Law360

What Constitutes Reasonable Security Per Calif. Privacy Law?

By **Amanda Lawrence, Michael Rome and James Chou** (June 15, 2020)

Amanda Lawrence

Michael Rome

James Chou

California Consumer Privacy Act compliance has been focused on developing the policies, procedures and infrastructure to support new privacy rights for California residents, which include, among other things, the right to know what personal information companies have on them, the right to delete and the right to opt out of the sale of that information to third parties.

While much ink has been spilled on how to come into compliance with these new privacy rights, companies subject to the CCPA also should focus their efforts on ensuring that they have an information security program that reasonably safeguards the personal information collected, stored and processed by their companies.

Designing reasonable policies and procedures is a task complicated by the fact that nowhere does the CCPA define "reasonable." It is also a task that may become more urgent, as plaintiffs already have taken advantage of the CCPA's private right of action and filed putative class actions asserting that the defendants violated the law's data breach provision.

California Data Breach Law and the CCPA's Private Right of Action

California, like all states, maintains data breach laws covering the loss of specific personal information such as Social Security numbers, driver's license information, credit card numbers with an associated security code and other sensitive information.[1] California's data breach law generally requires companies to notify California residents (and the California attorney general in some cases) in the event of a breach.[2]

Individuals suing companies for data breaches used to bring their claims under a series of statutes and common law theories, none of which squarely addressed data breaches. The CCPA changed that.

Under the law, which went into effect on Jan. 1, California became the first state to provide a statutory private right of action — along with statutory damages—for consumers whose personal information was compromised because of a business's failure to implement reasonable security procedures and practices.[3]

Specifically, the CCPA provides a private right of action for "[a]ny consumer whose nonencrypted and nonredacted personal information ... is subject to an unauthorized access and exfiltration, theft, or disclosure" because a business failed to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."[4]

In addition to injunctive, declaratory or other nonmonetary relief, each consumer affected by such a data breach may also recover the greater of actual or statutory damages between $100 to $750, depending on:

the nature and seriousness of the misconduct, the number of violations, the persistence of

the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.[5]

While the CCPA uses its own expansive definition of "personal information" for most of its regulatory compliance provisions, the private right of action borrows the more narrow definition of that term used in California's separate data breach law, which was recently expanded to include biometric data, among other things.[6] Biometric data, in this instance, may include such things as face- or finger-prints.[7]

The CCPA also builds one small, but important, hurdle to the private right of action: Consumers must first provide a written notice to the company that suffered the data breach identifying the specific provisions of the CCPA that have been allegedly violated.[8]

The business then has 30 business days to cure the defect (if possible) and provide an express statement to the consumer that the defect has been cured and that "no further violations shall occur."[9]

However, if a business is found to have later breached the expressed statement, then the consumer may pursue the business for each violation of the expressed statements and "any other violation ... that postdates the written statement."[10]

Although the 30-day opportunity to cure may be helpful to a business that maintains a comprehensive information security and incident-response program, it is not lot of time to fully understand the cause and scope of the breach.

In complex breaches, it is unlikely that a business will obtain all the necessary forensic information from an investigation to even understand whether there were any failures or gaps in its information security controls (for example, a compromise involving a zero-day exploit may have been impossible to defend against, regardless of the adequacy of existing controls).

For businesses that lack an information security program or have weak incident-response plans, it is likely to take much longer. Further, it is not clear under the law what it would mean for a company that suffered a significant breach and loss of personal information to a third-party to "cure" that breach. For these reasons, a 30-day cure period may not be as helpful as it sounds.

How Companies Can Assess Whether They Have Reasonable Security Measures

The CCPA does not set forth specific standards for reasonable security procedures and practices; California data breach law merely imposes a duty on any business that "owns, licenses, or maintains personal information about a California resident" to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information" and to "protect the personal information from unauthorized access, destruction, use, modification, or disclosure," consistent with the CCPA.[11]

Consequently, what is reasonable will likely be determined by California courts and supplemental guidance.

Until then, there are a number of places that companies may look for guidance. The California attorney general issued Data Breach Report 2012-2015,[12] which recommends that businesses implement the top 20 security controls published by the Center for Internet Security, [13] which includes such practices as asset inventory, malware defense, wireless

access and data protection.[14]

Additionally, businesses can reference the National Institute of Standards and Technology's cybersecurity framework and corresponding security controls set forth in NIST Special Publication 800-53.[15]

The Financial Services Sector Coordinating Council's cybersecurity profile provides another framework that is tailored to financial institutions,[16] and many businesses that process credit or other payment cards must comply with the Payment Card Industry Data Security Standard and may look to the PCI Standards Council for data protection guidance and attestation standards.

Federal regulatory guidelines, such as the Interagency Guidelines Establishing Information Security Standards[17] pursuant to the Gramm-Leach-Bliley Act and the Federal Financial Institutions Examination Council's information technology handbooks, also provide additional guidance to businesses, such as consumer notification and incident-response requirements for data breaches.[18] The FFIEC has recently published guidance related to cloud security.[19]

Business also can examine the Security Standards for the Protection of Electronic Protected Health Information established under the Health Insurance Portability and Accountability Act of 1996 for data protection rules for health information.[20]

Finally, states such as Massachusetts and New York maintain cybersecurity regulations,[21] which are modeled after industry frameworks and provide baseline standards for businesses maintaining personal information.

