

Data Security

Uniform National Standards, Penalties for Data Thieves Needed

Summary

Background

Access to information is vital. Government, law enforcement and the business community rely on data collectors to supply information for a variety of purposes. For example, schools must ensure their employees are qualified and have no criminal records. Law enforcement uses data collectors to quickly assemble a broader history of certain persons.

Recently, several businesses and government agencies have experienced the theft of data with which they operate. These data security breaches have prompted an increase in legislation addressing the issue of personal information—who has the information, who has access, how it is being used, what happens when a breach occurs and what the penalties are.

Current State/Federal Policy

California has passed more than 40 privacy laws over the last few years. Businesses that collect and share personal information are required to have privacy policies that are easily available to the public. For example, banking and financial institutions have complex rules governing how personal information is shared amongst affiliates and third parties. Other types of businesses have opt-in or opt-out provisions regarding sharing of personal information. Businesses are responsible for and must securely dispose of any records containing sensitive data. In 2003, California passed one of the first data breach notification laws requiring state government agencies, companies and non-profits to notify California customers if their personal information is reasonably believed to have been compromised. Since then, many other states have passed laws modeled on California's.

Impact on Business

When a business reasonably believes that it may have a data breach of its data systems, it must immediately notify its customers of the breach. Notification can be by surface mail or e-mail to individual customers. If costs of notification will exceed \$250,000, or the number of persons affected reaches 500,000, a business can transmit the notice via statewide media. The real damage to business comes from the loss of customer confidence and adverse media reports. Rebuilding a good business image during an economic downturn is especially challenging.

Anticipated Action

A California Chamber of Commerce-led coalition of businesses was able to negotiate amendments to legislation in 2009 to exclude information that was not necessary or useful for the customer to know, but could have compromised businesses' security and be used to harass businesses publicly. Although the coalition removed its opposition, Governor Arnold Schwarzenegger vetoed the bill. It was the third time this type of bill was introduced. Legislation expanding the type of information that must be placed in a breach notice will likely be introduced again in 2010.

CalChamber Position

The CalChamber supports establishing a uniform national standard for data security laws. The CalChamber also believes, however, that such a law must address the hackers who commit such crimes—not just the data brokers and financial institutions caught up in security breaches who are also victims. Increasing penalties on those who intentionally commit such crimes while establishing national data security standards would best help maintain the security of Americans' personal data. A safe harbor from strict liability should be provided for businesses that are in compliance with industry standards for data protection, but who suffer a breach through no fault of their own.

Reasons for Position

- Uniform national laws enhance business practices across state lines.
- Increased penalties, including jail time for both identity and data theft, deter criminal activity.
- A safe harbor encourages businesses to comply with industry standards.

Staff Contact

Valerie Nera

Policy Advocate

valerie.nera@calchamber.com

California Chamber of Commerce

P.O. Box 1736, Sacramento, CA 95812-1736; (916) 444-6670

www.calchamber.com

January 2010