MINTZ

The Target Breach Update

March 27, 2014 | Blog | By **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

It has been difficult to keep up with all the various permutations of the Target data breach saga.

Yesterday, the finger-pointing continued in the form of the release of a Harris Poll and testimony on Capitol Hill at a U.S. Senate hearing. First, the Harris Poll. It should come as no surprise to anyone, even Target, that shoppers blame any retailer for a data breach once the shopper is aware of it. According to a study conducted for big data analytics company Feedzai:

> **Who's to blame? Among U.S. adults who are aware of any data breaches, 60% believe merchants are responsible for preventing future incidents, while 13% believe responsibility falls on banks.**
>
> **Getting the flu is not as bad as having a credit card stolen. According to the survey, it seems many consumers find getting their credit or debit card stolen more aggravating than a number unpleasant activities, and in fact 43% of U.S. adults feel that nothing is more aggravating than theft. Survey says:**
>
> - **20% of Americans think losing their cell phone is more aggravating than card/debit card data theft; in the Northeast that figure drops to 15%, and it jumps to 30% among females age 18-34**
> - **20% feel getting the flu is more aggravating, which jumps to 25% for Americans age 35-44**
> - **14% of Americans find being stuck in rush hour traffic more aggravating**
> - **13% of Americans found going to the DMV more aggravating, while 12% say serving on jury duty and 11% thought preparing income tax returns was more aggravating than credit/debit card data theft**

For more on the Feedzai study - read **here**.

And while consumers were blaming retailers, Congress was also blaming retailers. Capitol Hill was buzzing all things cyber yesterday. There were two hearings yesterday that examined cybersecurity and data breach issues.

The Senate Commerce Committee held a hearing on ***Protecting Personal Consumer Information from Cyber Attacks and Data Breaches***. Chairman Rockefeller expressed his frustration with industry's failure to compromise on the establishment of data security standards. Just ahead of the the hearing, Committee staff released a **scathing report** suggesting that Target missed a number of opportunities to prevent the breach. The report states: "This analysis suggests that Target missed a number of opportunities along the kill chain to stop the attackers and prevent the massive data breach." Ranking Member Thune said that he supports a federal breach notification standard and wants to ensure that businesses have the tools they need to secure their networks through information-sharing and liability protections. When asked what kind of legislation the FTC would support, Chairwoman Ramirez said there should be federal data protection standards, civil penalties for inadequate security, and a uniform breach notification system. In addition, the witnesses discussed new credit card technologies, universal agreement on a uniform breach notification mandate, and possible federal security standards for the private sector. Target's CFO, John Mulligan, **appeared before the Committee** for the second time.

The Senate Homeland Security and Government Affairs Committee held a hearing on ***Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure***. The Committee met yesterday to determine the progress of implementing the President's cybersecurity executive order. Chairman Carper, Ranking Member Coburn, Under Secretary Schneck, Ms. Starkey and

Ms. Dodson all discussed the readiness of the cybersecurity workforce. Discussion specifically revolved around the federal cooperation with universities to create better education. Senators Johnson and McCain focused their questions on liability waivers to encourage information sharing between companies and the government. Ranking Member Coburn and Mr. Chabinsky advocated closer attention to deterrence of threats and less focus on mitigation.

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.