Pending Changes to California's Data Breach Law: New Burdens for Retailers?

September 2007
by Christine E. Lyon, William L. Stern

Related Practices:
- Privacy and Data Security

The California Legislature recently passed two bills that would substantially change California's data breach notification law, and impose new burdens on retailers. These bills, Assembly Bill 779 ("AB 779") and Assembly Bill 1298 ("AB 1298"), have been sent to Governor Schwarzenegger for his signature.[1] If enacted, these bills will:

(1) regulate the storage, retention, transmission, and security measures for credit card, debit card, and other payment-related data;

(2) require more detailed notifications in the event of certain breaches of payment-related data;

(3) shift the costs of breach notification to retailers and other merchants, if they fail to comply with these new limitations on handling of payment-related data; and

(4) expand the data breach notification law to cover medical information and health insurance information.

As our Firm has reported, similar legislation has already been enacted in Minnesota, and has been under consideration in Connecticut, Illinois, Massachusetts, and Texas.[2] If enacted, AB 779 and AB 1298 would take effect on July 1, 2008.

New Limitations On Handling Of Payment-Related Data

AB 779 would impose new limitations on any person, business, or agency[3] that (a) sells goods or services to any resident of California; (b) accepts as payment a credit card, debit card, or other payment device; and (c) is not already subject to regulatory oversight under the Gramm-Leach-Bliley Act's rules about disclosure of nonpublic personal information.[4] For purposes of this article, we will refer to such a person, business, or agency as a "Merchant." Under AB 779, Merchants would be prohibited from:

1. Storing Payment-Related Data,[5] except when: (1) the Merchant has an appropriate payment data retention and disposal policy; and (2) the Payment-Related Data is stored only for a time period and in a manner that is permitted by that policy. The policy must limit the amount of Payment-Related Data that is stored, and the length of time that this data is retained, to the amount and time that is required for business, legal, or regulatory purposes.[6] AB 779 also indicates that the policy must identify and document the business, legal, and/or regulatory purposes requiring the storage of Payment-Related Data.
2. Storing sensitive authentication data after authorization, even if that data is encrypted.[7]
3. Storing any Payment-Related Data that is not needed for business purposes.[8]
4. Storing payment verification code, payment verification value, or PIN verification value.[9]
5. Retaining the primary account number, unless retained in a manner consistent with AB 779 and in a form that is "unreadable and unusable by unauthorized persons anywhere it is stored."[10]

6. Sending Payment-Related Data over open, public networks unless the data is encrypted using "strong cryptography and security protocols, or otherwise rendered indecipherable."[11]
7. Failing to limit access to Payment-Related Data to only those individuals whose jobs require that access.[12]

These new limitations on the handling of Payment-Related Data create affirmative obligations for all Merchants. Merchants that fail to comply with these new rules may be liable for the costs of providing breach notification, as discussed in the following section.

Merchant Liability for Breach Notification Costs

California law requires the owner or licensee of computerized data (the "Data Owner") to notify California residents whose unencrypted "personal information" was (or is reasonably believed to have been) acquired by an unauthorized person.[13] In comparison, a person or business that maintains computerized "personal information" it does not own (a "Service Provider") is only required to notify the Data Owner of the actual or suspected breach.[14] The practical result is that the Data Owner bears the cost of providing notice, even if the breach occurs while the data is in the Service Provider's custody.

AB 779 includes a cost-shifting provision, which allows the Data Owner to recover breach notification costs from a Merchant in certain cases. Specifically, AB 779 provides that the Merchant is liable to the Data Owner for reimbursement of all reasonable and actual costs of notifying the affected California residents of the breach as required by California law; and for the reasonable and actual cost of card replacement as a result of the breach.[15] However, the Merchant may be excused from these reimbursement obligations, in whole or in part, if it can demonstrate compliance with all of the limitations on handling of Payment-Related Data discussed in Section I above.[16]

The cost-shifting provision of AB 779 is not a model of clarity. As explained above, this provision would require the Merchant to reimburse the breach notification costs of a data "owner or licensee" that is required to give notice under California's existing data breach notification law. However, neither this existing law nor these proposed amendments explain how to determine which entity is the "owner or licensee" that is required to give notice under the California breach notification law, and thus would be entitled to reimbursement under AB 779. They also fail to address whether multiple entities could be "owners" or "licensees" of the same data for purposes of California's breach notification law. For instance, even if a Merchant determines that it "owns" the affected data, and directly notifies consumers about a breach affecting their credit card information, the credit card issuer still can argue that it also "owns" the data, since it relates to the issuer's cardholders, and that the issuer is entitled to recover its reasonable and actual costs for notifying its cardholders if the issuer concludes that it should provide notice or that the Merchant has failed to properly do so.

