
Edward H. Freeman, JD, MCP, MCT

If you mess up, ‘fess up.

—Author Unknown

In recent months, the media have reported several major security breaches. Hackers have stolen the personal information of thousands of individuals from leading banks, credit bureaus, and insurance companies. In other cases, computers and disks with highly confidential data have simply vanished at the airport security counter or from vehicles parked in the company lot. Stolen data may include such sensitive information as Social Security and driver’s license numbers, financial history, and bank account numbers and balances.

In 2001, a teller at a Wisconsin branch of Bank One gave the account information and Social Security numbers of at least 250 people to a Chicago thief. The bank fired the teller but did not notify the victims. Eight months later, one of the victims discovered that someone had purchased a new Jaguar in his name. When a local television station broadcast the story, Bank One began informing the other victims.1

In March 2005, LexisNexis, a major supplier of legal and consumer research information, announced that 30,000 of its records — including individuals’ names, addresses, and Social Security numbers — may have fallen into the hands of thieves. Bank of America also announced that backup computer tapes containing information on 1.2 million of its customers were missing.2

Some security experts claim that the federal approach to such breaches has been more talk than action — to hold hearings on the urgency of the problem, to urge developers to make more secure products, and to recommend that organizations be more careful with their data. “Rather than impose affirmative obligations on manufacturers, owners, or operators of computer systems and software to take responsibility for cyber-security, these parties have been shielded from liability that might serve as an incentive to take action.”3 Efforts to combat security breaches have focused on criminal prosecution of the hacker or data thief, rather than requiring that organizations adequately secure the data entrusted to them.4

EDWARD H. FREEMAN, JD, MCP, MCT, is an attorney and educational consultant in West Hartford, Connecticut. He has written more than 50 articles on computer technology, privacy, security, and legal issues. He is also an adjunct faculty member at Central Connecticut State University, St. Joseph College in West Hartford, Connecticut, and the University of Connecticut. He can be reached at edfreeman@hotmail.com.
Congress and state legislatures are beginning to view poor system security as the cause of data breaches and to consider hacking as the inevitable result of poor system security. Although punishing hackers remains a focus of information security, some are beginning to realize that higher levels of data security are also crucial.

This article deals with the California Database Breach Notification Security Act, which requires that organizations notify California residents when they believe personal data has been compromised. It discusses the unusual case of ChoicePoint, a data-brokering company that lost 145,000 records of its customers.

**CALIFORNIA DATABASE BREACH NOTIFICATION SECURITY ACT**

In July 2003, California Senate Bill 1386, the *California Database Breach Notification Security Act*, went into effect. The bill requires businesses to notify California residents promptly if there has been a breach of security involving personal data. S.B. 1386 applies to any business with data records for California residents, even if the business is located outside the state. The business must notify affected residents when it knows or reasonably believes that an unauthorized person has accessed personal information. As defined by S.B. 1386, personal information consists of the individual’s first and last name, along with one of the following:

- Social Security number
- Driver’s license number or California identification card number
- Account number or credit or debit card number, if acquired in combination with any required security code that would allow access to the account

Notice is not required if the missing information is encrypted.

S.B. 1386 is a state law, so only California residents must be notified if a breach occurs. Companies that do not comply with the law may be subject to civil suits, including class action. Virtually every online merchant and financial institution conducts business with California residents, so all such businesses must be aware of the details of the legislation, even if they have no official presence (offices, employees, advertising) in California.

Proponents of S.B. 1386 claim that disclosure will allow individuals to protect themselves from the possibility of identity theft. Traditionally, organizations have not shared information about security breaches, choosing instead to hush up the incidents. This “conspiracy of silence” has made it more difficult for law enforcement and others to gauge the nation’s technical vulnerabilities. S.B. 1386 will force companies to pay more attention to security issues, rather than risk bad publicity and embarrassing questions after a breach.

