Stop Merchant Data Breaches

Quick Look:

- **Major merchant data breaches expose credit unions to significant monetary costs and reputational risk.**
    - In the wake of a data breach, credit unions cover the cost not only of fraud, but also of blocking transactions, reissuing cards, increasing staffing at call centers and monitoring consumer accounts.

Action:

- Support S. 961, the Data Security Act of 2015
    - Lead Sponsors: Sen. Carper (D-DE) and Sen. Blunt (R-MO)
- Credit unions urge Congress to pass legislation which includes the following principles:
    1. Strong national data protection and consumer notification standards with effective enforcement provisions must be part of any comprehensive data security regime, applicable to any party with access to important consumer financial information.
    2. Recognition of the robust data protection and notification standards which banks and credit unions are already subject to under section V of the Gramm-Leach-Bliley Act.
    3. Preemption of inconsistent state laws and regulations in favor of strong Federal data protection and notification standards.
    4. The ability for banks and credit unions to inform customers and members about information regarding a breach, including where it occurred.
    5. Shared responsibility for all those involved in the payments system for protecting consumer data. Too often, banks and credit unions bear a disproportionate burden in covering the costs of breaches occurring beyond their premises. Therefore, the costs of a data breach should ultimately be borne by the entity that incurs the breach.

Background:

- Retailers that accept electronic payments do not face the same strict data security standards that financial institutions are subject to under the Gramm Leach Bliley Act (GLBA). Millions of American consumers' personal financial information has been compromised as a result of merchant data breaches in recent years, demonstrating the need for retailers to live under Federal standards similar to GLBA.
    - In fact, the Identity Theft Resource Center has compiled a list of all publicly reported breaches in the United States and shows that banks accounted for only 5.5 percent of all breaches in 2014. Other businesses accounted for 33 percent.
    - As a result of the number of breaches occurring at retailers, credit unions are increasingly responsible for protecting consumer financial safety and are reporting significant costs as a result:
        - According to a survey of CUNA members, estimates of the Target data breach put credit union costs at approximately $5.68 per affected card by the security lapse. This equals, at a minimum, a total cost of $30.6 million for credit unions alone. Over one year after the breach, credit unions have not been reimbursed for a dime.
        - Another CUNA survey found that the Home Depot data breach cost credit unions nearly $60 million, a figure that represents 7.2 million compromised credit union member cards.
    - Retailers have hailed Euro Master Visa (EMV or chip and pin) cards as a fix to make the system safer, but it is not a panacea. Congress should not prescribe a static technology that will become easily outdated. Instead Congress must ensure all of those who participate in the payments system are held to the same standards to protect consumer data.