NATIONAL EDITION
Los Angeles Times

July 13, 2003

A Blow to Identity Thieves

Perhaps the only thing worse than learning that thieves have hijacked your Social Security and credit card numbers is to discover that you might have been able to stop them before they bought big screen TVs, leather jackets and a taste of the high life in Las Vegas.

The number of people who steal Social Security numbers to open credit card accounts, write bad checks and buy cars has surged in recent years. Usually, victimized consumers — an estimated 700,000 last year — don't know they've been hit until the thieves have maxed out the credit cards and bill collectors start calling. Often it takes years to restore their good credit.

Until now, a database hacker could be running up bills on your credit card while you were kept in the dark. A worthy new state law aims to remedy that.

A welcome new law that took effect last week can help deter these identity crooks before they begin their shopping sprees. Assemblyman Joe Simitian's (D-Palo Alto) AB 700 requires businesses and government agencies to quickly notify customers if their personal information might have been stolen from computer databases. In the past, some outfits have kept silent for weeks or months, either too embarrassed to acknowledge the break-in or indifferent to the consequences.

The law works like this: When an agency or company of any size, anywhere in the country, discovers that a hacker or other criminal may have obtained customers' personal data, it must now inform Californians in that database of the security breach "without unreasonable delay." This is a loose standard but better than the current lack of any standard, which gives consumers no way to measure liability.

If companies fail to notify, the fraud victims can sue for damages. Even better, consumers who know their personal information may have been stolen can cancel credit cards, close accounts or just monitor their bank statements more closely.

Acting on the principle that what's good for Californians is good for all Americans, Sen. Dianne Feinstein (D-Calif.) introduced a bill last month to impose virtually the same notification requirements nationally.

Some consumer and business attorneys grumble that these measures should be more specific — for example, spelling out how quickly individuals should be notified and under what circumstances.

The measures may indeed have to be tightened if businesses try to turn the vague language into loopholes. However, Simitian and Feinstein have struggled to help consumers without saddling business with costly burdens or impeding criminal fraud probes.

Legislation intended to prevent identity theft is much needed, and it treads new terrain. Simitian and Feinstein say their goal is as much to push businesses toward tighter information security as it is to prevent consumer rip-offs. These are worthy first efforts.

SERVING THE COUNTY SINCE 1856

Santa Cruz Sentinel

June 24, 2003

Businesses must tell customers if hackers break in

SENTINEL STAFF & WIRE REPORT

SAN JOSE — California consumers will learn next month whether their favorite shopping sites are steeled against computer fraud — or haunts of hackers and identity thieves.

Starting July 1, companies must warn California customers of security holes in their corporate computer networks. When a retailer discovers its credit card numbers have been stolen, it must e-mail customers, essentially saying, "We've been hacked, and the hacker may have your credit card number."

State politicians call the regulation the first of its kind in the United States, and it could become the model for a nationwide law. U.S. Sen. Dianne Feinstein plans to introduce similar legislation within a month.

"Corporate and government databases are increasingly becoming targets of identity thieves seeking Social Security numbers and other sensitive personal data," the California Democrat said in an e-mail. "Under current law, all too often people are unaware that an identity thief has gained this information and may be using it to run up credit card bills or use it to manufacture a new identity."

Assemblyman Joe Simitian, D-Palo Alto, author of the bill, said Monday the goal was to "give consumers the information they need to protect themselves."

"Obviously, they can't do that if they aren't aware that their security has been compromised," he said.

Also, he said, the bill gives some companies "a nudge" toward improving security faster.

"The question was ... whether consumers have a right to know when their security has been compromised, and the Legislature said, 'Yes, they do,'" said Simitian.

Simitian expects more companies will begin using data encryption technology in light of the bill, since encrypted data is exempted from the legislation.

California's new regulation contrasts with the Bush administration's hands-off treatment of the technology industry, particularly when it comes to controversial e-commerce issues such as privacy and fraud.

Although the FBI and Federal Trade Commission have hunted down Web site operators involved in fraudulent sales and auctions, proponents of the laissez-faire approach worry that regulations would hamper innovation in a fledgling industry.

