



Mass. bill wants stores to pay more in data breaches

By Anne Broache

http://news.com.com/Mass.+bill+wants+stores+to+pay+more+in+data+breaches/2100-7348_3-6161536.html

Story last modified Fri Feb 23 01:47:19 PST 2007

Businesses would have to reimburse banks for costs stemming from data security breaches, under a Massachusetts bill that could be mimicked by other states and in Congress.

In what appears to be the first stab at such an approach, the proposal would require any "commercial entity" that handles personal financial data to foot the bill for various banking costs caused by hacks or other intrusions into their systems. The bill, which does not yet have a public hearing date set, is being put forward by Boston-based [Rep. Michael Costello](#), a Democrat in the Massachusetts House of Representatives.

The costs would include any fees associated with canceling or reissuing credit cards, opening and closing bank accounts, and restoring customers' account balances after fraudulent transactions. The bill defines "commercial entity" as including everything from corporations to governmental agencies to associations, whether for-profit or not-for-profit.

The bill's backers say their goal is to urge any business or organization that handles sensitive personal information--whether they be retailer [TJ Maxx](#), the U.S. Department of Veterans Affairs, or the American Red Cross--to place more stringent security controls on their systems.

"Anything that places an incentive on commercial entities to keep that information as secure as possible is a good thing," said Adam Martignetti, Costello's chief of staff. "If that incentive happens to be financial, which it is in the case of our legislation, then perhaps the commercial entities will follow through and will take extra precautionary measures to make sure the information is not lost."

The impact of the proposed policy on consumers is unclear. Federal law already places a \$50 limit on consumers' liability for fraudulent charges on their credit cards, and many major credit card companies boast they will waive that requirement. (The liability limits vary for debit cards, depending on how soon card losses or thefts are reported.)

Advocacy group Consumers Union, for instance, has not taken a position on the "who pays" issue, said Gail Hillebrand, a senior attorney for the organization, but "we want to make sure that it doesn't slow down or stall efforts to require notice of security breaches."

National push next?

Congress may be eyeing similar legislation on a national scale. U.S. House of Representatives Financial Services Committee Chairman Barney Frank (D-Mass.) has said he supports the concept. However, it is unclear what sort of language will end up in a new data-security bill Frank is drafting, said a committee aide who asked not to be named.

A spokesman for Christopher Dodd (D-Conn.), the chairman of the Senate Banking Committee, was less certain where that chamber may be headed. Dodd "intends to work with his colleagues on the committee and in the Senate to further examine current risks to financial data, and also examine what steps Congress can take to better protect the data and consumers," spokesman Marvin Fast said.

Like many [data-security efforts](#) circulated in Congress and state legislatures, the Massachusetts bill proposes a mandatory consumer notification scheme.

Shifting the liability away from banks--a step beyond previous proposals--has been a focus of discussion among advocacy groups for smaller banks. These banks argue that they are absorbing all the costs associated with data leaks, and they're distressed they have to pick up the tab for damage they didn't even create.

The proposed remedy is primarily targeted at retailers, such as [discount retailer TJX Companies](#). These have recently reported breaches potentially affecting thousands of customers, said Steve Kenneally, director of payments and technology policy for

America's Community Bankers, which advocates for smaller banks. ACB, which supports the state bill, would prefer to see national legislation.

"Just because you have fire insurance, doesn't mean you give your three-year-old matches to play with in the basement. And just because the retailers have the banks to be the backstop on these costs to consumers, doesn't mean they don't have a responsibility to protect that data," Kenneally said.

Retail industry representatives dispute the suggestion that they're not paying their fair share. Under their current contracts with major card-issuers like Visa and MasterCard, merchants end up eating many of the costs associated with breaches, they said.

"There seems to be this notion that retailers or breached entities don't pay in these situations, and that's the furthest from the truth," said Elizabeth Oesterle, government relations counsel to the National Retail Federation.

Retailers typically also agree to adhere to security standards through those contracts, so there's no need for legislation as well, said Jim Harper, director of information policy studies at the Cato Institute, a free-market think tank.

"The payment networks or card issuers should condition merchants' use of their systems on agreeing to keep data secure," he said. "Failing to do so, merchants should be liable for cleaning up the mess--by contract."

Now on News.com:

- [Dell's new focus: Don't look back](#)
- [Adobe to bring Photoshop online](#)
- [House panel grills Sirius CEO on XM merger](#)
- [Extra: \\$10 wok works as TV satellite dish](#)
- [Video: 2007 Acura MDX](#)

[Copyright](#) ©1995-2007 CNET Networks, Inc. All rights reserved.