits, among other things:

(A) knowingly caus[ing] the transmission of a program, information, code, or command and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer;
(B) intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage; or
(C) intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss.

(*Id.* § 1030(a)(5)(A)-(C).)

Additionally, the CFAA makes it unlawful to knowingly and with the intent to defraud, [access] a protected computer without authorization, or [exceed] authorized access, and by means of such conduct [further] the intended fraud or [obtain] anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1 year. (*Id.* § 1030 (a)(4); see *Fidlar Techs v. LPS Real Estate Data Solutions, Inc.* (7th Cir. 2016) 810 F.3d 1075, 1079 [intent to defraud means that the defendants acted willfully and with specific intent to deceive or cheat, usually for the purpose of getting financial gain for himself or causing financial loss to another.].)[1]

While it is a criminal statute, the CFAA also provides a civil remedy to any person who suffers damage or loss by reason of a violation of [the act]. (*Id.* § 1030(g)). Such person may obtain compensatory damages and equitable (including injunctive) relief. (*Ibid.*) For a civil plaintiff to recover, subsection 1030(g) requires that the plaintiff allege and prove that the offensive conduct caused any one of the following five circumstances set forth in 18 U.S.C. § 1030(c)(4)(A)(i), namely:

1. Loss to 1 or more persons during any 1-year period, aggregating $5,000 in value;
2. The modification, impairment, or potential modification or impairment of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
3. Physical injury to any person;
4. A threat to public health or safety;
5. Damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security. (18 U.S.C. § 1030(c)(4)(A)(i)(I)-(V).)

As the Ninth Circuit summarized in *LVRC Holdings LLC v. Brekka* (9th Cir. 2009) 581 F.3d 1127, 1132: a civil plaintiff suing under subsection 1030(a)(2) must show that a defendant (1) intentionally accessed a computer, (2) without authorization or exceeding authorized access, and that he (3) thereby obtained information (4) from any protected computer [,] and that (5) there was a loss to one or more persons during any one-year period aggregating at least $5,000 in value. In contrast, a plaintiff suing under subsection 1030(a)(4) must prove that a defendant (1) accessed a 'protected computer,' (2) without authorization or exceeding such authorization that was granted, (3) 'knowingly' and with 'intent to defraud,' and thereby (4) 'further[ed] the intended fraud and obtain[ed] anything of value,' causing (5) a loss to one or more persons during any one-year period aggregating at least $5,000 in value. (*Ibid.*; citations omitted.)

Both subsections (a)(2) and (a)(4) prohibit access to a protected computer without authorization or in excess of authorization. (*Facebook, Inc. v. Power Ventures, Inc.* (9th Cir. 2016) 844 F.3d 1058, 1066, quoting *Musacchio v. United States* (2016) 136 S. Ct. 709, 713 [The statute thus provides two ways of committing the crime of improperly accessing a protected computer: (1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly.].) Additionally, fraud under the CFAA only requires a showing of unlawful access and does not require proof of common law fraud. (*eBay Inc. v. Digital Point Solutions, Inc.* (N.D.Cal. 2009) 608 F.Supp.2d 1156, 1164.)

The CFAA is "designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to access and control high technology processes vital to our everyday lives." (*LVRC Holdings LLC v. Brekka, supra*, 581 F.3d at p. 1130.) The CFAA is not meant to serve as a supplement or replacement for misappropriation claims. (*United States v. Nosal* (9th Cir. 2012) 676 F.3d 854, 862–63 (en banc); see also *Craigslist Inc. v. 3Tops, Inc.* (N.D.Cal. 2013) 942 F.Supp.2d 962, 968–970 [CFAA governs access not use]; *Omega Morgan, Inc. v. Heely* (W.D.Wash. April 29, 2015, No. C14-556RSL) 2015 U.S.Dist. Lexis 56288, a pp. *15–*16 [trade secrets act preempts CFAA claim that defendants used company servers to copy confidential information; however, claim that defendants wiped computers of information is a viable claim under the CFAA].)[2]

The limitations period under the CFAA is 2 years from the date of the action complained of or the date of discovery of the damage. (18 U.S.C. § 1030(g).)