"You cannot legislate good behavior," said eBay Chief Security Officer Howard Schmidt, who resigned this spring as a top cyber security adviser to President Bush. "The administration's policy was not to look to legislation or regulation to improve security but to look to market forces to drive it."

But many technology executives and legal experts applaud the bold attempt to crack down on identity theft, one of the fastest growing crimes.

The U.S. Postal Service reports

that 50,000 people a year have become victims of identity theft, and the U.S. Treasury Department says thieves ring up $2 billion to $3 billion per year on stolen credit cards alone. As victims expend hours or days canceling debit and credit cards, obtaining new ones and re-establishing accounts and passwords, corporate America loses billions of dollars more in productivity.

Proponents say the California bill makes executives more accountable for computer fraud. It doesn't impose specific monetary fines, but the regulation makes companies with questionable computer networks more vulnerable to lawsuits and public scorn.

"It's a wake-up call for companies to make major, across-the-board changes in every part of the company," said Nick Akerman, an attorney specializing in computer fraud in the New York office of Dorsey & Whitney. "Companies are afraid to report breaches because they think it reflects badly on them, and they don't want the bad publicity of becoming known as a company that's been hacked into. This bill says, 'You can't continue business as usual.'"

The regulation applies to any company that stores data electronically and does business in California. Companies must alert customers whenever "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

The bill defines "personal information" as an individual's first name or initial and last name, with one of the following: Social Security number; driver's license number; state identification number; or credit or debit card account number and security code.

Except when disclosure would impede a criminal investigation, companies must notify consumers "in the most expedient time possible," with an e-mail or letter.

If a hacker gains access to data for 500,000 or more customers, the company might have to notify people through e-mail, a "conspicuous" posting on a Web site and disclosure to a major media outlet.

Locally, the Lighthouse Venture Forum will tackle the topic of whether the government should regulate corporate security on Wednesday at 7 a.m. at DeLaveaga Golf Course Lodge, 401 Upper Park Drive, Santa Cruz.

Speakers are Robert Mykland, a high-tech entrepreneur, and Davi Ottenheimer, an information systems security expert.

For reservations, call 457-7778.

Staff Writer Karen Davis contributed to this report.

Contact Karen A. Davis at kdavis@santa-cruz.com.

San Jose Mercury News

September 30, 2005

U.S. no help in quest for database security law

INACTION OBLIGES STATES TO PROTECT CITIZENS' PRIVACY

By Joe Simitian

Lead, follow or get out of the way. It's not a particularly gracious sentiment, but when it comes to our federal government's role in protecting our privacy, it certainly is apt.

To date, Washington has proven itself either unable or unwilling to take the lead in protecting our personal privacy. That being the case, California passed legislation in 2002 requiring that notice be provided to individuals in a public or private database whose personal information has been compromised.

Now the folks in our nation's capital would do well to either follow California's example (as California Sen. Dianne Feinstein has suggested with her Database Security Breach Notification Act), or get out of the way and let the states take action one by one if that's the only way to get the job done.

California's privacy-protection law is simplicity itself: When your personal information is lost, is stolen or has strayed from a database, the folks who own or manage that database — and hold your identity information in trust — are obliged to tell you about it so you can take steps to protect yourself.

The premise is simple. What you don't know can hurt you. Ignorance is not bliss. Until and unless you know that your personal information is in the wrong hands, you can hardly take the steps to protect yourself.

In protecting the public's privacy, Washington certainly has not led; and now, it appears, Washington is unprepared to follow.

Regrettably, this rather simple, commonsense notion has met stiff resistance in Washington.

When the California Legislature took action in 2002 requiring notice of a security breach, our goals were clear and specific.

First, of course, to provide Californians with the knowledge they need to protect themselves. Also, to provide an incentive to those responsible for public and private databases to improve their security (and thus reduce the risk of identity theft for all of us). These goals have clearly been realized.

We also hoped, but were not sure, that consumers around the country would also be protected to some degree, since as a practical public-relations matter it's difficult to inform only the customers in California when a national database is hacked.