Further, injured organizations are reluctant to bring criminal charges against hackers. Banks and insurance companies establish and maintain their reputations based on the integrity of their financial and customer data. Public revelation at trial that a teenager has accessed and may have tampered with customer records could be devastating to a firm’s credibility and reputation for integrity and financial prudence. In many cases, victimized companies have refused to press charges and allowed hackers to go unpunished, rather than risk an embarrassing trial and public disclosure of the system’s weakness. In extreme cases, firms have hired the hackers to show them how to avoid future problems.

Critics claim that S.B. 1386 will generate unending litigation from injured customers and shareholders. The act will be expensive for organizations to implement and will unnecessarily alarm citizens who receive notice. “The practical result may be a rash of false alarms delivered via notice required by this law, even though no actual acquisition of customer information has occurred. A barrage of notices warning consumers of security breaches might also eventually desensitize consumers and cause them to ignore the notices.”

By forcing companies to notify affected individuals, S.B. 1386 takes an approach...
that is radically different from the Bush administration’s cyber-security policies. Current federal policy encourages self-regulation by organizations in the industry. When problems occur, the preference is secret disclosure to government and law enforcement officials, rather than public warnings. The federal government’s policies are constructed to limit the requirement for broad disclosure and even propose to exempt companies from having to disclose such events under the Freedom of Information Act so long as they report successful attacks to law enforcement. S.B. 1386 was designed to have the opposite effect, requiring companies to report all such incidents publicly. The rapid growth of fraud and identity theft may give the Bush Administration little choice but to promote consumer notice over corporate self-regulation.

CHOICEPOINT
ChoicePoint, Inc., is a data-brokering company, traded on the New York Stock Exchange and based outside of Atlanta. The company concentrates on selling information and data services to the insurance industry, businesses, government agencies, and direct marketers. The company reported 2004 revenues of almost $800 million. ChoicePoint is a spin-off of Equifax, one of the three major credit-reporting firms in the United States. On its Web site, ChoicePoint describes itself as: “the nation’s premier source of data to the insurance industry … [and] the premier provider of decision-making intelligence to businesses and government. Through the identification, retrieval, storage, analysis and delivery of data, ChoicePoint serves the informational needs of businesses of all sizes, as well as federal, state and local government agencies.”

Most states do not consider ChoicePoint to be a financial services company, so the firm is not subject to the same data laws as banks and credit bureaus. As businesses have tried to reduce their credit risks, the demand for organizations that will provide data on potential customers has increased. Customer information also allows organizations to target their sales and marketing efforts. To meet these goals, ChoicePoint has gathered information about virtually every adult in the United States, accumulating more than 19 billion records. Any organization that controls that much personal information (almost always without the consent or knowledge of the individual) would seem to have a moral, if not legal, obligation to use highly sophisticated technology to safeguard the data. Interestingly, the theft of data from ChoicePoint was not the result of computer hacking.

An imposter accessed the data by simply claiming over the telephone and on written forms to be somebody he wasn’t. Olatunji Oluwatosin, a 41-year-old Nigerian national, claimed to be a collection agent. He filed the paperwork to download reports on individuals at $15 each, using Kinko’s Copy Center in Hollywood, California, as his return address. ChoicePoint’s business policy required that customers fax copies of their business licenses. ChoicePoint would conduct a background check to ascertain that the licenses were valid for nonbank financial institutions. They did not generally check or visit the addresses to make sure they were legitimate.

On October 27, 2004, Oluwatosin was lured to Kinko’s, arrested, and charged with identity theft. Investigators said that he had submitted forged business licenses to gain access to the personal data, including Social Security numbers, of several thousand people. Oluwatosin pled “no contest” to a single count of identity theft and was sentenced to 16 months in jail.

In February 2005, ChoicePoint acknowledged that other thieves had used previously stolen identities to create bogus businesses and open at least 50 accounts with the firm. The thieves obtained volumes of data about consumers, including names, addresses, Social Security numbers, and credit reports. Under S.B. 1386, ChoicePoint was required to notify California consumers that their personal data was at risk. Originally, ChoicePoint had announced that it was
going to inform only California residents. When California residents received letters about the security breach, attorneys general in 18 other states also requested notification for their residents. After criticism in the media, ChoicePoint announced that it would notify affected customers everywhere. One victim stated, “Thank God for California because if they didn’t have that law, this stuff would have been swept under the rug.” The list of those whose private information was at risk includes residents of all 50 states, as well as Guam, Puerto Rico, and the Virgin Islands.

