



# The California Breach Law

## Table of Contents

- The California Breach Law
  - Scope of the law
  - 'Safe harbor'
  - Who must comply
  - What constitutes a breach
  - Reporting requirements
  - Ambiguities in the law
  - Steps that companies can take
  - Protect your customer information
  - Conclusion
  - About Us
  - Contact Information



[www.centuric.com](http://www.centuric.com)

Toll Free: 1.866.376.6767 ▪ Main: 954.691.1669 ▪ Fax: 954.691.1689  
6682 NW 16<sup>th</sup> Terrace ~ Fort Lauderdale, FL 33309 USA

Centuric, the Centuric logo, and other trademarks, service marks, and logos are registered or unregistered trademarks of Centuric, LLC and its subsidiaries in the United States and other countries. All other trademarks belong to their respective owners. All rights reserved. 02/2008

### **The California Breach Law**

Last year, hackers broke into a California state database that contained the payroll and Social Security numbers of more than 250,000 state employees. It took state officials more than a month to discover the breach and two more weeks before workers were told that their personal information may have been stolen. The incident galvanized lawmakers into action.

Thus was born California Senate Bill 1386, also known as the Security Breach Information Act, which went into effect on July 1 of this year. The law requires companies that do business in California or that have customers in the state to notify them promptly whenever their personal information may have been compromised. The new law has profound implications for companies in almost every industry. Among other things, the law stipulates that companies failing to properly safeguard information or notify consumers of intrusions can be sued in civil court and face injunctions. Plus, some companies have voiced concern that going public about a security breach could damage their reputation and dampen customer confidence.

### **Scope of the law**

The California Breach Law comes at a time of sharply rising incidents of identity theft (using a broad definition of "identity theft" to include credit card fraud in addition to actual possession of someone else's identification documents). Earlier this month, the Federal Trade Commission announced that more than 27 million people have been victims of identity theft in the last five years, costing them \$5 billion and businesses and financial institutions almost \$48 billion. The FTC said that in the last year alone, 9.9 million people were victims of identity theft, primarily through credit-card fraud. Indeed, according to the FTC, identity theft is the fastest-growing crime in the United States.

The law also arrives amid increased legislative activity in Washington - aimed at making companies more accountable for the security of the information they hold. Recent passage of the Health Information Portability and Accountability Act (or HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Sarbanes-Oxley Act suggest that more laws intended to protect consumers are on the way. In fact, U.S. Senator Dianne Feinstein (D.-Calif.) introduced federal legislation in June that is largely modeled on the California Breach Law.

The new law attempts to address the problem of identity theft by requiring companies to notify California residents whose personal information has been released without authorization. "Personal information" is defined to mean "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social Security number; (2) driver's license number or California Identification Card number; (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account."

### **'Safe harbor'**

The law provides a so-called safe harbor to encrypted data. While it isn't clear whether any type of encryption will satisfy the requirements of the law, news reports have stated that some companies are deploying encryption systems to take advantage of this protection. However, deployment of an encryption system is not a safe harbor. The safe harbor applies only to data that is encrypted. To be useful, data must be decrypted; if, during that time, the data is breached, a company would be under the same reporting obligations.

### **Who must comply**

The new law requires any person or organization that conducts business in California and owns or licenses computerized personal data to notify California residents of any actual or suspected security breach. The breach can occur anywhere. For example, an insurance agency in New York whose hacked database is located in Boston must notify California customers if their financial data was stored in that database.

### **What constitutes a breach**

The law defines "breach of the security of the system" as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee of the business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

### **Reporting requirements**

The law's disclosure requirements are triggered when "unencrypted personal information was or is reasonably believed to be acquired by an unauthorized person." If there has been a breach, companies must notify the required persons "in the most expedient time possible and without unreasonable delay."

Notification may be provided by one of three methods: (1) actual notice, in writing or electronically; (2) substitute notice, in certain cases, via e-mail, Web sites, and statewide media; or (3) through a company's existing information security policy. The third option creates an incentive for companies to document a preferred notification method as part of their information security policy.

The law allows for a delay of notification only if a law enforcement agency determines that the notification will impede a criminal investigation. It is expected that this potential for obtaining delay in notification will prompt more companies to report breaches to law enforcement, resulting in a greater crackdown on identify theft.

Notification may also be delayed until completion of any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

### **Ambiguities in the law**

Legal commentators have not been shy about identifying what they consider to be the ambiguities of the new law. For example, what constitutes "reasonable belief" that personal information has been acquired by an "unauthorized person"? What is "unauthorized acquisition"? What qualifies as "encrypted"? Who must be notified when a breach occurs -- only the people affected, everyone in California, all customers? The new law also allows courts to enjoin businesses that have violated the bill from "any further activity," although it is not clear from the law what this means. Other legal commentators say the question of third-party responsibility is suggested but not clearly articulated in the law.