Finally, though, we hoped to prod the federal government into taking meaningful action on a national level. Indeed, many of the opponents to California's privacy law argued against a state law in favor of a federal approach. A patchwork quilt of state-by-state statutes, they argued, was not the ideal.

This argument would have been more persuasive, perhaps, had not those same opponents been arguing against such requirements in Washington. Or if Washington has shown an inclination to tackle the problem.

Regrettably, despite Sen. Feinstein's prodding, that does not appear to be the case. In protecting the public's privacy, Washington certainly has not led; and now it appears, Washington is unprepared to follow.

This past week we were treated to yet another report of a data breach/security lapse (this one close to home, at the Children's Health Council on the Peninsula). A constant flow of such reports, however, has not moved our federal government. So get out of the way, D.C., and let those who will lead take the next steps in protecting the privacy of Americans throughout the 50 states.

SEN. JOE SIMITIAN, D-Palo Alto, represents California's 11th District and is the author of California's Security Breach Notification Law. He wrote this article for the Mercury News.

USA TODAY

March 1, 2007

Lawmakers get less combative on data-breach bills

Change from previous years

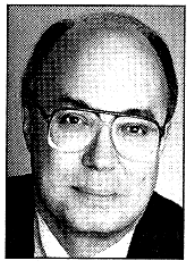
By Jon Swartz
USA TODAY

SAN FRANCISCO — It's Round 2 in Congress' bid to craft federal law that would require businesses to notify U.S. consumers about computer data-security breaches.

Technology

Legislation introduced in February soon could become law, given the cooperative tone of federal lawmakers, says Ari Schwartz, a privacy advocate and deputy director of the Center for Democracy & Technology. That would be a reversal from the previous few years, when members of the House and Senate could not agree on a national data-breach law, and dozens of states passed their own laws.

But the feds waited too long to act, and their actions now are unnecessary, say state legislators and privacy advocates. "With so many conflicting agendas from the financial industry, data brokers and security companies, there is the danger any bill could be watered down," says Evan Hendricks, editor of *Privacy Times* newsletter.



Simitian: California state senator.

The fear is that a federal law would pre-empt stronger state laws. "A national standard that provides less protection than currently afforded is really a step backward, not a step forward," says state Sen. Joe Simitian, D-Calif., author of the first law in the USA that required companies to publicly disclose data breaches.

More than 100 million records containing personal information have been subject to some sort of security breach since February 2005, starting with data broker ChoicePoint, according to the non-profit Privacy Rights Clearinghouse.

There are at least four bills in Congress this year to address data-breach notification that would pre-empt 35 state laws on the books.

Last year, Congress came up with at least six bills. They all fizzled.

One bill watched closely this year is by Sens. Patrick Leahy, D-Vt., and Arlen Specter, R-Pa. It would require companies to publicly disclose data breaches and would make it a federal crime to intentionally conceal them.

Introduced Feb. 6, it would mandate security programs at companies that handle sensitive personal data and allow consumers to view and correct information that data brokers have about them.

Another provision would let federal agencies examine the quality of data security at private data brokers with which they contract.

Businesses with operations nationwide prefer a uniform standard rather than a patchwork of laws they would have to address on a state-by-state basis, says Thomas Boyd, an attorney who represents financial services companies.

"(They're) anxious for legislation that protects consumers in the 15 states that have not yet acted, along with those which have, by mandating data security and reasonable notification procedures," Boyd says.

Security companies also prefer a uniform law, and beyond that, security standards, says Liz Gasster, general counsel at the Cyber Security Industry Alliance, which represents about 20 companies, including Symantec and McAfee.

"We've got 35 states with data-breach laws, but only six have data security requirements," she says. "A federal law is necessary beyond just reporting data breaches after the fact."

Simitian wants to keep data laws simple. He says public disclosure is enough incentive for companies to protect sensitive information.

Historically, state laws precede federal regulations and go further protecting consumers, privacy experts say.

"California has set a national standard, for the most part," says Deirdre Mulligan, a law professor specializing in tech issues at the School of Law at University of California, Berkeley.

When Californians are notified of a breach, it's hard to keep that a secret, Mulligan says.