2. "Without Authorization"

The CFAA requires that a defendant access a protected computer without authorization. According to the Ninth Circuit in *Brekka, supra*, 581 F.3d at p. 1133,

> [A] person who uses a computer without authorization has no rights, limited or otherwise, to access the computer in question. In other words, for purposes of the CFAA, when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the computer even if the employee violates those limitations.

Further addressing without authorization, the Ninth Circuit stated:

> [A] person uses a computer without authorization under §§ 1030(a)(2) and (4) when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.

(*Id*. at p. 1135; see also *Facebook, Inc. v. Power Ventures, Inc., supra*, 844 F.3d at pp. 1067–68 [defendant violated CFAA where although it did initially have access to plaintiff's social networking website, it accessed plaintiff website's computer without authorization after plaintiff rescinded permission by issuing a cease and desist letter and imposed IP blocks]; *In re iPhone Application Litig.* (N.D.Cal. 2012) 844 F.Supp.2d 1040,1064–1066 [where iDevice users voluntarily downloaded free applications that contained software that obtained and retrieved certain personal information such as geographic location, Apple did not violate the CFAA].) Therefore, a defendant can violate the CFAA when he or she has no permission to access a computer or when such permission has been explicitly revoked. (*Facebook, Inc. v. Power Ventures, Inc., supra*, 844 F.3d at p. 1067.) Once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability. (*Ibid*.)

It appears that the weight of authority does not require circumvention of technological access barriers (e.g., unauthorized use of passwords and evading a firewall) for use to be considered unauthorized. (*NetApp., Inc. v. Nimble Storage, Inc.* (N.D.Cal. 2014) 41 F.Supp.3d 816, 831–832.) In *United States v. Nosal* (9th Cir. 2016) 844 F.3d 1024, 1038–1039, the Ninth Circuit held that a showing that a party circumvents a technological access barrier is not necessary to prove access was unauthorized and in violation of the CFAA. The federal court reasoned that not only is such a requirement missing from the statutory language, but such requirement would make little sense because some [section] 1030 offenses do not require access to a computer at all. (*Ibid.* [explaining [h]ad a thief stolen an employee's password and then used it . . . access would have been without authorization.].); see also *United States v. Nosal* (N.D.Cal. 2013) 930 F.Supp.2d 1051, 1060 [suggesting that unauthorized access does not require circumvention of technological access barriers].)[4] Ninth Circuit authority . . . indicates that if a former employee accesses information without permission, even if his prior log-in information is still operative as a technical matter, such access would violate the CFAA. (*Weingand v. Harland Financial Solutions, Inc.* (N.D.Cal. June 19, 2012, No. C-11-3109 EMC) 2012 U.S.Dist. Lexis 84844, at p. *9, citing *LVRC Holdings LLC v. Brekka, supra*, 581 F.3d at p. 1136 [There is no dispute that if Brekka accessed LVRC's information on the LOAD website after he left the company in September 2003, Brekka would have accessed a protected computer 'without authorization' for purposes of the CFAA.].)

It is a factual issue whether a defendant has exceeded authorization. (*Weingand v. Harland Financial Solutions, Inc., supra*, 2012 U.S.Dist. Lexis 84844 at pp. *9–*10; see also *Synopsys, Inc. v. ATopTech, Inc., supra*, 2013 U.S.Dist. Lexis 153089, at p. *34 [[T]he state of CFAA doctrine in the Ninth Circuit suggests that while a breach of a contractual provision may in some cases be enough to allege unauthorized access, such an alleged breach must be pled with enough clarity and plausibility to state that access itself—not just a particular use—was prohibited. (Citation omitted.)].) Thus, it is important to clearly delineate the scope of authorization in writing if practicable. Moreover, employment policy manuals, employment agreements and consulting agreements should make clear that when an employee leaves employment, authority to access computer systems is terminated whether or not log in access is disabled. Of course, an employer should disable log-in access upon an employee's or consultant's termination.

