

RELIEF FROM THE ID THIEF

Lawmakers continue to battle the growing crime of identity theft.

By Heather Morton

The number of consumers whose personal information, including Social Security numbers, driver's licenses and credit card numbers, has been exposed to potential identity theft is staggering. Hackers gained information on 1.4 million consumers from Discount Shoe Warehouse, for example. Bank of America back-up tapes containing information on 1.2 million government workers have been lost. Other large companies—including Ameritrade, CardSystems and Motorola—have also suffered security breaches.

Businesses are not the only ones having trouble keeping their databases safe. Information on more than 100,000 University of California students and applicants was stolen, and 33,000 Air Force officers and some enlisted personnel were notified that their online Assignment Management Sys-

tem was hacked. Even the Federal Deposit Insurance Corporation in 2003 disclosed that information regarding roughly 6,000 current and former employees was breached.

Consumers are justifiably concerned. Results from a May 2005 Gartner survey revealed that one third of the 5,000 people contacted are "very concerned" about being victimized by identity theft, causing nearly half to curtail their online activities. A smaller survey of likely voters released by the Cyber Security Industry Alliance, an industry group, had similar results. According to that survey, 71 percent of voters believe new laws are needed to protect consumer privacy on the Internet.

Responding to constituent concerns, legislators have increased penalties, made it easier for victims to report identity theft, and limited the availability of personal information. State lawmakers also have created new solutions such as security breach notifica-



tions, consumer report security freezes and identity theft passports. Despite these measures the crime continues to grow.

PUBLIC NOTIFICATION

The practice of letting the public know about the breaches in database security is due in part to California's 2002 Notice of Security Breach law. This law, sponsored by Senator S. Joseph Simitian, requires that Cal-



ifornia residents be notified when unencrypted computerized data that include personal information maintained by a business or a state agency may have been acquired by an unauthorized person.

"It is a simple law that we hope will do four things: give every California resident the protection of notice, improve data security around the state and nation, spread awareness to other states and get the federal government involved," says Senator Simitian.

As news of the recent breaches spread, lawmakers in at least 17 states passed legislation. Although many states have followed California's law, several have expanded the

DATA DESTRUCTION

More identity thefts occur because of information retrieved from the garbage can than from computers, according to a recent survey by the Better Business Bureau/Javelin. So several states have passed laws to control the way documents—and in some cases computer hard-drives—can be discarded.

In Texas, records to which public access is restricted may be destroyed only by burning, pulping or shredding. California allows court records to be destroyed by shredding, burial, burning, erasure, obliteration or recycling, as long as the text of confidential and sealed records is obliterated before recycling.

In the past few years, lawmakers have focused on what should be destroyed. Tennessee specifically requires businesses to destroy customer records containing personal identifying information, including Social Security numbers, driver's license numbers, checking or savings account numbers, credit card numbers, health insurance numbers and unique biometric data. If they don't, they'll be fined \$500 for each record, up to \$10,000. Wisconsin's law applies to medical businesses, financial institutions and tax preparation businesses. Washington includes records that can be transmitted electronically.

Recent bills focused on security breach notification have included provisions about destroying records containing personal information. Arkansas, Montana, New Jersey and Rhode Island have all included such provisions in their 2005 security breach notification laws.

Federal laws also mandate destruction of certain records. The Fair and Accurate Credit Transactions Act applies to information derived from a consumer credit report and the Health Insurance Portability and Accountability Act covers "protected health information" which relates to physical and mental health conditions and any health care plans.

—Ricardo Ochoa, NCSL

definition of personal information that would trigger the notification requirement.

SECURITY FREEZES

State lawmakers have also tried to combat identity theft and help victims by requiring a consumer report security freeze. First enacted in 2001 in California, sponsored by Senator Debra Bowen, the freeze limits a consumer reporting agency from releasing a credit report or any information regarding the consumer without specific authorization from the consumer. In practice, the freeze allows identity theft victims to track whether the thief is trying to open new accounts with their identification. By using a special password or identification number, a victim can temporarily lift the freeze if he or she needs to open a new account. Louisiana and Texas enacted similar legislation in 2003, and Vermont followed in 2004. Colorado, Connecticut, Illinois, Maine, Nevada, New Jersey, North Carolina and Washington enacted laws in 2005.

