

Importance of a PCI Security Assessment

Written by Dave Hogan

Regulatory scrutiny and compliance requirements have significantly increased over the past year. The requirements imposed by the credit card companies have now been consolidated into a single standard named the Payment Card Industry (PCI) Data Security Standard. ([PCI Data Security Standard](#))

In addition to these requirements, several states have enacted laws requiring disclosure of any potential breach of consumer privacy. The laws, based off the CA SB 1386 requirement, establish penalties and expose companies to civil liability litigation. Such regulations are now on the books in California, Arkansas, Georgia, Montana, North Dakota and Washington and are in process in New York City, Florida, Illinois and Indiana. The number of states enacting these regulations makes disclosure a de facto national requirement.

The widespread nature of the threat to personal data is now obvious, based on the number of companies that have been forced to disclose breaches of security. These have ranged from DSW, BJ's, ChoicePoint Inc. and Axiom to Lexis Nexis.

Some of these breaches have resulted in lawsuits such as Sovereign Bank's lawsuit on BJ's Wholesale club.

<http://philadelphia.bizjournals.com/philadelphia/stories/2005/02/14/story4.html>

The California Department of Consumer Affairs reported May 27 that since the state's notification law went into effect in July 2003, it has been aware of 61 significant breach notifications involving an average of 163,500 individuals each

In the last few months, several major companies reported that customer data, including credit-card information, was compromised. The list includes:

COMPANY	DATE ANNOUNCED TO GENERAL PUBLIC	# OF PEOPLE AFFECTED	AFFECTED DATA	SECURITY BREACH	RESPONSE
Major Clothing retailer (See article)	April 14	As many as 180,000 customers who hold GM-branded MasterCard	Credit-card data	n.a.	Card issuer HSBC notified consumers
Major Shoe store chain (See article)	March 8	Initially, the theft was said to be limited to about 100,000 customers; a month later, it was raised to 1.4 million	Credit- and debit-card, checking account and driver's license numbers, and personal-shopping information	Hackers stole data from a database for 108 of the chain's 175 stores	Reported to federal authorities. Customers advised to check credit-card statements.
Compiler of consumer data (See article)	Feb. 15	About 145,000 consumers had data in the system. At least 750 fraud cases are known.	Addresses, Social Security numbers and credit reports	Thieves posing as legitimate customers bought information.	Informed federal authorities. Will no longer sell sensitive personal data to clients other than governmental

					agencies, accredited corporate customers or other businesses whose use is driven by a consumer-initiated transaction.
Online discount stock broker (See article)	April 19	About 200,000 current and former customers from 2000 to 2003	Varies by customer	Backup computer tape was lost in shipping	Notified affected consumers
Media conglomerate (See article)	May 2	About 600,000 current and former U.S. employees back to 1986	Social Security numbers and details on beneficiaries and dependents	Backup computer tape was lost in shipping by an outside data-storage company	Notified those affected
Telecommunications company (See article)	May 23	About 16,500 current and former employees	Social Security numbers	Laptop containing the names and Social Security numbers was stolen from a car that was parked in the garage at the home of an MCI financial analyst.	Notified law-enforcement officers and those affected in April after the incident
Bank and financial-services company (See article)	June 6	About 3.9 million current and former U.S. customers of its CitiFinancial lending unit	Undefined "personal information"	Computer tapes were lost by UPS while in transit to a credit bureau	Notified affected customers, offered credit monitoring
Bank and credit-card company (See article)	Feb. 25	Holders of as many as 1.2 million federal-government charge cards	Social Security numbers	Computer backup tapes were lost.	Contacted federal authorities, then consumers.

Sources: WSJ, Associated Press, the companies

Note: Unless where noted, these are cases of data being at risk, not of data being fraudulently used. In all cases the stolen data included the names of the affiliated consumers.