NOSSAMAN LLP

STRATEGIES FOR BUSINESSES PROTECTING ELECTRONIC DATA WITHIN CALIFORNIA

By

STEPHEN P. WIMAN

PARTNER

NOSSAMAN LLP

STRATEGIES FOR BUSINESSES PROTECTING ELECTRONIC DATA WITHIN CALIFORNIA

Businesses in California have a number of tools with which to fight off unauthorized intrusions into their electronic data whether perpetrated by employees, former employees, disreputable competitors or random hackers. Knowledge of these tools is essential for counsel to advise their clients both as to preventive and remedial measures. Set forth below is a primer on three key statutes which businesses have in their arsenal to deal with breaches of electronic security. They are 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.

Working hand in glove with these statutory provisions, businesses should undertake preventive measures to minimize the need to resort to the statutes. The last section below contains specific recommendations to protect the businesses' electronic data.

THE COMPUTER FRAUD AND ABUSE ACT (18 U.S.C. § 1030 ET SEQ.)

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).) 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).)

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, section 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 **section 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 person during any one-year period aggregating at least $5,000 in value." In contrast, a plaintiff suing under section **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, *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].)[1]

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.

[1] In *Omega Morgan, Inc. v. Heely* (W.D.Wash., April 29, 2015, No. C14-556RSL) 2015 U.S. Dist. Lexis 56288, *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., Sept. 3, 2013, No. 1:15-cv-0967-JLT) 2015 WL 5173535, *5–*7 [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].)

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. 1067–1068 [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.)[2] “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].)[3] “Ninth Circuit

[2] 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.)

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

> It is true that some courts have held that the CFAA applies to access restrictions that are contractual, as well as

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, *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 S*ynopsys, 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

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).

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.[4] 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. 857–863.) 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 p. 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; see also *Facebook, Inc. Power Ventures*, *supra*, 844 F.3d at p. 1067 ["[A] violation of the terms of use of a website [or information]—without more—cannot establish liability under the CFAA."]; *Welenco, Inc. v. Corbell* (E.D.Cal. 2015) 126 F.Supp.3d 1154, 1169 [defendant did not exceed his authorized access where files used to form competitor were not "hacked," there was no breach of security protocols, and he only accessed files he was authorized to access].)[5]

[4] 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, 511–512 (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).

[5] For additional cases on exceeding access see: *Vaquero Energy, Inc. v. Herda*, *supra*, 2015 WL 5173535, *5–*7; *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

4. Damages And Other Relief

As noted, section 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).) "[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., May 2, 2017, No. 08-CV-05780-LHK) 2017 U.S. Dist. Lexis 66948, *31 [costs are compensable "as long as those costs were reasonably incurred responding to the offense"].)[6]

"[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, 894–895.) "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. 947–948; cf. *In re iPhone Application Litig.*, *supra*, 844 F.Supp.2d at pp. 1065–1070 [alleged cost of memory space on iphones on downloaded

employee who accesses a computer with initial authorization but later acquires, with an improper purpose, files to which he is not entitled).

[6] The court in *Facebook, Inc. v. Power Ventures, Inc.*, *supra*, 2017 U.S. Dist. Lexis at pp. *30–*31, 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, 1174–1175 (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)).

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, *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 *Power Ventures*, *supra*, 844 F.3d at p. 1066 [employee time spent analyzing, investigating, and responding to defendant's actions counted towards the $5,000 damage]; *Vaquero Energy, Inc. v. Herda*, *supra*, 2015 WL 5173535, *5–*7 [damages included cost of expert to attempt to access password blocked computer system]; cf. *Mintz v. Mark Bartelstein and Associates, Inc.* (C.D.Cal. 2012) 906 F.Supp.2d 1017, 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].) "[C]ourts 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. (*Mintz v. Mark Bartelstein and Associates, Inc.*, *supra*, 906 F.Supp.2d at 1029.)

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, *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. 1184–1185 ["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 Litig.* (N.D.Cal., March 26, 2013, No. 11-MD-02264 JSW) 2013 U.S. Dist. Lexis 42724, *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. 937–938; 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].) Section 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, *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, *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, *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, *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].)