"This is a proactive approach that will allow consumers to block fraudulent credit applications. It gives victims an important tool to help repair their damaged credit," says Washington Senator Jean Berkey. The security freeze laws in Illinois, Texas, Ver-



SENATOR
JEAN BERKEY
WASHINGTON

mont and Washington are limited to identity theft victims, while the other states give all consumers the option to place a freeze on their credit history.

The consequences of identity theft can take years for the victim to resolve. Victims often report that identity thieves use their information over and over, even if the crime has been reported to the police. And a thief may use the victim's information for more than just opening new credit card accounts. A thief may use the victim's name and address if pulled over by the police for a traffic offense and issued a speeding ticket. More than likely, the thief does not appear for the scheduled court date, leading to an arrest warrant in the name of the victim. It can be very hard for the victims to prove their innocence.

Identity theft costs \$55 billion annually, \$50 billion of which is borne directly by businesses, according to a July 2005 study by the Progress & Freedom Foundation (PFF). Firms also lose business after disclosing security breaches, and 58 percent of Americans have a decreased sense of trust and confidence in an organization reporting a security breach, according to an August 2005 survey by the Ponemon Institute, a privacy research organization. However, a majority of Americans—59 percent—also do not have confidence that state or federal regulations will protect them from data security breaches, according to Ponemon.

According to PFF, the costs of security breach notifications to business and commerce are likely to be substantially higher than the benefits to consumers. PFF notes that most security breaches do not result in harm to individuals, but "can heap huge expenses on businesses pocketbooks and reputations." Companies also complain about the difficulties in complying with differing requirements in state security breach laws.

Credit freeze legislation has also come under criticism. Industry representatives note a lack of evidence showing that credit freezes are effective in reducing identity theft. Stuart K. Pratt of the Consumer Data Industry Association, in testimony before the U.S. Senate Committee on Banking, Housing and Urban Affairs in September 2005, said that although some state laws have been effective for years, only a small percentage of consumers have taken advantage of them.

The potential losses to businesses provide strong incentives for companies to protect against identity theft. Both business and government are seeking the best ways to protect consumers from the growing problem of identity theft.

—Pan Greenberg, NCSL

IDENTITY THEFT PASSPORTS

Legislators have created the identity theft passport to document the innocence of ID theft victims. In order to obtain the identification card, the victim must submit a police report or a judicial expungement order to show that he or she has been victimized. The victim's name is then placed in a database that law enforcement agencies can access and the ID theft victim receives an identification card. These passports may be used to help victims when they are disputing bogus accounts and charges.

Virginia was the first state to enact the passport program in 2003. Mississippi and Oklahoma followed in 2004. "While much of the identity theft legislation we've seen in the past has targeted the criminal, this bill was written to provide some aid to the victims," says Oklahoma Senator Mike Johnson, co-sponsor of the Oklahoma legislation.

This year, Ohio went one step further by requiring a picture and fingerprint to be included in the victim's record in the database.



SENATOR
MIKE JOHNSON
OKLAHOMA

Arkansas, Montana and Nevada enacted laws in 2005 as well.

"Identity theft passports are the first major way to help consumers use something tangible to get their credit back in order," says Ohio Representative Jim Hughes. "Requiring a



REPRESENTATIVE
JIM HUGHES
OHIO

photo and fingerprint helps to prevent sophisticated criminals from abusing this program." Hughes speaks from experience as both a victim of identity theft and a former prosecutor.

EVOLVING STRATEGIES

Despite various efforts to halt ID theft—increasing penalties, streamlining reporting, and limiting the availability of personal information—it continues to grow. The Federal Trade Commission reports that ID theft has topped the list of consumer complaints for the last five years. Identity thieves change and adapt in response to legislation and law enforcement efforts. Combating it takes a team effort from policymakers, businesses and vigilant consumers. Staying one step ahead of the thieves is an ongoing battle. ■