



I NEED...
Fewer Servers

experience IT

What kind of experience are you looking for?
Learn more with our free download:
"Business Strategy for a Successful
Consolidation Implementation"

LOGICALIS

COMPUTERWORLD Security

 Print Article  Close Window

Retailers urge caution in drafting of federal data breach law

Jaikumar Vijayan

June 06, 2007 (Computerworld) The National Retail Federation (NRF) today said that lawmakers considering any federal data-breach law should be careful not to impose the same data security requirements on retailers as they do on financial institutions.

Doing so would put an unnecessary regulatory burden on the entire business community, especially small businesses, Mallory Duncan, the NRF's general counsel, said in testimony before a House Small Business Committee today. The hearing was held to air out small business perspectives on data security.

"We believe it would be an unfair regulatory burden for Congress to require onerous new security standards similar to those found in [the Gramm-Leach-Bliley Act] to be applicable to the entire business community," Duncan said in prepared testimony released today. "This would be particularly burdensome for small businesses, which, if found in violation of such mandated standards, could be subject to a law enforcement action by the Federal Trade Commission," he said. "Instead, we hope that if Congress acts in this area, that they give measured consideration to how it would affect businesses of all types and sizes."

Speaking with *Computerworld* after the hearing, Duncan said that measured steps are needed because the kind of personal data generally held by retailers is very different from the kind of data held by financial institutions. Most retailers and small business typically retain only basic credit card information pertaining to transactions made by a customer. A breach of this type of information usually results only in account fraud that in most cases can be relatively easily remedied, he said.

A financial institution, on the other hand, holds much more sensitive data -- including Social Security numbers -- which, if breached, could result in ID theft, he said.

"There's a big difference between ID theft and credit card fraud. This is a very complicated issue. Rather than scatter-shooting hopeful solutions," it's important to draft a federal bill that matches the scope of the issue, Duncan said. Any legislation on data security should take into account the differences in the type of data held by retailers and financial companies, he said.

Duncan's testimony came even as credit unions are intensifying their [efforts to get retailers to take](#)

Learn how to increase sales
with Extended Validation SSL
Certificates from VeriSign.



[financial responsibility](#) for data breaches in the wake of the [massive data compromise](#) at The TJX Companies Inc. earlier this year.

In testimony today before same subcommittee, the National Association of Federal Credit Unions (NAFCU) called for a federal law that would hold retailers and others accepting payment cards accountable for the costs associated with a data breach.

"It is not our intent to have data breaches put any company out of business," said John Milazzo, chairman of the NAFCU in prepared testimony released today. "Instead, we believe that there must be a strong incentive for businesses to properly protect consumer's financial data. Otherwise, as evidenced by recent instances of payment card breaches, the information may not be adequately protected and the credit union could end up being the one that pays."

The NAFCU's testimony builds on other attempts by credit unions to drum up support for laws holding retailers financially responsible for data breaches. One example is the Plastic Card Security Act that was signed into law in Minnesota last month with the active support pushed of the Minnesota Credit Union Network. Another example is a bill being sponsored by California Credit Union League that is similar to the Minnesota bill.