Additionally, it is unclear whether the Merchant is required to reimburse the issuer of credit or debit cards for the cost of card replacement, if the Merchant has notified the cardholders as the "owner or licensee" of the data affected by the breach. To paraphrase AB 779, the cost-shifting provision states that the Merchant is liable to the owner or licensee for breach notification costs and for the cost of card replacement as a result of the breach of security of the system. This may leave room to debate whether the second type of liability runs only to the "owner or licensee" that has provided notice, or whether the second type of liability could extend to reimbursing another entity that incurs card replacement costs due to the breach, whether or not the other entity also could be viewed as an owner or licensee of the data for purposes of providing notice. What is clear is that the legislation contemplates that a Merchant that suffers a breach should reimburse card reissuance costs resulting from that breach, and that card reissuance costs are not likely to be experienced by any entity other than a card issuer; however, getting to this result given the unclear language of the statute may not be as easy as the authors of the legislation might have anticipated.

AB 779 effectively creates a "strict liability" standard for Merchant liability. The cost-shifting provision does not require any showing that the Merchant was to blame for the breach, or that the Merchant's failure to comply with AB 779 may have contributed to the breach. However, the Merchant may be excused from reimbursement obligations under this section if the Merchant can demonstrate "compliance with all provisions of Section 1724.4 at the time of the breach."[17]

Enhanced Breach Notification Requirements

As discussed above, California law already requires a Service Provider—i.e., a person or business

maintaining computerized data that includes Personal Information which it does not own—to notify the Data Owner of a security breach. AB 779 would increase the level of detail required in such a notice, if the Service Provider also happens to be a Merchant. It also would require the Data Owner to pass along this enhanced level of detail to the affected California residents, if the Data Owner happens to be the issuer of the credit or debit card or the payment device, or maintains the account from which the payment device orders payment.

Additional Notice Requirements for Merchants
If a Merchant is required to notify a Data Owner of a security breach, the Merchant must include the following information, to the extent such information is available at the time the notice is provided: [18]

1. The date of the notice;
2. The name of the agency, person, or business that maintained the computerized data at the time of the breach;
3. The date, or estimated date, when the breach occurred, if the date or estimated date is possible to determine;
4. A description of the categories of personal information that were, or are reasonably believed to have been, acquired by the unauthorized person;
5. A toll-free number for the agency, person, or business whose system was subject to that breach (or, if the primary method used to communicate with the affected individuals whose information is the subject of the breach is by electronic means, an email address that can be used to contact that agency, person, or business so that the individuals may learn what types of personal information were subject to the breach); however, if the agency, person, or business does not have a toll-free number, it can provide a local phone number to the owner or licensee of the information to contact the agency, person, or business; and
6. Toll-free telephone numbers and addresses for the major credit reporting agencies.

Consistent with existing law, this notification can be delayed "if a law enforcement agency determines that notification will impede a criminal investigation."[19]

Additional Notice Obligations for Issuers of Payment Device or Account
In turn, if the Data Owner is the issuer of the credit or debit card or the payment device, or maintains the account from which the payment device orders payment, the Data Owner must include these same categories of information in the notice provided to the affected California residents under California Civil Code Section 1798.82(a).[20] However, an email address may be provided in lieu of a toll-free or local telephone number to those individuals with whom the primary method of communication is by electronic means.[21]

Substitute Notice to Office of Privacy Protection
California's data breach notification law allows a Data Owner to use "substitute notice," rather than individually notifying each affected California resident, if the Data Owner demonstrates (a) that the cost of providing notice would exceed $250,000, (b) that the number of affected California residents exceeds 500,000, or (c) that the Data Owner does not have sufficient contact information.[22] "Substitute notice" currently requires email notice (when the Data Owner has an email address for the affected California residents), conspicuous posting of the notice on the Data Owner's website, and notification to major statewide media.[23] Under AB 779, substitute notice would also require notification to the California Office of Privacy Protection.[24]

Expansion of Data Breach Law to Medical and Health Insurance Information

The California data breach notification law currently defines "personal information" as an individual's first name or first initial and last name in combination with any of the following data elements, when either the name or the data element is not encrypted:

