MORRISON | FOERSTER

Legal Updates & News

Legal Updates

California Expands Its Security Breach Notification Law But Rejects Merchant Liability Standard

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

Related Practices:

- Financial Services Law
- Privacy and Data Security

On October 13, 2007, Governor Schwarzenegger vetoed Assembly Bill 779, which would have regulated the handling of payment-related data and imposed greater liability on merchants for data security breaches.[1] The following day, Governor Schwarzenegger signed Assembly Bill 1289, which expands California's data breach notification law to cover medical information and health insurance information. This article summarizes these new developments.

I. Governor Schwarzenegger's Veto of AB 779

As explained in our September 27 update, AB 779 would have placed additional burdens on any person, business, or agency 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.[2] These obligations would have included enhanced data security standards, as well as liability for the breach notification costs of a data "owner or licensee" that is required to give notice under California's existing data breach notification law.

In vetoing AB 779, Governor Schwarzenegger acknowledged the need to protect consumers' financial information. However, he described AB 779 as an attempt "to legislate in an area where the marketplace has already assigned responsibilities and liabilities that provide for the protection of consumers."[3] He expressed concern that AB 779 "creates the potential for California law to be in conflict with private sector data security standards," such as the Payment Card Industry standards. Governor Schwarzenegger also criticized AB 779's failure to provide a clear definition of which business "owns" or "licenses" data. He commented that this ambiguity and the heightened data security requirements would "drive up the costs of compliance, particularly for small businesses." The Governor concluded by encouraging the bill's author and the payment card industry "to work together on a more balanced legislative approach" addressing these concerns.

II. Expansion of Data Breach Law to Medical and Health Insurance Information

While vetoing AB 779, Governor Schwarzenegger has expanded California's breach notification law by signing AB 1298. AB 1298 will add "health information" and "medical insurance information" to the categories of "personal information" covered by California's breach notification law.

California's 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.[4]

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

- "Medical Information" is defined as "any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional."[5]
- "Health Insurance Information" is 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."[6]

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

III. Other Effects of AB 1298

In addition to its effect on California's breach notification law, AB 1298 expands California's Confidentiality of Medical Information Act to create a new category of entity subject to its limitations on the use and disclosure of medical information. More specifically, AB 1298 amends the California Civil Code to provide that any business maintaining medical information for use by individuals or health care providers in managing that information or receiving or providing medical diagnoses or treatment is subject to the general requirements imposed on "providers of health care" by the Confidentiality of Medical Information Act.[7] Among other things, this amendment subjects such businesses to the civil and criminal penalties prescribed by the Confidentiality of Medical Information Act for improper uses and disclosures of medical information.[8]

AB 1298 also provides that, regardless of the existence of a security freeze, a consumer reporting agency may disclose public record information lawfully obtained from an open public record to the extent otherwise permitted by law.[9]

IV. Preparing for AB 1298

If your company maintains personal information about California residents, you will want to consider taking the following steps before AB 1298 takes effect on January 1, 2008:

A. Identify what types of computerized Medical Information or Health Insurance Information your company maintains, and consider the business reasons for collecting and maintaining this data. Limiting the collection and retention of protected data helps to reduce the risk and/or magnitude of a potential security breach.

B. Ensure that Medical Information and Health Insurance Information are protected by the same data security measures applied to other personal information covered by the breach notification laws (such as Social Security numbers and credit card numbers).

C. Consider encryption of Medical Information, Health Insurance Information, and other personal information covered by the breach notification laws. California's breach notification laws and the majority of other state breach notification laws provide an exemption or "safe harbor" for encrypted data.

D. Train your human resources personnel, IT personnel, and managers that Medical Information and Health Insurance Information must be handled in the same manner as Social Security numbers and other personal information covered by the breach notification laws.

E. Update your company's breach response plan to explain that Medical Information and Health Insurance Information are now covered information.

---

[1] We reported on AB 779 and AB 1298 in our September 27, 2007 update, "Pending Changes to

[2] *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.

[3] The Governor's veto message is available at http://gov.ca.gov/pdf/press/2007bills/AB%20779%20Veto%20Message.pdf.

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

[5] *See* AB 1298, amendments to Sections 1798.82(e)(4) and 1798.29(e)(4).

[6] *See* AB 1298, amendments to Sections 1798.82(e)(5) and 1798.29(e)(5).

[7]AB 1298, amendments to California Civil Code Section 56.06.

[8] AB 1298, amendments to California Civil Code Section 56.06(c).

[9] AB 1298, Cal. Civ. Code 1785.11.2(n).