Manage Insider (as Well as External and Third-Party) Risk

Most businesses have come to grips with the fact that they operate under constant threat of cyberattacks and need third-party risk management, but the number of insider-related breaches rises every year. The Verizon Communications Inc. 2019 data breach investigations report notes that 34% of all breaches in 2018 were caused by insiders.[22]

Therefore, any credible information security program must consider the risks posed by insiders, whether through negligent or malicious activity, and implement appropriate controls to mitigate those risks. The acceleration of virtualization and movement to cloud solutions, as a consequence of the pandemic, has only exacerbated and complicated insider risk.

Unauthorized access is not specifically defined in the CCPA, but it is generally understood to include unauthorized actions of nefarious or negligent insiders, employees, contractors or other personnel who have authorized access to personal information. An employee who steals personal information collected and stored by the company may qualify as a reportable incident under data breach laws.

This type of incident arguably could give rise to a claim under the CCPA's private right of action if such insider risk was known (or should have been known) by the business and the business did not mitigate it.

Industry controls for insider activity are not necessarily on a par with controls for external threats, but most companies have started addressing insider risk through data-loss prevention programs, including automated email screening and restrictions on the use of

removable storage media.

Given the statutory damage provisions of the CCPA, there is a risk of significant and potentially crippling liability from a data breach if it resulted from inadequate security procedures.[23]

Don't Forget About Incident Management

Incident management is key to controlling costs. A study by International Business Machines Corp. and Ponemon Institute found that the average cost of a data breach in 2019 for a U.S. company was approximately $8.2 million, or $242 per record, up from $3.5 million in 2006, with smaller companies facing higher average costs.[24]

However, the study also found that data breach costs are reduced by an average of $1.2 million per incident if an incident-response plan was properly exercised (live or table-top tested), staffed and maintained.

Incident response, which has been in the crosshairs of federal and state regulators, as well as cyber insurers in the wake of COVID-19, is an inherent requirement for information security programs and must be implemented to avoid unnecessary costs, regulatory scrutiny and civil liability.

For example, as part of new proposed regulations, the Federal Trade Commission will require financial institutions to implement a written incident-response plan with specific components, such as "[d]documentation[ng] and reporting ... security events and related incident response activities."[25]

Even with good information security practices, a business may be exposed to liability under the CCPA if it maintains poor incident-response plans or procedures. Poor incident management also may lead to escalation failures and improper or inadequate investigation, which could adversely affect a business's consumer and regulatory obligations under state data breach laws.

Conclusion

One study predicts that a business's chance of experiencing a data breach in the next two years is about 30%, and, should it happen, the CCPA may potentially impose costs far greater than the already expected costs experienced by affected businesses today. With the CCPA now in full effect, businesses must consider information security as part of its overall CCPA compliance efforts.

Amanda Lawrence is a partner, Michael Rome is counsel and James Chou is an associate at Buckley LLP.

[1] Cal. Civ. Code § 1798.81.5, .82.

[2] Cal. Civ. Code § 1798.82.

[3] Cal. Civ. Code § 1798.150.

[4] Cal. Civ. Code § 1798.150(a)(1).

[5] Cal. Civ. Code § 1798.150(a)(1), (2).

[6] Cal. Civ. Code § 1798.81.5(d)(1)(vi).

[7] Cal. Civ. Code § 1798.81.5(d)(1)(vi).

[8] Cal. Civ. Code § 1798.150(b).

[9] Cal. Civ. Code § 1798.150(b).

[10] Cal. Civ. Code § 1798.150(b).

[11] Cal. Civ. Code § 1798.81.5(b).

[12] Kamala D. Harris, California Data Breach Report (Feb. 2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

[13] See id. at Appx. A, B.

[14] Id.

[15] The NIST Cybersecurity Framework is accessible here: https://www.nist.gov/cyberframework.

[16] The FSSCC's Cybersecurity Profile is accessible here: https://fsscc.org/Financial-Sector-Cybersecurity-Profile.

[17] 12 C.F.R. Pt. 30, Appx. B.

[18] The FFIEC handbooks are accessible here: https://ithandbook.ffiec.gov/.

[19] Security in a Cloud Computing Environment, FFIEC (Apr. 30, 2020).

[20] 5 C.F.R. Pt. 160; 5 C.F.R. Pt. 164.

[21] 201 Mass. Code Regs. § 17.00 et seq.; N.Y. Comp. Codes R. & Regs. tit. 23, § 500.01 et seq.

[22] See 2019 Verizon Data Breach Investigation Report (2019), https://enterprise.verizon.com/resources/reports/dbir/.

[23] See IBM & Ponemon Institute, Cost of a Data Breach (2019), https://www.ibm.com/security/data-breach (finding the CCPA's private right of action could substantially increase the cost per record in the event of a data breach).

[24] IBM & Ponemon Institute, Cost of a Data Breach (2019), https://www.ibm.com/security/data-breach.

[25] 84 Fed. Reg. 13158, 13160-61, 13176 ("[T]he Commission proposes an amendment to the Rule to require covered financial institutions to develop an incident response plan as part of their information security program.").