Stopping Merchant Data Breaches

Retailers 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.

Major merchant data breaches expose credit unions to significant monetary costs and reputational risk. Credit unions cover the costs of fraud, blocking transactions, reissuing cards, increasing staffing at call centers and monitoring consumer accounts.

S. 961/H.R. 2205 provides:

- Strong national data protection and consumer notification standards with effective enforcement provisions.
- Recognition of robust data protection and notification standards that credit unions and banks are already subject to.
- Preemption of inconsistent state laws and regulations in favor of strong Federal data protection and notification standards.
- Ability for credit unions and banks to inform customers and members about a breach, including where it occurred.
- Shared responsibility for all those involved in the payments system for protecting consumer data. The costs of a data breach should ultimately be borne by the entity that incurs the breach.

Ensure that merchants that accept cards for payment are held to the same data security standards as the credit unions and banks that issue the cards:

Support S. 961/H.R. 2205, the Data Security Act of 2015