

Victims of ChoicePoint data breach didn't take advantage of free offers

Panel of industry, government leaders discuss finding better ways to protect personal data and notify consumers

By [Jon Brodtkin](#), Network World, 04/10/07

When ChoicePoint became [one of the first companies](#) to admit to a high-profile data breach involving sensitive consumer information, the company offered 163,000 affected individuals free credit monitoring, credit reports and identity-theft insurance.

Barely anyone took the company up on its offer.

"We put out a 1-800 number, all this free stuff that people pay a lot of money to get . . . and fewer than 10% of the people we sent notices to ever called us, ever asked us for any of the free services," Robert Kamerschen, ChoicePoint's vice president of law and public policy, said Monday during a panel discussion on cybersecurity and consumer data in Boston. "People debated why this is, and I'm not sure I know what the answer is."

The American public may be so jaded that people simply throw mail in the trash when it comes from organizations they've never heard of, Kamerschen suggested. Monday's discussion, hosted by [O'Neill and Associates](#), focused partly on the issue of how consumers should be notified of data breaches in the context of state laws that are popping up around the country.

ChoicePoint, which provides information to the home and auto industries and performs background checks for about half of the companies on the Fortune 500, is one of many firms [forced to apologize](#) after data breaches that have exposed more than 150 million records containing personal information since 2005. In the ChoicePoint case, the records of 163,000 consumers were compromised after criminals pretending to be legitimate ChoicePoint customers sought details about individuals listed in the company's database of personal information.

Although U.S. law covers privacy in industries such as healthcare and the financial sector, "there is no generally applicable federal statute that governs the protection of personal data," Lois Johnson, senior counsel for policy and government for Massachusetts Attorney General Martha Coakley, said during the panel session.

About 35 states require notification of customers after security breaches involving personal information, and 25 states give consumers the right to freeze access to their credit reports to prevent new credit from being taken out under their names, Johnson said. Massachusetts has done neither, but Coakley is making identity theft a priority, she said.

"A security breach at Massachusetts' own TJX Corp. may have affected as much as [47 million people worldwide](#)," Johnson said. "The attorney general herself was a victim of ID theft. Earlier this year, her credit card was used to purchase a computer in another state. That was really the wrong credit card number to steal."

Massachusetts lawmakers Tuesday are scheduled to discuss several proposals to tighten protection of personal data. Monday's event, titled "Cyber Security and Consumer Data: State and Federal Efforts to Prevent Cyber Fraud," included Sen. Michael Morrissey of Massachusetts, chairman of the Joint Committee on Consumer Protection and Professional Licensure.

Efforts to protect sensitive information over the years have been hampered by concern from various groups, including genealogists, Morrissey said. The information cyberterrorists need to make phony IDs is also used by genealogists in their line of work, he said.

Also speaking Monday was Doug Maughan, who works in cybersecurity research and development in the [U.S. Department of Homeland Security](#).

Cyberattacks on publicly traded firms result in a 1% to 5% loss in stock price, which can represent \$50 million to \$200 million, federal research has found, according to Maughan. A [report from Symantec](#) found that 54% of e-mail traffic is [spam](#), he said.

Maughan's department funds research-and-development products, such as work at [Stanford University](#) to create improved browser plug-ins that help users identify attacks as they surf the Web.

But the problems leading to [security](#) breaches are vast, as the infrastructure of the Internet itself is flawed, Maughan said. He argued that, if there were unlimited resources to tackle the problem, the Internet should be thrown out, so we can "start over and build it right this time."

"In the dot-com and in the dot-net domain alone, domain name queries average about 25 billion queries a day, according to [Verisign](#), yet you as an Internet user have no guarantee that the Web site you're trying to reach will be the one that you get to," Maughan said. "This is a serious Internet infrastructure problem."

Later in the discussion, Maughan said "It's always more difficult to play defense. . . . The systems we've created have many more holes than we have defenses."

All contents copyright 1995-2007 Network World, Inc. <http://www.networkworld.com>

This story appeared on Network World at <http://www.networkworld.com/news/2007/041007-choicepoint-victim-offers.html>