MCUL & Affiliates Governmental Affairs

Data Breach Liability

2014

Federal Issue Brief

Background

At the close of 2013, several major national retailers reported large data breach events. The national retailer Target was compromised during the peak of the holiday shopping season, and nearly 70 million consumers lost either card or personal identifying information as part of the event. By early 2014, stolen information from this event began turning up on the "black market" and in related arrests for fraud. Following the Target event, significant breaches were reported at Neiman Marcus and Michaels.

Despite standards held up by the retail industry as protections for consumer data, industry self-policing and enforcement of such is inadequate and often retroactive. It is the financial institution supporting the breached card, and not the retailer, that is often "left holding the bag" for the initial costs related to card replacement (including analysis and member communication) and the later cost of fraud itself. While retailers certainly endure risk to their reputation, as well as investigations and possible fines, the true cost of these crimes is born by financial institutions and their insurers that have little to no control over the actions, preparation, and protections utilized by the retailer.

Effect

- With regard to recent breach events, early estimates conclude that each potentially affected card costs credit unions $6.38. This includes costs associated with member service, increased call volume, and card replacement – it does not include the cost of actual fraud.
- Initial damage estimates for credit unions total $30.6 million nationally, and growing. In Michigan, credit unions have reported $1.6 million in damage so far.
- During passage of the Dodd-Frank Act, the "Durbin Amendment" shifted billions in interchange income to retailers, with no corresponding price-relief or consumer benefit resulting. However, financial institutions still bear the brunt of the risk and the cost for a retailer's lack of preparation and failure to adequately store and protect consumer data. This liability dynamic represents an arbitrary windfall that does nothing to encourage real reform or consumer protection, and cuts at financial institutions particularly hard – lost revenue, and lost wherewithal to pay for the sins of the retail community.
- It is time to restore shared accountability for consumer and data protection, by increasing standards and holding retailers accountable.

Status/MCUL Position

S. 1976 has been introduced by Sen. John D. Rockefeller IV (D-West Virginia) to create the **Data Security and Breach Notification Act of 2014**, referred to the Senate Committee on Commerce, Science and Transportation.

S. 1927 has been introduced by Sens. Thomas Carper (D-Delaware) and Roy Blunt (R-Missouri) to create the **Data Security Act of 2014**, and establish a national standard for data breach notifications, to replace the patchwork of state laws. The Senate Committee on Banking, Housing, and Urban Affairs Committee has held one hearing on the measure.

S. 1897 has been introduced by Sen. Patrick Leahy (D-Vermont) to create the **Personal Data Privacy and Security Act of 2014**, referred to the Senate Committee on Judiciary.

S. 1193 has been introduced by Sen. Pat Toomey (R-Pennsylvania) to create the **Data Security and Breach Notification Act of 2013**, referred to the Senate Committee on Commerce, Science and Transportation.

Consumer protections must be enhanced and retailer accountability increased for data security. There must also be recourse for affected consumers and financial institutions. Financial institutions should be allowed to disclose where a breach occurred, and retailers should have parallel security requirements with regard to privacy and payment products. Finally, the FTC and appropriate agencies should have adequate enforcement and civil penalty tools, so as to effectively and more efficiently enforce standards.