



Credit Union National Association

CUNA Issue Summary

DATA SECURITY

ISSUE: There have been increasing problems over the theft of sensitive information resulting from data security breaches. The frequency of major credit data compromises continue at an alarming rate, resulting in severe consequences on American consumers, credit union members and the financial institutions that issue credit and debit cards – particularly credit unions and small banks.

CUNA POSITION: CUNA supports legislation that would incorporate the following principles:

Consumer Notice -- Data security breaches have negatively impacted credit unions, exposing their members and consumers to identity theft and fraud. Without being able to disclose the source of the breach, credit unions are exposed to “reputation risk” – the loss of confidence in the credit union by the members, in addition to actual monetary costs. CUNA would like to see initiatives pursued that would require the major credit card companies to notify financial institutions when a breach has occurred, and for financial institutions to be able to disclose the source of the breach to the consumer.

Reimbursement -- CUNA supports the requirement that the breaching party (i.e., the merchant) reimburse the consumer or financial institution for any losses incurred. Contracts undoubtedly cannot adequately resolve this problem because the credit union or another financial institution typically will not have a contractual agreement directly with a merchant or other data collector responsible for a particular data breach.

Preemption of State Laws (National Standard) -- CUNA supports uniform, national standards to impose data security safeguards and notification requirements on a wide range of entities engaged in the business of collecting or handling sensitive personal financial information.

Regulatory Burden -- Since credit unions and other regulated financial institutions are not the problem, CUNA urges that new data protection legislation does not impose additional, unnecessary regulatory burdens on financial institutions already subject to the Gramm-Leach-Bliley Act (GLBA) requirements. CUNA would support amending the GLBA to broaden its coverage.

Safe Harbor -- CUNA supports the inclusion of a safe harbor provision which would allow credit unions and other financial institutions to reasonably conclude that the misuse of the illegally acquired information is unlikely to occur when the information has been encrypted.

Data Destruction -- CUNA supports efforts to require merchants to comply with existing regulations on data destruction, ensuring that no merchant or its agent accepting a credit or debit card in connection with a transaction, or processing the information, shall retain personal data from that credit or debit card.

STATUS/OUTLOOK: On June 3, 2009, H.R. 2221, the *Data Accountability and Trust Act*, passed the House Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection. The bill would require businesses to notify affected customers when outside parties gain access to sensitive information due to a security breach. Although it supports the goal of granting greater information to consumers whose personal information has been compromised by security breaches, CUNA wrote a [letter](#) to Committee members with suggestions to improve the bill (some of which were adopted by the Committee).

While most businesses lack the contact information needed to alert their customers, financial institutions normally have the means to directly communicate with their account holders. While any notification of data breach victims should be done by the financial institutions, the cost of this notification should be covered by the entity that compromised the data. Financial institutions should also be allowed to disclose the source of the information leak to their cardholders to avoid any harm that could be done to their reputation, CUNA stated in the letter.

The amended bill also excludes federally insured credit unions from Federal Trade Commission (FTC) oversight of their security risk mitigation procedures as the amended version excludes businesses following standard security precautions of equal or greater quality to those set out by the bill.

No date has been set for the full Energy and Commerce Committee to consider this legislation.

CONTACT: [John Hildreth](#), (202) 508-6724, jhildreth@cuna.coop

RELATED DOCUMENTS:

[June 3, 2009: Letter from CUNA President and CEO Dan Mica to House Energy and Commerce Subcommittee on Commerce, Trade and Consumer Protection Chairman Bobby Rush \(D-IL\) and Ranking Member George Radanovich \(R-CA\) regarding H.R. 2221, the Data Accountability and Trust Act](#)

[March 1, 2006: Letter from CUNA President and CEO Dan Mica to House Committee on Financial Services Chairman Mike Oxley \(R-OH\) and Ranking Member Barney Frank \(D-MA\) Regarding Data Security](#)

[February 3, 2006: Letter from CUNA President and CEO Dan Mica to House Committee on Financial Services Regarding H.R. 3997, the Financial Data Protection Act of 2005](#)

[April 4, 2005: Testimony of Eugene Foley on behalf of Harvard University Employees Credit Union to the House Financial Institutions and Consumer Credit Subcommittee Hearing on "Assessing Data Security"](#)

LAST UPDATED: June 19, 2009

Copyright © 2009 - Credit Union National Association, Inc.