3. Exceeding Authorized Access

While a defendant may not have accessed a computer without authorization, he may still have exceeded authorized access. Exceeding authorized access, as noted above, can be a basis for a CFAA violation. The phrase exceeds authorized access means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter. (18 U.S.C. § 1030(e)(6).)

According to the Ninth Circuit in *United States v. Nosal*, supra, 676 F.3d at p. 864, exceeding authorized access is limited to violations of restrictions on access to information, and not restrictions on its use. For example, an employee who is given access to **product information** on a company computer but who accesses **customer data** would exceed authorized access.[5] In contrast, an employee who has access to customer lists but is not authorized to send them out would not violate the CFAA by doing both. The latter conduct may be the subject of a claim for misappropriation of trade secret. (*Id.* at pp. 857–63.) In sum, one who exceeds authorized access is someone who is authorized to access only certain data or files but accesses unauthorized data or files—which is colloquially known as 'hacking.' (*Id.* at pp. 856–857; internal quotes omitted.) The CFAA is not applicable to a person who is authorized to access a computer or parts of

the computer but who, in so doing, misuses or misappropriates information. (*Id*. at p. 863.)[6]

4. Damages And Other Relief

As noted, subsection 18 U.S.C. § 1030(g) provides a private remedy to a person who suffers damage or loss by reason of certain violations of the CFAA. With respect to 18 U.S.C. § 1030(c)(4)(A)(i)(I),loss to 1 or more persons during any 1-year period, aggregating $5,000 in value, recovery under the CFAA is limited to only economic damages. (See 18 U.S.C. § 1030(g); *Hancock v. County of Rensselar* (2d Cir. 2018) 882 F.3d 58,63.) [T]he $5,000 floor applies to how much damage or loss there is to the victim over a one-year period, not from a particular intrusion. (*Creative Computing v. Getloaded.com, LLC* (9th Cir. 2004) 386 F.3d 930, 935.) The statute does not require $5,000 in damages for each single intrusion. (*Ibid*.)

18 U.S.C. § 1030(e)(8) defines damage to mean any impairment to the integrity or availability of data, program, a system, or information. 18 U.S.C. § 1030(e)(11) provides that loss means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service. (*Creative Computing v. Getloaded.com, LLC, supra*, 386 F.3d at pp. 935–936.) The compensable damages are not limited to the precise time that the unauthorized access is occurring. (*Facebook, Inc. v. Power Ventures, Inc.* (N.D.Cal. 2017) 252 F.Supp.3d 765, 778 [costs are compensable as long as those costs were reasonably incurred responding to the offense].)[7]

[D]istrict courts in the Ninth Circuit have held that it is not necessary for data to be physically changed or erased to constitute damage to that data. (*Multiven, Inc. v. Cisco Sys., Inc.* (N.D.Cal. 2010) 725 F.Supp.2d 887, 894–95.) It is sufficient to show that there has been an impairment to the integrity of data, as when an intruder retrieves password information from a computer and the rightful computer owner must take corrective measures 'to prevent the infiltration and gathering of confidential information.' (*Ibid*.; citations omitted; accord *NovelPoster v. Javitch Canfield Group, supra*, 140 F.Supp.3d at pp. 947–48; cf. *In re iPhone Application Litig., supra*, 844 F.Supp.2d at pp. 1065–70 [alleged cost of memory space on iphones on downloaded applications monitoring iPhone users was insufficient to establish $5,000 damage minimum].)

