Strategies for Businesses Protecting Electronic Data within California: Part Two

06.17.2015

**Updated June 2019.*

PART TWO: The California Computer Data Access and Fraud Act (Cal. Pen. Code, § 502)

In Part One of this e-alert series, we discussed the federal Computer Fraud And Abuse Act ("CFAA"). In Part Two, we present a discussion of the California state law analogue to the federal act, namely the California Computer Data Access And Fraud Act, Cal. Pen. Code, § 502 ("CDAFA"). Advantages of the state act over the federal act include provision for the recovery of attorney's fees and no requirement on minimal loss.

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]; see generally 1 Serwin, *Information Security and Privacy - A Guide To Federal And State Law And Compliance, supra*, § 6.13 et seq., pp. 244 et seq.) 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.)

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, subd. (c)]. (Cal. Pen. Code, § 502, subd. (e).) Subdivision 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;[1]
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;[2]
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;[3] (But see *Welenco, Inc. v. Corbell, supra*, 126 F.Supp.3d 1154, 1170 [withholding a password for two hours resembles vexing, not hacking behavior].)
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;[4]
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.[5]

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, subd. (e)(5).)

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. (*Synopsys, Inc. v. ATopTech, Inc.* (N.D.Cal. Oct. 24, 2013, No. C 13-2965 SC) 2013 U.S.Dist. Lexis 153089, at pp. *36–*38 [collecting cases].)
[6] 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, at p. *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, at pp. *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 Litigation, supra*, 2013 U.S.Dist. Lexis 42724, at pp. *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, at p. *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); *Synopsys, 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. 1090–91 (holding that a defendant's access to a plaintiff's website by using information voluntarily supplied by authorized users was 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, at pp. *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*, 220 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

Subdivision 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, Plaintiffs must allege they suffered damage or loss by reason of a violation of Section 502(c). (*In re Google Android Privacy Litigation, supra*, 2013 U.S.Dist. Lexis 42724, at

p. *34; 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 Litigation, 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, at pp. *13–*14.) As with the CFAA, one must take care in pleading damages under the CDAFA.

Exemplary damages are expressly available under subdivision 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, subdivision 502(e)(2) provides that [i]n any action brought pursuant to this subdivision the court may award reasonable attorney's fees.

Read Part One here.

Read Part Three here.

[1] 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).

[2] *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.

[3] Penal Code subdivision 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 subdivision 502(c)(5) of the Penal Code. On appeal, the defendant argued that the court should interpret subdivision 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 subdivision 502(c)(5). After extensive discussion, the Court of Appeal rejected the defendant's argument, holding that the statute was unambiguous and clear: [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.)

By its language, subdivision 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 U.S.Dist. Lexis 115717, at pp. *14–*18 and *23-*26 [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, 944–51 [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].)

[4] 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 subdivision 502(c)(7); court rejected the argument that the section applied only to unauthorized access of hardware as opposed to software).

[5] Subdivisions 502(e)(10) to (14) describe violations related to government and public safety infrastructure computer related material. See *Ticketmaster LLC v. Prestige Entertainment West, Inc., supra*, 2019 U.S.Dist. Lexis at pp. *57-*61 for application of the CFAA to defendants' use of automated bots to obtain large numbers of tickets to popular events; compare *Oracle USA, Inc. v. Rimini St. Inc.* (2018) 879 F.3d 948,962. Reversing jury award on CDAFA claim because taking data using a *method* prohibited by the applicable terms of use, when the taking itself generally is permitted, does not violate the CDAFA. (Original italics.) In *Oracle USA, Inc.* the defendants had authority to access the relevant database but used (contrary to the plaintiff's desire and later terms of use) automated downloading tools as a means to obtain a large amount of data.

[6] 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, at p. *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, at p. *28.)