ChoicePoint announced that they had notified 145,000 people that their personal information might have been stolen. The letter, signed by CEO Derek Smith, started, “I’m writing to inform you of a recent crime committed against ChoicePoint that MAY have resulted in your name, address and Social Security number being viewed by businesses that are not allowed to access such information.” It urged consumers to check their credit reports for suspicious activity. “We believe that several individuals, posing as legitimate business customers, recently committed fraud by claiming to have a lawful purpose for accessing information about individuals…. You should continue to check your credit reports frequently for the next year.” The two-page letter offered details on how to spot fraud but provided no additional information about the incident or what information may have actually been stolen.

After conducting its own investigation, ChoicePoint described the kind of data that had been compromised: “These fraudsters accessed products that contained basic telephone directory-type data (name and address information) as well as combination of Social Security numbers and/or driver’s license numbers, and, at times, abbreviated credit reports. They were also able to obtain other public record information including, but not limited to bankruptcies, liens, and judgments, professional licenses, and real property data.”

On its Web site, ChoicePoint apologizes for its actions and explains how it will avoid any repetitions. Among other changes, ChoicePoint will:

- Provide affected customers with free credit reports and a one-year subscription to a credit monitoring service.
- Discontinue sale of personally identifiable information products unless the customer meets strict qualification requirements.
- Reestablish the credentials of business clients to be sure that they can access only the data to which they are entitled.
- Company officials will be visiting customer sites.
- Private investigators and some debt collectors will be allowed to see only “truncated versions” of Social Security numbers, driver’s licenses, and credit reports.
- Create an independent office of Credentialing, Compliance and Privacy that will report to the Board of Directors’ Privacy Committee.
- Appoint an executive to serve as liaison with law enforcement officials.

Pam Dixon of the World Privacy Forum, a nonprofit privacy watchdog group in San Diego, referred to the incident as the “Exxon Valdez of privacy.” The Senate Banking Committee and the Federal Trade Commission (FTC) are conducting hearings over the issues raised. Several class action suits are pending against ChoicePoint.

ANALYSIS
Identity theft has become a critical issue in recent years. Almost every general-interest magazine contains articles about identity theft and how an innocent victim’s life and reputation are destroyed when an outside party gains access to confidential financial data.

S.B. 1386 serves two purposes: to warn individuals when their financial data has been accessed by inappropriate parties and to shame organizations that are lax in protecting this data. This approach will encourage data gatherers to be more careful with
their databases, but only after the damage has been done. Self-regulation has been shown to be ineffective in policing the industry. ChoicePoint’s troubles came about because it failed to develop an adequate method to protect their databases from inappropriate access. A data gatherer such as ChoicePoint does not have the same need to maintain its reputation for integrity as does a bank or insurance company.

There is a clear need for Congress and the FTC to police data-gathering firms and data brokers. S.B. 1386 is a positive step, but it is not enough. Steps to crack down on “mail order credit cards” would be beneficial, and would have prevented a situation in California where a dog applied for and received a credit card. The FTC must develop a firm set of rules for data brokers such as ChoicePoint. States should also have the right to develop stronger measures if they see fit. Individuals should have the absolute right to see their records, with streamlined procedures to modify incorrect data. Such a system has worked well with the three credit reporting agencies for many years.

ChoicePoint has presented the issues of data security in clear terms. The courts and the federal and state governments must take appropriate actions to prevent such mishaps from recurring. Only then will personal data truly be personal.

Additional Information

Notes
1. Matthew Heimer and Stephanie Williams, Identity Crisis, Smart Money, December 17, 2002.
5. California Civic Code §1798.82.
17. Bob Sullivan, Database Giant Gives Access to Fake Firms, ChoicePoint Warns More Than 30,000 They May Be at Risk, MSNBC, February 14, 2005.