Cognizable costs . . . include 'the costs associated with assessing a hacked system for damages [and] upgrading a system's defenses to prevent future unauthorized access.' (*AtPac, Inc. v. Aptitude Solutions, Inc.* (E.D.Cal. 2010) 730 F.Supp. 2d 1174, 1184, quoting *Doyle v. Taylor* (E.D.Wash. May 24. 2010, No. 09-158) 2010 U.S.Dist. Lexis 51058, at p. *8.) Moreover, where the offense involves unauthorized access and the use of protected information[,] . . . the cost of discovering the identity of the offender or the method by which the offender accessed the protected information [is] part of the loss for purposes of the CFAA. (*SuccessFactors, Inc. v. Softscape, Inc.* (N.D.Cal. 2008) 544 F.Supp.2d 975, 981; see also *Brown Jordan International, Inc. v. Carmicle, supra,* 846 F.3d at pp 1172-1176 [allowing recovery of (a) cost to outside consultant to determine how defendant accessed e-mails and (b) payment to security firm to sweep office building for audio and video surveillance devices.]; *Facebook, Inc. v. Power Ventures, supra*, 844 F.3d at p. 1066 [in-house employee time spent analyzing, investigating, and responding to defendant's actions counted towards the $5,000 damage]; *Mintz v. Mark Bartelstein and Associates, Inc.* (C.D.Cal. 2012) 906 F.Supp.2d 1017, 1029 [courts in the Ninth Circuit have recognized the general principle that 'costs associated with investigating intrusions into a computer network and taking subsequent remedial measures are losses within the meaning of the statute.]; *Vaquero Energy, Inc. v. Herda, supra*, 2015 U.S.Dist. Lexis 115717, at pp.*20-*23 [damages included cost of expert to attempt to access password blocked computer system]; cf. *Mintz v.*

Mark Bartelstein and Associates, Inc., supra, 906 F.Supp.2d at pp. 1029–1031 [rejecting litigation expenses as satisfying the $5,000 threshold because the litigation costs in question were not essential in remedying the harm of the unauthorized access]; *Turner v. Hubbard Systems, Inc.* (3d Cir. 2017) 855 F.3d 10, 13 [plaintiff failed to prove loss of $5,000].)

Loss of business and business goodwill are included within economic damages. (*Creative Computing v. Getloaded.com, LLC, supra*, 386 F.3d at p. 935.) When an individual or firm's money or property are impaired in value, or 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.' (*Ibid*.; cf. *New Show Studios LLC v. Needle* (C.D.Cal. June 30, 2014, No. 2:14-cv-01250-CAS (MRWx)), U.S.Dist. Lexis 90656, at p. *19 [[S]ubsequent economic damage unrelated to the computer itself does not constitute 'loss.' Here, the only 'loss' alleged by plaintiffs is 'competitive[] benefit[]' to their competitor . . .; plaintiffs do not allege that their computer systems were damaged in any way.]; *AtPac, Inc. v. Aptitude Solutions, Inc., supra*, 730 F.Supp.2d at pp. 1184–85 [To allege a loss of revenue, the loss must result from the unauthorized server breach itself.].) Economic damages under 18 U.S.C. § 1030(c)(4)(A)(i)(I) precludes damages for death, personal injury, and mental distress. (*Ibid*.)

One must be careful in pleading damages. For example, in *NovelPoster v. Javitch Canfield Group, supra*, 140 F.Supp.3d at p. 949, the district court granted a motion for judgment on the pleadings (albeit with leave to amend) for a CFAA claim on which the plaintiff alleged that it has suffered damages and/or loss in excess of $5,000 in the year preceding the date of this filing, but the damages grow each day . . . . According to the district court, this allegation was merely conclusory and speculative. (*Ibid*.; see also *In re Google Android Consumer Privacy Litigation* (N.D.Cal. March 26, 2013, No. 11-MD-02264 JSW) 2013 U.S.Dist. Lexis 42724, at pp. *21–*24 [bare legal conclusions as to purported costs incurred and couched as fact are insufficient].)

Injunctive relief under 18 U.S.C. § 1030(g) can include prohibition of a defendant's access even to publicly available websites for past egregious and numerous instances of violations. (*Creative Computing v. Getloaded.com, LLC, supra*, 386 F.3d at pp. 937–38; see also *Facebook, Inc. v. Grunin* (N.D.Cal. 2015) 77 F. Supp.3d 965, 973–974 [reasoning public interest would be served by granting a permanent injunction preventing defendant from accessing or using social networking website and services where website had terminated more than 70 fraudulent accounts].) Subsection 1030(g) also provides for other equitable relief without further specifying what that relief may be. It could possibly mean disgorgement of profits (a remedy specifically available under the Stored Communications Act, 18 U.S.C. § 2701 et seq. discussed below) or restitution/restoration (also available under California's Unfair Competition Law, Bus. & Prof. Code, § 17203).