- Social Security number;
- Driver's license number or California Identification Card number; or
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to the individual's financial account (i.e., "Payment-Related Data").[25]

AB 1298 would expand this definition by adding "medical information" and "health insurance information" to the list of covered data elements:

- Medical information, defined as "any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional."[26]
- Health insurance information, defined as "an individual's health insurance policy number or subscriber information number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records."[27]

These provisions would not be limited to health care providers, but may affect any employer or other entity with computerized employee benefits or other health data.[28]

Conclusion

If enacted, AB 779 and AB 1298 will expand the scope of information covered by California's data breach notification law. They will also impose significant new burdens and liabilities on merchants doing business with California residents. Governor Schwarzenegger's actions on these bills will be available through the California Legislative Counsel's website at **http://www.leginfo.ca.gov/** and reported in an update on our Firm's Privacy and Data Security Legal Updates & News page at **http://www.mofo.com/practice/practice/privacy/overview/news.html**.

Footnotes:

[1] Copies of AB 779 and AB 1298 are available through http://www.leginfo.ca.gov/bilinfo.html.

[2] *See* Morrison & Foerster Legal Update: Merchant Liability for Security Breaches (June 2007), available at http://www.mofo.com/news/updates/files/12393.html; Morrison & Foerster Financial Services Report (August 2007), "Minnesota Ramps Up Breach Notification," available at http://www.mofo.com/news/updates/bulletins/12738.html.

[3] The term "agency" is defined in Section 1798.3(b) of the California Code of Civil Procedure. *See* AB 779, Section 1724.4(b). Under this definition, an "agency" includes any state office, officer, department, division, bureau, board, commission, or other state agency, subject to certain exceptions for the California Legislature and certain other government entities.

[4] *See* AB 779, Section 1724.4(c) ("This section shall not apply to any person or business subject to Sections 6801 to 6809, inclusive, of Title 15 of the United States Code and state or federal statutes or regulations implementing those sections, if the person or business is subject to compliance oversight by a state or federal regulatory agency with respect to those sections."). The cited provisions of the United States Code are found in the Gramm-Leach-Bliley Act, and regulate the disclosure of nonpublic personal information by financial institutions.

[5] "Payment-Related Data" means any of the following types of computerized information: account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to the individual's financial account. *See* AB 779, Section 1724.4(a) (incorporating by reference California Civil Code section 1798.82(e)).

[6] *See* AB 779, Section 1724.4(b)(1).

[7] *See* AB 779, Section 1724.4(b)(2). Sensitive authentication data includes, but is not limited to: (1) the full contents of any data track from a payment card or other payment device; (2) the card verification code or any value used to verify transactions when the payment device is not present; and (3) the PIN or encrypted PIN block. *Id.*

[8] *See* AB 779, Section 1724.4(b)(3).

[9] *See* AB 779, Section 1724.4(b)(4).

[10] *See* AB 779, Section 1724.4(b)(5).

[11] *See* AB 779, Section 1724.4(b)(6).

[12] *See* AB 779, Section 1724.4(b)(7).

[13] *See* California Civil Code Section 1798.82(a). The scope of "personal information" covered by California's breach notification law, and by the proposed expansions of AB 1298, is discussed in Section IV below. California's existing data breach notification law is available in Morrison & Foerster's free online Privacy Library, located at http://www.mofoprivacy.com/.

[14] *See* California Civil Code Section 1798.82(b).

[15] *See* AB 779, Section 1724.5(d)(1).

[16] *See* AB 779, Section 1724.5(d)(2).

[17] *See* AB 779, Section 1724.5(d)(2). The requirements of Section 1724.4 are described in Section I above.

[18] *See* AB 779, Section 1724.5(a). AB 779 adds that this information must be provided in "plain language." *Id.*

[19] *See* AB 779, Section 1724.5(b).

[20] *See* AB 779, Section 1724.5(c).

[21] *Id.*

[22] California Civil Code Section 1798.82(g)(3).

[23] *Id.*

[24] *See* AB 779, Section 1798.82(g)(3)(C). Information about the California Office of Privacy Protection is available on its website at http://www.privacy.ca.gov/.

[25] *See* California Civil Code Section 1798.82(e).

[26] *See* AB 1298, amendments to Section 1798.82(e)(5).

[27] *See* AB 1298, amendments to Section 1798.82(e)(5).

[28] AB 1298 also includes separate provisions related to security freezes on credit reports and expansion of California's Confidentiality of Medical Information Act, which are beyond the scope of the present discussion.