California Computer Data Access And Fraud Act (Cal. Pen. Code, § 502)

1. Summary Of Prohibitions

The California Computer Data Access And Fraud Act ("CDAFA"), Cal. Pen. Code, § 502, is similar to the federal Computer Fraud And Abuse Act ("CFAA"), 18 U.S.C. § 1030 et seq. (See *Craigslist Inc. v. 3Taps Inc.* (N.D.Cal. 2013) 942 F.Supp.2d 962, 968 [identifying the California statute as a state law corollary to the federal statute].) "The CDAFA is similar to the CFAA, but prohibits a wider range of conduct. (See Cal. Pen. Code, § 502(c)(1)–(9).) Furthermore, it contains no minimal loss requirement in order to support a private right of action." (*DocMagic, Inc. v. Ellie Mae Inc.* (N.D.Cal. 2010) 745 F.Supp.2d 1119, 1150.)

However, according to the Ninth Circuit, there is a significant difference between the California and federal statute. (See *United States v. Christensen* (9th Cir. 2016) 828 F.3d 763, 789.) The federal court stated that, "the California statute does not require *unauthorized* access. It merely requires *knowing* access." (*Ibid.* [choosing not to interpret the CDAFA consistently with the CFAA as interpreted by *Nosal*]; *see also Power Ventures, Inc.*, *supra*, 844 F.3d at p. 1069 [reaffirming that the California statute is "different" than the CFAA].) According to the court, "what makes access unlawful is that the person 'without permission takes, copies, or makes use of' data on the computer." (*Christensen*, *supra*, 828 F.3d at p. 789 [CFAA criminalizes *unauthorized access*, while the California statute criminalizes *unauthorized taking or use of information*], emphasis added.) Yet, the court acknowledged that there is currently a split of authority in the California courts on the issue addressed by *Christensen* (for a greater discussion on the case, see "The Ninth Circuit Holds That California's Anti-Hacking Law, Penal Code Section 502, Does Not Proscribe Unauthorized 'Access' To A Database; Rather The Section Prohibits Unauthorized Use, Copying or Manipulation of Information In The Database." <http://www.jdsupra.com/legalnews/the-ninth-circuit-holds-that-california-73048/>)

In addition to criminal sanctions, the CDAFA provides a civil remedy for an owner of a "computer, computer system, computer network, computer program or data who suffers damage or loss by reason of a violation of any of the provisions of [Cal. Penal Code § 502(c)]." (Cal. Pen. Code, § 502(e).) Section 502(c) of the California Penal Code, inter alia, lists the following violations regarding "knowingly accessing" and using "without permission" a computer or data from a computer:

(1) knowingly accessing and without permission altering, damaging, deleting, destroying, or otherwise using any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to

defraud, deceive, or extort, or (B) wrongfully controlling or obtaining money, property, or data;[7]

(2) knowingly accessing and without permission taking, copying, or making use of any data from computer, computer system, or computer network, or taking or copying any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network;[8]

(3) knowingly and without permission using or causing to be used computer services;

(4) knowingly accessing and without permission adding, altering, damaging, deleting, or destroying any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network, computer system, or computer network;

(5) knowingly and without permission disrupting or causing the disruption of computer services or denying or causing the denial of computer services to an authorized user of a computer, computer system, or computer network;[9]

[7] See *People v. Tillotson* (2007) 157 Cal.App.4th 517, 537–540 (jury instruction on elements of violation of section 502(c)(1) failed to include the requirement that the defendant "without permission alters, damages, deletes, destroys, or otherwise uses the data obtained from . . . access."); see also *People v. Gentry* (1991) 234 Cal.App.3d 131, 140–141 (defendant convicted under prior version of the CDAFA for fraudulently accessing credit evaluation companies computers and entering false information to create false identities).

[8] *Facebook, Inc. v. ConnectU LLC* (N.D.Cal. 2007) 489 F.Supp.2d 1087, 1090–1091, applied this subsection to a defendant that accessed information available only to registered users. The defendant used log-in information voluntarily supplied by registered users and contended that it had not violated the subsection because it had not gained "unauthorized" access. The district court rejected the argument observing that the subsection required "knowingly" accessing a computer and "without permission" taking, copying, or making use of data on the computer. In other words, the phrase "without permission" relates to the taking, copying or making use of data on the computer, not the access.