The CFAA does not expressly provide for attorney's fees. (*Leibert Corp. v. Mazur* (N.D.Ill. Sept. 16, 2004, No. 04 C 3717) 2004 U.S.Dist. Lexis 18797, at p. *10; *Tyco International (US) Inc. v. John Does, 1-3* (S.D.N.Y. Aug. 29, 2003, No. 01 Civ. 3856 (RCC) (DF)) 2003 U.S.Dist. Lexis 25136, at pp. *15–*16; see 18 U.S.C. § 1030(g) [containing no provision for attorney's fees].) However, as discussed below, attorney's fees are available under section 502 of the California Penal Code (California Computer Data Access And Fraud Act) and the Stored Communications Act (18 U.S.C. § 2707(b)(3)) for similar conduct. Thus, it will usually be advisable to combine claims under the CFAA with claims under the California statute and the Stored Communications Act where possible. (See, e.g., *Tech Systems, Inc. v. Pyles* (E.D.Va. Aug. 6, 2013, No. 1:12-CV-374 (GBL/JFA)) 2013 U.S.Dist. Lexis 110636, at pp. *12–*14 [attorney's fees available under Virginia Computer Crimes Act were also available for CFAA claim where the claims shared common facts]; cf. *Dice Corp. v. Bold Techs* (E.D. Mich. June 18, 2014, No. 11-cv-13578) 2014 U.S.Dist. Lexis 82591, at p. *58 [defendant entitled to fees in

defense of copyright claim was also entitled to fees associated with defense of CFAA claim where the claims arose from the same alleged set of facts].)

Read Part Two here.

Read Part Three here.

[1] In *Ticketmaster LLC v. Prestige Entertainment West, Inc.* (C.D.Cal. May 29, 2018 No. 2:17-cv-07232-ODW-JC) 2018 U.S.Dist. Lexis 89347, involved application of 18 U.S.C. § 1030(a)(4). In the case, the district court applied the section to the defendants' use of automated bots to obtain from Ticketmaster large numbers (thousands) of tickets to popular events. The conduct was contrary to Ticketmaster's terms of use and continued after Ticketmaster served the defendants with a cease and desist letter. The court ruled that plaintiff's allegations of the scheme which the defendants utilized were sufficient under rule 9(b) of the Federal Rules of Civil Procedure to defeat a motion to dismiss. (*Id*., pp. *56-*57.)

[2] In *Omega Morgan, Inc. v. Heely* (W.D.Wash. April 29, 2015, No. C14-556RSL) 2015 U.S.Dist. Lexis 56288, at pp. *15–*16, the district court allowed both a CFAA claim and a claim under the Stored Communications Act to proceed where the defendants wiped their computers of information prior to terminating their employment with the plaintiff. (Cf. *Vaquero Energy, Inc. v. Herda* (C.D.Cal. Aug. 28, 2013, No. 1:15-cv-0967-JLT) 2015 U.S.Dist. Lexis 115717 [preliminary injunction issued compelling consultant to turn over passwords he installed to prevent owner from accessing computers; conduct was both without authority and exceeded authority]; *NovelPoster v. Javitch Canfield* (N.D.Cal. 2014) 140 F.Supp.3d 938, 941, 944–951 [defendants changed passwords preventing plaintiff's access to business information and exposed themselves to claims of violating section 502 of the California Penal Code and the CFAA].)

[3] The Ninth Circuit chose not to decide whether websites, such as Facebook, are presumptively open to all comers, unless and until permission is revoked expressly. (*Facebook, Inc. v. Power Ventures, Inc., supra*, 844 F.3d at p. 1067, fn. 2.)

