

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 that their employees are qualified and have no criminal records. Financial institutions probably would not be inclined to hire or promote persons with bad credit histories to handle certain accounts. Realtors are sensitive to leasing or renting to persons with no viable history. Law enforcement often uses data collectors to quickly assemble a broader history of certain persons.

Recently, several businesses and government agencies have experienced the loss or theft of data with which they operate. These data security breaches and losses 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 pieces of privacy legislation during 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 various opt-in or opt-out provisions regarding sharing of personal information in their privacy policies. 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, as well as companies and non-profit organizations, to notify California customers if their personal information has been compromised. Since then, many other states have passed legislation modeled on the California data security law.

Impact on Business

Identity theft is rapidly becoming the fastest-growing crime in the United States. It is the number one complaint filed with the Federal Trade Commission. The term “identity theft” refers to crimes in which someone obtains and uses another person’s personal information to commit unlawful acts, usually for financial gain. Credit card theft is not necessarily identity theft, though it often is incorrectly referred to as such.

Knowing the difficulty of prosecuting perpetrators of identity theft, business spends significant resources on prevention techniques. For example, large online merchants are seeing that between 0.3 percent and 0.5 percent of sales are fraudulent, representing billions of dollars. To combat the losses, businesses are investing heavily in new fraud prevention strategies and technologies. Some have hired third-party services that provide a “risk score” on transactions, on which the merchants can base their decisions. Others have made internal changes in their processes and conduct much more consumer outreach on transactions — all of which affect a business’s bottom line.

The Payment Card Industry (PCI), which consists of the five major credit card brands, established data protection standards that apply to every organization that processes credit or debit card information. By the end of 2007 any organization that accepts payment card transactions must be in compliance. Penalties for non-compliance range from an array of monetary fines to denying an organization the ability to transact business using credit and debit cards. The PCI standards are dynamic, allowing for changes over time. New standards are always being phased in as new and better methods for protecting information are developed.

Anticipated Action

For the last two years, legislation that would prohibit many of the commonly accepted practices used by businesses dealing with credit and debit card information has been vetoed by Governor Arnold Schwarzenegger. Those bills sought to codify some of the PCI standards, creating a conflict that forces businesses to be out of compliance with either state or industry standards; punished businesses adhering to the rules but still suffering a breach; interfered with existing contractual obligations between businesses; created a strict liability standard for breach notices; and imposed other costs on many small and medium-sized businesses.

It is likely that similar legislation will be reintroduced in 2009.

Data Security (continued)

CalChamber Position

The California Chamber of Commerce supports the establishment of a uniform national standard for data security laws. The CalChamber also believes, however, that such a law must address the hackers and identity thieves who commit such crimes — not just the data brokers and financial institutions caught up in security breaches. 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 in compliance with industry standards for data protection but who suffer a breach.

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 2009