[9] Penal Code section 502(c)(5) is unique in that it does not require access without permission. In *People v. Childs* (2013) 220 Cal.App.4th 1079, a jury convicted the defendant of locking the City and County of San Francisco out of its computer system. The defendant, a network engineer for the City and County, had violated section 502(c)(5) of the Penal Code. On appeal, the defendant argued that the court should interpret section 502(c)(5) to require accessing a computer system without permission. Since he had access to the computer system via his employment, he thus claimed that he had not violated section 502(c)(5). After extensive discussion, the Court of Appeal rejected the defendant's argument, holding that the statute was unambiguous and clear:

(6) knowingly and without permission providing or assisting in providing a means of accessing a computer, computer system, or computer network in violation of this section;

(7) knowingly and without permission accessing or causing to be accessed any computer, computer system, or computer network;[10]

(8) knowingly introducing any computer contaminant into any computer, computer system, or computer network; and

(9) knowingly and without permission using the Internet domain name or profile of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages or posts and thereby damages or causes damage to a computer, computer data, computer system, or computer network.[11]

The limitations period under the CDAFA is "3 years from the later of the date of the wrongful act or the date of the discovery of damage. (Pen. Code, § 502(e)(5).)

"[S]ubdivision (c)(5) may properly be applied to an employee who uses his or her authorized access to a computer system to disrupt or deny computer services to another lawful user." (*Id*. at p. 1104; but see *Welenco, Inc. v. Corbell*, *supra*, 126 F.Supp.3d 1154, 1170 [withholding a password for two hours resembles "vexing," not "hacking" behavior].)

By its language, section 502(c)(5) should be available to challenge conduct not only of employees who have permitted access to a computer system but to non-employee consultants who seek to lock businesses out of their systems to gain leverage in contractual disputes over compensation or ownership of software and hardware. (See *Vaquero Energy, Inc. v. Herda*, *supra*, 2015 WL 5173535, *9–*10 [preliminary injunction issued based upon the CFAA and section 502(c)(5) of the CDAFA compelled consultant to turn over passwords he installed to prevent owner from accessing computers]; *NovelPoster v. Javitch Canfield*, *supra*, 140 F.Supp.3d at pp. 941, 944–951 [defendants changed passwords preventing plaintiff's access to business information and exposed themselves to claims of violating section 502 of the Penal Code and the CFAA]; cf. *Omega Morgan, Inc. v. Heely*, *supra*, 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].)

[10] See *People v. Lawton* (1996) 48 Cal.App.4th Supp. 11, 14–16 (hacker entered non-public areas of library computer system in violation of section 502(c)(7); court rejected the argument that the section applied only to unauthorized access of "hardware" as opposed to software).

[11] Sections 502(e)(10) to (14) describe violations related to government and public safety infrastructure computer related material.

2. Knowingly And Without Permission

There is a split of authority as to whether the phrase “knowingly and without permission” used in the CDAFA requires access in a manner that overcomes technical or code-based barriers. (S*ynopsys, Inc. v. ATopTech, Inc.* (N.D.Cal., Oct. 24, 2013, No. C 13-2965 SC) 2013 U.S. Dist. Lexis 153089, *36–*38 [collecting cases].)[12] Cases holding that overcoming technical or code-based barriers is required include: *NovelPoster v. Javitch Canfield Group*, *supra*, 140 F.Supp.3d at p. 950 (“Parties act ‘without permission’ when they ‘circumvent[] technical or code-based barriers in place to restrict or bar a user’s access.’”); *New Show Studios LLC v. Needle* (C.D.Cal., June 30, 2014, No. 14-CV01250-CAS(MRWx)) 2014 U.S. Dist. Lexis 90656, *21 (“[P]laintiffs have not alleged that defendants circumvented any technical or code-based barriers[.]”); *Perkins v. LinkedIn Corp.* (N.D.Cal, June 12, 2014, No. 13-CV-4303-LHK) 2014 U.S. Dist. Lexis 81042, *60–*61 (“[I]ndividuals may only be subjected to liability for acting ‘without permission’ under Section 502 if they access or use a computer, computer network, or website in a manner that overcomes technical or code-based barriers.”); *In re Google Android Consumer Privacy Litig.* (N.D.Cal., March 26, 2013, No. 11-MD-02264JSW) 2013 U.S. Dist. Lexis 42724, *34–*37 (circumvention of technical or code based barriers is required); *Facebook, Inc. v. Power Ventures, Inc.* (N.D.Cal. 2012) 844 F.Supp.2d 1025, 1036 (same); *In re iPhone Application Litig.* (N.D.Cal., Sept. 20, 2011, No. 11-CV-2250-LHK) 2011 U.S. Dist. Lexis 106865, *38 (same); *In re Facebook Privacy Litig.* (N.D.Cal. 2011) 791 F.Supp.2d 705, 716 (same).

