

Data breaches affect million state residents

Credit cards, health records compromised

By Hiawatha Bray

Globe Staff / January 3, 2010

One million Massachusetts residents - or 1 in 6 people - have had their credit card numbers, medical records, or other personal information leaked or stolen over the past two years, according to records provided to the Globe by state officials.

Many thousands of the leaks were first reported between June and November - including confidential data on customers of Blue Cross Blue Shield of Massachusetts, Eastern Bank, JPMorgan Chase Bank, and other major institutions, documents released by state regulators revealed.

The breaches occurred in a variety of forms, including theft of laptop computers and the loss of a computer data tape. But most involved successful hacker attacks on computer centers, where large amounts of personal data are stored.

It is unclear whether any of the incidents of leaked or stolen data resulted in any instances of identity theft. The state's records reflect only that the information was exposed.

Barbara Anthony, undersecretary of consumer affairs and business regulation, said that businesses, schools, and government agencies must cultivate "a culture of security" to protect the millions of sensitive personal documents under their control.

Under a state law passed in 2007, all such institutions must inform consumers and state regulators about security breaches that might result in identity theft. Such leaks involve the release of a person's name along with sensitive information such as Social Security numbers, driver's license numbers, or bank account, credit card, and debit card numbers.

As of November, the state had received 807 data breach notifications from a variety of institutions that collect personal information, from companies to banks and colleges. In most cases, only a few consumers were affected, but in other instances, information on thousands of people was compromised.

"In 60 percent of the cases, the breaches were due to criminal acts," said Anthony. "Forty percent were negligence."

In response to a request from the Globe, Anthony's office provided 13 data breach notifications filed between June and November. The most serious incident occurred in August, when a laptop at the Chicago headquarters at the Blue Cross and Blue Shield Association was stolen. The laptop contained files with the personal information of tens of thousands of doctors and other health care providers nationwide, including 39,000 in Massachusetts. The breach was widely reported in October, when it was disclosed by Blue Cross Blue Shield.

Another major lapse occurred at Network Solutions LLC, a Virginia-based Internet services provider, where an intruder gained access to the company's server computers. Network Solutions estimated that personal information of 14,677 Massachusetts residents was exposed.

Smaller incidents include the theft in October of three laptop computers from the Springfield accounting firm Moriarty & Primack. The computers held personal data from more than 1,600 state residents, including more than 1,100 employees and retirees of Smith College in Northampton, one of the accounting firm's clients.

Another school, the University of Massachusetts at Amherst, reported that a break-in at one of its server computers exposed names and Social Security numbers of "thousands" of former students, though the school did not disclose the exact number.

Eastern Bank Corp. of Lynn disclosed in September that it mailed financial data regarding about 2,500 customers to the wrong addresses. Joe Bartolotta, a spokesman for the bank, said it welcomed the law requiring such disclosures.

"The regulations are a good reminder of what we're in the business to do," he said

On March 1, new state regulations will require organizations to take stronger measures to ensure data security. Institutions that hold such personal data will have to write an official security program and train employees to follow it. In addition, organizations will have to encrypt all personal data stored on laptops, flash drives, or other portable devices, or that is transmitted over the public Internet or wireless networks.

Still, Bartolotta said the Massachusetts law can only go so far in preventing identity theft. He noted that any waiter in a restaurant can easily copy the credit card data of a customer.

"That person has your name, your number, your three-digit security code on back, and before you can get home, could order products online," Bartolotta said. "They could double the amount of regulation and incidents would still occur."

Todd Wallack of the Globe staff contributed to this report. Hiawatha Bray can be reached at bray@globe.com. ■