E-Alerts

Strategies For Businesses Protecting Electronic Data Within California: Part One

By: Stephen P. Wiman
06/10/15

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.

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") applies to a "protected computer" which the statute defines as one "which is used in or affecting interstate or foreign commerce or communication." The CFAA prohibits, among other things:

- 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;
- intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage; or
- intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss.

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."

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]." Such person may obtain compensatory damages and equitable (including injunctive) relief. For a civil plaintiff to recover, the CFAA requires that the plaintiff allege and prove that the offensive conduct caused any one of the following five circumstances:

1. loss to one or more persons during any one-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 one 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

A civil plaintiff 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. Alternatively, a plaintiff may seek to 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) furthered the intended fraud and obtained something of value, causing (5) a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

The CFAA is designed to target hackers who access computers to steal information or to disrupt or destroy computer functionality, as well as criminals who have the capacity to access and control high technology processes vital to our everyday lives. The CFAA is not meant to serve as a supplement or replacement for trade secret misappropriation claims.

The limitations period under the CFAA is two years from the date of the action complained of or the date of discovery of the damage.

2. "Without Authorization"

The CFAA requires that a defendant access a protected computer "without authorization." According to the federal court of appeals,

[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 federal court of appeals 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.

It appears that most courts do not require circumvention of "technological access barriers" (e.g., unauthorized use of passwords) for use to be considered unauthorized. Whether a defendant has exceeded authorization is a factual issue. 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 clarify that any authority to access computer systems is terminated when an employee departs a job, whether or not log-in access is disabled. Of course, an employer should disable log-in access upon termination of an employee or consultant.
3. Exceeding Authorized Access

While a defendant may not have accessed a computer "without authorization," he may have exceeded authorized access nonetheless. Exceeding authorized access, as noted above, can be grounds 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.

According to the federal court of appeals in United States v. Nosal (9th Cir. 2012) 676 F.3d 854, 864, "exceeding authorized access" implicates 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. 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 would be the subject of a claim for misappropriation of trade secret. 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 – colloquially known as "hacking." 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.

4. Damages And Other Relief

As noted, the CFAA provides a private remedy to a person who "suffers damage or loss" resulting from certain violations of the CFAA. For most private litigation, the CFAA is limited to "economic damages."

The CFAA defines "damage" to mean "any impairment to the integrity or availability of data, program, a system, or information." Under the act, 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. The definition also covers any lost revenue, cost incurred, or other consequential damages because of interruption of service. Courts have held that it is not necessary for data to be physically changed or erased to constitute damage to that data. It is sufficient to show that data integrity has been impaired, 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."

Cognizable costs include the costs associated with assessing a hacked system for damages and upgrading a system's defenses to prevent future unauthorized access. Moreover, in situations in which 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.

Loss of business and business goodwill are included within "economic damages." Such damages include scenarios in which the value of an individual or firm's money or property is impaired, or money must be spent to restore or maintain some aspect of a business affected by a violation.

Injunctive relief under the CFAA can include barring a defendant's access even to publicly available websites for past egregious and numerous instances of violations.

The CFAA does not expressly provide for attorney's fees. However, as will be discussed in the future e-alerts, 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.
The CFAA is a powerful statute. It provides a basis for federal court jurisdiction which is advantageous to a plaintiff because resolution is likely to be speedier than in state court. The federal judge's expertise on the technical issues is likely to be greater as well.

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 is similar to the federal Computer Fraud And Abuse Act, 18 U.S.C. § 1030 et seq. ("CFAA"). Indeed, courts have identified 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. Furthermore, it contains no minimal loss requirement in order to support a private right of action.

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 Section 502(c) of the California Penal Code which, inter alia, lists the following violations:

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 control or obtain money, property, or data;
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;
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;
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;
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 damaging or causing damage to a computer, computer data, computer system, or computer network.

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).)"

2. Knowingly And Without Permission

There is a split of legal 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. That split should not be a deterrence to asserting a violation of the act even where there was no breach of technical or code-based barriers since some courts have allowed claims in that circumstance.

3. Damages And Other Relief

Section 502 of the Penal Code addresses damages and equitable relief, including injunctive, 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). As noted above, unlike the CFAA, the CDAFA does not require that the plaintiff actually incur a minimum dollar amount of damages. Some courts have concluded that any amount of loss or damage may be sufficient to establish statutory standing.

Exemplary (punitive) 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."

Section 502 of the California Penal Code is a useful corollary to the CFAA. Its terms are somewhat broader. There is no requirement that a plaintiff establish a minimum amount of damages. The statute provides for recovery of attorney's fees and exemplary damages, neither of which are available under the CFAA.
In our next and final e-alert, we will discuss the federal Stored Communications Act, 18 U.S.C. 2701 et seq. That statute provides an alternative basis for federal court jurisdiction as well as an alternative basis for an award of attorney's fees. We will also provide a checklist of best practices for businesses to preserve the integrity of their electronic data.
Strategies For Businesses Protecting Electronic Data Within California: Part Three

By: Stephen P. Wiman
06/24/15


In Parts One and Two of this e-alert series, we discussed the federal Computer Fraud And Abuse Act ("CFAA") and its California corollary the California Computer Data Access And Fraud Act (CDAFA). In Part Three, we provide a presentation of the federal Stored Communications Act, 18 U.S.C. 2701 et seq. ("SCA"). The act is similar to the CFAA; however, unlike the CFAA, the SCA provides for the recovery of attorney's fees and does not contain a minimal loss requirement. We conclude this e-alert with suggested best practices for preserving data security.

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.

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).

1. Summary of Prohibitions

The SCA creates criminal and civil liability for certain unauthorized access to stored communications and records. Among other things, the act creates a private right of action against anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided; or 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. . . ." "Electronic storage" means either "temporary, intermediate storage incidental to electronic transmission, or storage for purposes of backup protection.

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. 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."
2. Without, Or Exceeding, Authorization

Federal courts have interpreted the meaning of "without authorization" and "exceeds authorized access" in the same way that they have interpreted use of those terms under the CFAA.

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. In fact, the SCA provides for a statutory damages award of at least $1,000, presumably per violation. The SCA further empowers the court to assess punitive damages for willful or intentional violations. The SCA explicitly provides for a disgorgement of profits, while such disgorgement is only implicit in the CFAA's provision for "equitable remedies." Unlike the CFAA, the SCA provides for recovery of reasonable attorney's fees. Like the CFAA, the SCA provides for "such preliminary and other equitable or declaratory relief as may be appropriate." 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."

The CFAA, California Penal Code Section 502 and the SCA provide a helpful triumvirate for businesses seeking to remedy an unlawful data breach. The federal acts provide a basis for federal court jurisdiction which is likely to result in speedier relief. Both the California statute and the SCA provide a basis for claiming attorney's fees and the California statute allows for an award of a penalty by way of exemplary damages.

While businesses can use these statutes as tools for remediing data breaches, the best case scenario is exercising data security best practices to avoid reliance on the statute in the first place. Below is a set of best practices we recommend.

Best Practices: 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 an ATM card (something you have) and 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. Encryption methods include encrypting your computers' hard drives; implementing "Transport Layer Security ("TLS") for email delivery; and using "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 passwords 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 the business owns any software developed, including written materials; the consultant's access to electronic
systems may be terminated at any time; and the consultant shall not lock the business out of access to its computer system.

Should you experience any data breach, the attorneys at Nossaman stand ready to assist you in remedying the consequences of that breach.