Cases that hold that a breach of a technical or code-based barrier is not required include: *Facebook, Inc. v. Power Ventures, Inc.*, *supra*, 844 F.3d at pp. 1067–1068 (defendant knowingly accessed plaintiff’s website “without permission” in violation of CDAFA, where plaintiff issued defendant a written cease and desist letter rescinding permission); S*ynopsys, Inc. v. ATopTech, Inc.*, *supra*, 2013 U.S. Dist. Lexis 153089, at pp. *37–*38 (“The Court cannot find as a matter of law that Plaintiff does not state a claim under the CDAFA solely because Plaintiff relies on the alleged breach of a license agreement instead of a technical breach.”); *DocMagic, Inc. v. Ellie Mae, Inc.*, *supra*, 745 F.Supp.2d at p. 1151 (section 502 also prohibits knowing access “where the access is by means of a third-parties,” voluntarily-provided log-in credentials); *Multiven, Inc. v. Cisco Sys., Inc.* (N.D.Cal. 2010) 725 F.Supp.2d at p. 895 (“Since the necessary elements of Section 502 do not differ materially from the necessary elements of the CFAA for purposes of this action, the Court finds that there are no genuine issues of material fact remaining as to Cisco Section 502 claim.”); *Facebook, Inc. v. ConnectU LLC*, *supra*, 489 F.Supp.2d at pp. 1090–1091 (holding that a defendant’s access to a plaintiff’s website by using information voluntarily supplied by authorized users was

[12] “Although cases interpreting the scope of liability under the CFAA do not govern the Court’s analysis of the scope of liability under [s]ection 502, CFAA cases can be instructive.” (*Weingand v. Harland Fin. Solutions, Inc.* (N.D Cal., June 19, 2012, No. C-11-3109 EMC) 2012 U.S. Dist. Lexis 84844, *13, fn. 1, citing *Facebook, Inc. v. Power Ventures, Inc.* (N.D.Cal., July 20, 2010, No. C 08-05780 JW) 2010 U.S. Dist. Lexis 93517, *28.)

“without permission” and a violation of the CDAFA); see also *Weingand v. Harland Financial Solutions, Inc.* (N.D.Cal., June 19, 2012, No. C-11-3109) 2012 U.S. Dist. Lexis 84844, *13–*17 (discussing cases but refusing to apply at early stage of proceeding a requirement that a technical or code-based breach is required); *People v. Childs*, *supra*, 164 Cal.App.4th at p. 1104 (the fact that defendant was an employee who had passwords to the system did not preclude conviction).

3. Damages And Other Relief

Section 502(e)(1) of the Penal Code addresses damages and equitable relief, including injunctive relief, under the CDAFA:

> In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor, pursuant to the provisions of Section 1714.1 of the Civil Code.

“In order to state a claim under the CDAFA, [p]laintiffs must allege they suffered damage or loss by reason of a violation of [s]ection 502(c). (See also *In re Carrier IQ, Inc.*, (N.D.Cal. 2015) 78 F.Supp.3d 1051, 1098 [in bringing a claim under the California statute, plaintiffs are require to specifically allege which of nine enumerated offenses defendant violated].) As noted above, unlike the CFAA, the CDAFA does not include a monetary threshold for damages.” (*NovelPoster v. Javitch Canfield Group*, *supra*, 140 F.Supp.3d at p. 948; *DocMagic, Inc. v. Ellie Mae Inc.*, *supra*, 745 F.Supp.2d at p. 1150.) Some courts have concluded that any amount of loss or damage may be sufficient to establish statutory standing. (*In re Google Android Consumer Privacy Litig.*, *supra*, 2013 U.S. Dist. Lexis 42724, at p. *34, citing *Mintz v. Mark Bartelstein and Associates, Inc.*, *supra*, 906 F.Supp.2d 1017, and *Facebook, Inc. v. Power Ventures, Inc.* (N.D.Cal., July 20, 2010, No. C 08-05780 JW) 2010 U.S. Dist. Lexis 93517, *13–*14.) As with the CFAA, one must take care in pleading damages under the CDAFA.