[4] See also *Synopsys, Inc. v. ATopTech, Inc.* (N.D.Cal. Oct. 24, 2013, No. C 13-2965 SC) 2013 U.S.Dist. Lexis 153089, at pp. * 32–*33:

It is true that some courts have held that the CFAA applies to access restrictions that are contractual, as well as technological restrictions. See *Weingand v. Harland Fin. Solutions, Inc*., No. C 11-3109 EMC, 2012 U.S. Dist. LEXIS 84844, 2012 WL 2327660, at *3 (N.D.Cal. June 19, 2012); see also *Nosal*, 676 F.3d at 864 (distinguishing between access restrictions and use restrictions, but not the form of the restrictions); *Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 2013 U.S. Dist. LEXIS 61837, 2013 WL 1819999, at *3-4 (N.D. Cal. Apr. 30, 2013) (noting Nosal's distinction). But other courts have asserted that statutes like the CFAA apply only to breaches of technical barriers. See, e.g., *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 715-16 (N.D.Cal. 2011) (holding, in a California Penal Code section 502 case, that the rule of lenity requires interpreting access "without permission" to apply only to access exceeding technical barriers); *Facebook, Inc. v. Power Ventures, Inc.*, No. C 08-05780-JW, 2010 U.S. Dist. LEXIS 93517, 2010 WL 3291750, at *11 (N.D. Cal. July 20, 2010) (same).

[5] Accord, *WEC Carolina Energy Solutions LLC v. Miller* (4th Cir. 2012) 687 F.3d 199, 203; see also *United States v. Valle* (2d Cir. 2015) 807 F.3d 508, 511–12 (employee did not violate the CFAA by putting his authorized computer access to personal use); contra *United States v. Teague* (8th Cir. 2011) 646 F.3d 1119,

1121–1122 (although having access to computer data, government employee had no legitimate purpose in specifically accessing President Obama's student loan records); *United States v. Rodriguez* (11th Cir. 2010) 628 F.3d 1258, 1263 (employee had authorized access to databases but used such access for an improper purpose in obtaining information concerning seventeen women); *United States v. John* (5th Cir. 2010) 597 F.3d 263, 271–273 (employee exceeded authorized access when she used employer information, to which she had access for other purposes, to perpetrate a fraud); *Int'l Airport Ctrs., LLC v. Citrin* (7th Cir. 2006) 440 F.3d 418, 420 (employee's authorization to use employer's laptop ended once he violated duty of loyalty to employer, and thus employee accessed computer without authorization); *EF Cultural Travel BV v. Explorica, Inc.* (1st Cir. 2001) 274 F.3d 577, 583–584 (exceeds authorized access encompasses breach of an employer confidentiality agreement where disloyal employee allegedly helped competitor obtain proprietary information).

[6] For additional cases on exceeding access see: *Shamrock Foods Co. v. Gast* (D.Ariz. 2008) 535 F.Supp.2d 962, 967–968 (holding that a violation for exceeding authorized access occurs where initial access is permitted but access to certain information is not permitted, and dismissing CFAA claim because defendant admittedly was permitted to view the specific files at issue); *Diamond Power International, Inc. v. Davidson* (N.D.Ga. 2007) 540 F.Supp.2d 1322, 1342–1343 (exceeding authorized access included an employee who accesses a computer with initial authorization but later acquires, with an improper purpose, files to which he is not entitled).

[7] The court in *Facebook, Inc. v. Power Ventures, Inc., supra*, 252 F.Supp.3d 765, 778, reasoned that its decision was consistent with the plain language of the statute and the following persuasive case law: *Brown Jordan Int'l, Inc. v. Carmicle* (11th Cir. 2017) 846 F.3d 1167, 1174–75 (affirming damages award for extensive forensic and physical review of [the victim's] systems to determine the extent of . . . hacking activity after a hack occurred); *EF Cultural Travel BV v. Explorica, Inc.* (1st Cir. 2001) 274 F.3d 577, 584 fn. 17 (affirming damages award for money plaintiffs paid to assess whether their website had been compromised); *A.V. ex rel. Vanderhye v. iParadigms, LLC* (4th Cir. 2009) 562 F.3d 630, 646 (the costs of responding to the offense are recoverable including costs to investigate and take remedial steps (internal quotations omitted)).