

Security Breaches Result in Flurry of Legislation

According to Senator Dianne Feinstein (D-CA), since February 2004 there have been at least 12 major breaches of security databases, placing 10.7 million people at risk of identity theft. Among those whose security has been compromised are ChoicePoint (145,000), Bank of America and Wachovia Corp (100,000 combined) and at least two other banks may have had up to 600,000 customers affected; LexisNexis (310,000); DSW Shoe Warehouse (half its customer base); Boston College (106,000 alumni); and Chico State University of California (59,000 current, former, and prospective students). As expected, these breaches have prompted privacy advocates and state and federal officials to call for greater scrutiny of companies that buy, store, and sell consumer data. Currently, there is no federal law that requires data brokers to notify customers of security breaches. Rather, the industry is governed by a myriad of state and federal laws.

Reaction to this has been quick and promises to protect consumers as many state legislatures have introduced bills that will require customer notices when personal data has been compromised. According to recent information several states have already passed laws and as many as 20 other bills may be pending. Here's what happened:

- California and Texas have "security freeze" laws in place. Texas is looking at additional legislation to strengthen the existing laws. Security freeze laws are set to take effect this summer in Louisiana and Vermont. The Illinois bill that was introduced would give identity theft victims the ability to freeze their credit reports and prevent others from changing or revising the information.
- Colorado, Connecticut, Hawaii, Indiana, Maine, Maryland, Massachusetts, Nevada, Oregon, and Utah also have security freeze legislation pending, according to Gail Hillebrand, senior attorney for Consumers Union.
- New York is considering three bills modeled after the California law. One bill would require businesses and state agencies to notify consumers of any security breach of their data. It also provides for the recovery of damages by security breach victims. The other two bills would cover only businesses, not state agencies, and would establish a private right of action for individuals whose data security has been breached.
- Washington and Florida are considering bills. In Washington, the bill would require that consumers be notified of any breach of data security "without unreasonable delay, consistent with the needs of law enforcement." Personal information is defined as Social Security numbers, driver's license, and credit and debit card numbers in combination with access codes. In Florida the proposed law would require immediate disclosure when an individual's private personal financial information or Social Security number is stolen from a data collection agency.
- Minnesota has two proposed bills that would require notification in "the most expedient time possible and without unreasonable delay" if information is taken by an unauthorized person.
- Rhode Island and Georgia have introduced bills that would require any business experiencing a security breach to immediately notify residents that their financial documents or identities may have been compromised.

With many of the states considering security freeze laws, consumers should be aware of the pros and cons of such laws. The freeze technique makes it almost impossible for criminals to use stolen information to open bogus new accounts because once the information is frozen creditors cannot review the credit history. Because most companies will not open new accounts without this type of information, it follows that the criminal will be out of luck. On the other hand, though, consumers need to realize that freezing their account can be a real hassle because they usually have to send a certified letter to all the credit reporting agencies (CRAs), sometimes including copies of police reports of the theft, and pay fees. When the consumer wants to “unfreeze” the account and get credit, they may have to pay additional fees and send another notification to the CRAs. Consumers may well decide it is worth the effort if they believe their personal information has been compromised.

While consumers may believe they have little if any ability to prevent identity theft, it is important that they remain vigilant in checking credit reports frequently and protecting their personal information as best they can.

In the meantime, Senator Feinstein is taking the lead in the U.S. Senate by introducing a tougher version of her identity theft bill that would set federal standards for consumer notification of security breaches involving personal information. Her bill does not include a substitute notice provision that would allow companies to use the Internet Web site posting or media release. It would require that consumers receive individual letters or e-mails. With the identity theft problem growing, Senator Feinstein believes that companies must ensure that all people will be notified personally when their private information is at risk.