Exemplary damages are expressly available under section 502(e)(4): “In any action brought pursuant to this subdivision for a willful violation of the provisions of subdivision (c), where it is proved by clear and convincing evidence that a defendant has been guilty of oppression, fraud, or malice as defined in subdivision (c) of Section

3294 of the Civil Code, the court may additionally award punitive or exemplary damages."

Additionally, section 502(e)(2) provides that "[i]n any action brought pursuant to this subdivision the court may award reasonable attorney's fees."

Stored Communications Act, 18 U.S.C. § 2701 et seq.

Congress enacted the Stored Communications Act ("SCA") in 1986 as Section II of the Electronic Communications Protection Act. (18 U.S.C. § 2701 et seq.)

> The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, *cf. Prosser and Keeton on the Law of Torts* § 13, at 78 (W. Page Keeton ed., 5th ed. 1984), the Act protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility

(*Theofel v. Farey-Jones* (9th Cir. 2004) 359 F.3d 1066, 1072.) In applying the CFAA and the SCA, federal courts have noted that their "general purpose . . . was to create a cause of action against 'computer hackers (e.g. electronic trespassers).'" (*Cousineau v. Microsoft Corporation* (W.D.Wash. 2014) 6 F.Supp.3d 1167, 1171.)

1. Summary Of Prohibitions

"[T]he SCA creates criminal and civil liability for certain unauthorized access to stored communications and records." (*In re iPhone Application Litig.*, *supra*, 844 F.Supp.2d 1040, 1056–1057.) Among other things, the act creates a private right of action against anyone who: "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility, and thereby obtains, alters, or prevents authorized access to wire or electronic communication while it is in electronic storage in such system. . . ." (18 U.S.C. §§ 2701(a)(1)–(2), 2707(a); *Konop v. Hawaiian Airlines, Inc.* (9th Cir. 2002) 302 F.3d 868, 879.) "Electronic storage" means either "temporary, intermediate storage . . . incidental to . . . electronic transmission," or "storage . . . for purposes of backup protection." (18 U.S.C. § 2510(17).)[13]

[13] The SCA adopts the definitions contained in 18 U.S.C. § 2510. (18 U.S.C. § 2711.) There is some disparity within the Ninth Circuit over the application of the definition of "electronic storage" contained in 18 U.S.C. § 2510(17). The district court in *In re iPhone Application Litig.*, *supra*, 844 F.Supp.2d at pp. 1058–1059, required temporary electronic storage and rejected storage on a hard drive. In contrast, the Ninth Circuit in *Theofel v. Farey-Jones*, *supra*, 359 F.3d at pp.1075–1076, rejected an argument that messages remaining on an ISP's server after delivery no longer fall within the Act's coverage: "But even if such messages are not within the purview of subsection (A), they do fit comfortably within subsection (B). There is no dispute that messages remaining on NetGate's server after delivery are stored 'by electronic communication service' within the meaning of 18 U.S.C. § 2510(17)(B)." (*Id.* at p. 1075; cf. *Hilderman v. Enea TekSci, Inc.* (S.D.Cal. 2008) 551 F.Supp.2d 1183, 1205 ["E-mails

As noted above, under section 2701(a), in order to state a claim under the SCA a plaintiff must allege that the defendant accessed without, or in excess of, authorization a "facility through which an electronic communication services is provided." An "electronic communication service" is "any service which provides to users thereof the ability to send and receive wire or electronic communications." (18 U.S.C. § 2510(15).) There is a split of authority on whether an individual's computer, laptop or mobile device fits the statutory definition of a "facility through which an electronic communication service is provided." *In re iPhone Application Litig.*, *supra*, 844 F.Supp.2d at pp. 1057–1058, in collecting the cases, answered the question in the negative while acknowledging that "the computer systems of an email provider, a bulletin board system, or an ISP are uncontroversial examples of facilities that provide electronic communications services to multiple users." (See also *Vaquero Energy, Inc. v. Herda*, *supra*, 2015 WL 5173535, *10–*11 [business computer was not a "facility" for purposes of the SCA]; *Roadlink Workforce Solutions, LLC v. Malpass* (W.D.Wash., Sept. 18, 2013, No. 3:13-cv-05459-RBL) 2013 U.S. Dist. Lexis 133786, *9 [individual's computer was not a "facility through which an electronic communication service is provided"].)