Legal and technology experts nevertheless urge companies to immediately familiarize themselves with all aspects of the new law. In the words of Peter Coffee, technology editor at eWEEK: "Don't let yourself become the test case that defines lack of reasonable care."

### **Steps that companies can take**

Beyond being aware of the provisions of SB 1386, there are three important steps companies can take to be responsive.

1. Above all, companies should implement information security controls to protect customer information so that the risk of being the source of a breach is minimized. Most financial services firms are likely to have sufficient information security controls already in place (and, if they don't, they will as soon as they make themselves GLBA-compliant). While it's not within the scope of this article to describe how to set up a good information security program, that may be what is required if one does not already exist.

A key objective is to explore whether full advantage is being taken of the encryption safe harbor clause. Encrypting customer data in storage is important wherever practical, although this may be difficult if the data is widely scattered across an IT environment. When encrypting data in storage is not practical, other mitigating security controls can often be implemented (such as strong access controls to the unencrypted data and intensive logging). It is also important to ensure that customer data is strongly encrypted whenever it moves across a network link. Virtual Private Network (VPN) technology is a good example of how this can be accomplished.

2. Next, companies must take reasonable measures to be able to detect when a breach has occurred so they can then fulfill their duty to notify. Waiting to learn about a breach in the newspaper is clearly a bad idea. Such detection controls should also operate to give advance warning of intrusions in many cases, allowing companies to prevent a breach and actually avoid the burden of notification. It is impossible to catch all forms of breach activity, but much can be detected.

The security tools that address this need are called Intrusion Detection Systems, or IDSs. IDSs can monitor network activity or monitor events at the device level. Firewall logs can also play a role in intrusion detection. The various intrusion detection tools tend to operate independently and generate a lot of data, however. Luckily, there are excellent tools that can gather all this data, correlate it, analyze it, and deliver more reliable alerts of intrusive activity than any single detector could provide.

3. The last step involves defining and implementing the notification processes. These processes need to be documented, and the staff involved must be trained. All those who may be involved with breach detection must know how to initiate the evaluation and notification processes - including, in some cases, communication to law enforcement.

### **Protect your customer information**

It is important for companies to keep aware that SB 1386 makes no distinction between the different possible sources of an "attack" that results in a breach. Outsiders and insiders alike can cause a breach, and breaches can be caused by simple mistakes and errors. Information may be breached in electronic, paper, or some other form. For these reasons, an information security program based on recognized sound practices is the best approach to avoiding suits under SB 1386.

Companies should also protect their systems at all levels: network, operating system/application, and the desktop. Special attention should be paid to firewalls, intrusion protection, vulnerability management, and encryption.

### **Conclusion**

While the California Breach Law has provoked concerns among some in the financial community, who worry about the long-term fallout from disclosing security breaches, it does focus attention on the importance of information security. Moreover, by strongly encouraging companies to share information about breaches with law enforcement agencies, the law could have the ultimate effect of guiding more companies to develop and implement formal security policies.

### **About Us**

Centuric offers a comprehensive suite of products and services tailored to address the complex issues facing businesses today. Some of our main areas of expertise include Network Support Consulting Services, STORServer® Managed Data Services, Infrastructure Buildout and De Novo Services.

Centuric offers great value to its clients. In business since 2001, we employ a highly credentialed staff of professionals who deliver exceptional client service. Our company is nimble enough to react quickly to market changes, and we use the latest proven technologies. We have extensive regulatory compliance expertise. We also offer options for no capital expenditures through our managed services solutions. And our dedicated support and Help Desk personnel are always available to assist our clients.

For these reasons – and more – the 2008 South Florida Business Journal recently honored Centuric with a listing in four of its “Top 25” categories:

- Fastest Growing Private Companies
- Fastest-Growing Technology Companies
- Largest IT Consultant Firms
- Largest Computer Networking Companies

Centuric uses a federally recognized standard methodology to help our clients meet compliance and mitigate security risks. We have staff certified by the National Security Agency (<http://www.nsa.gov/>) utilizing INFOSEC Assessment Methodology (IAM). Our enhanced IAM methodology encompasses the GLBA requirements as well as the responsibility to protect institutional information and systems infrastructure.

### **Our Mission Statement**

Centuric is focused on improving our clients’ business performance by providing technology solutions. Our core portfolio comprises on-site and remote support, managed services, systems integration and business applications. Our purpose and passion is to provide signature service that consistently exceeds client expectations.

### **Contact Information**

Centuric, LLC  
6682 NW 16<sup>th</sup> Terrace  
Fort Lauderdale, FL 33309 USA  
954.691.1650  
[411@centuric.com](mailto:411@centuric.com)  
Toll Free 1-866-376-6767  
<http://www.centuric.com>

*White Paper / January, 2004  
Revised February, 2008  
Source: [www.symantec.com](http://www.symantec.com)*