2. Without, Or Exceeding, Authorization

Within the Ninth Circuit, courts have interpreted the meaning of "without authorization" and "exceeds authorized access" in the same way that it has interpreted use of those terms under the CFAA. (*Theofel v. Farey-Jones*, *supra*, 359 F.3d 1066, 1078; see also *Craigslist Inc.* (N.D.Cal. 2013) 964 F.Supp.2d 1178, 1183 [language between CFAA and SCA is "almost identical"]; *Capitol Records, Inc. v. Weed* (D.Ariz., April 21, 2008, No. 06-CV-1124-PHX(JATx)) 2008 U.S. Dist. Lexis 35298, *14–*15 [jointly analyzing "without authorization" under the SCA and the CFAA].) Courts have interpreted the phrase "exceeding authorized access" as meaning accessing "information that the party has no authority to see, or information that is stored in a place where the party has no authority to be." (*Cousineau v. Microsoft Corporation*, *supra*, 6 F.Supp.3d at p. 1171.)

3. Damages And Other Relief

While there are similarities between the CFAA and the SCA, there are some significance differences. There is no minimum damages requirement under the SCA. The SCA does provide for a statutory minimum award of damages of at least $1,000, presumably per violation. (18 U.S.C. § 2707(c); see *Konop v. Hawaiian Airlines, Inc. (In re Hawaiian Airlines, Inc.)* (Bankr. D.Hawaii 2006) 355 B.R. 225, 229–233 ["statutory damages may be multiplied by the number of violations" and need not be based upon a plaintiff suffering "at least some actual damages or have proved some profits gained by the alleged violator"].) The SCA further empowers the court to assess punitive damages for willful or intentional violations. (18 U.S.C. § 2707(c).) The SCA

stored on the laptop computer are not in "temporary, intermediate storage" . . . [and] the e-mails on the laptop are not stored "by an electronic communication service for purposes of backup protection" as required by subsection (B)."].)

explicitly provides for a disgorgement of profits, while such disgorgement is only implicit in the CFAA's provision for "equitable remedies." The SCA allows users to authorize third parties to access those wire and electronic communications. (*Konop v. Hawaiian Airlines, Inc.*, *supra*, 302 F.3d at p. 880.) The SCA, unlike the CFAA provides for recovery of reasonable attorney's fee. (18 U.S.C § 2707(b)(3).) Like the CFAA, the SCA provides for "such preliminary and other equitable or declaratory relief as may be appropriate." (18 U.S.C § 2707(b)(1).) Also, similar to the CFAA, the limitations period under the SCA is "2 years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation." (18 U.S.C. § 2707(f).)[14]

[14] In addition to these statutory remedies, businesses also may have claims for various common law violations, including such claims as, breach of contract, misappropriation of trade secrets, intentional interference with contractual relations, interference with prospective economic relations, trespass to chattels, trespass to real property, unfair competition (both common law and statutory under California Business. and Professions Code sections 17200 et seq.) and conversion. There may also exist federal statutory claims for copyright and trademark infringement and unfair competition.

An Ounce Of Prevention

1. Conduct an annual security assessment using either a third party consultant or in house expertise and establish and implement a security plan and policy.

2. Audit third party vendors where feasible, particularly those that provide in-house services such as filing, copying, mailing and production services.

3. Periodically change employee passwords and assure that the passwords are complex.

4. For remote access to computer systems, have two factor or two step authentication. Two factor authentication is a process involving two subsequent but dependent stages to check the identity of someone trying to access services on your network and systems. An example is use of (a) an ATM card (something you have) and (b) a PIN (something you know) to access one's bank account at an automated teller machine. Another example is requiring input of a user ID and password and then a single use code or PIN sent to another device such as the user's mobile phone or tablet.

5. Use encryption for data at rest and data in transit. Encryption protects your data and allows client server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. Examples of encryption methods include: encrypting your computers' hard drives, implementing "Transport Layer Security ("TLS") for email delivery, and use "Secure Sockets Layer" ("SSL") VPN connections when connecting remotely to your network.

6. Ensure that your software is up to date.

7. Have a clearly defined policy in an employee manual regarding confidentiality and use of company information both electronic and otherwise.

8. Have employees execute confidentiality agreements at the time of hire.

9. Immediately disable logins and electronic password of separated employees.

10. Clearly identify trade secret information and limit access to it.

11. Formalize agreements in writing with outside technical consultants making it clear that: (a) the business owns any software developed, including written materials, (b) the consultant's access to electronic systems may be terminated at any time, and (c) the consultant shall not lock the business out of access to its computer system.