Published on *The National Law Review* https://natlawreview.com

Privacy Law Monday – August 18, 2014

Article By:

Cynthia J. Larose

There is another retail data breach to talk about in this Privacy Monday post – privacy & security bits and bytes to start your week.

Supermarket Chain Reports Data Breach

Minnesota-based food retailer Supervalu Inc. has reported breach of its point-of-sale (POS) system, apparently by hackers. A press release on the corporate website describes the incident as a "criminal intrusion" and says that it "may have" resulted in the theft of credit or debit card numbers. According to Supervalu, there is no evidence that data were stolen, and it has not had any reports of misuse of any such data. Affected stores are reported by the company to be operated under the **Cub Foods, Farm Fresh, Hornbacher's Shop 'n Save and Shoppers Food & Pharmacy** banners as well as other stand-alone liquor stores and franchised stores. The complete list is at the company's Consumer Security Advisory on its website.

In addition to the Supervalu stores, Supervalu maintains IT systems for a number of other regional market chains owned by AB Acquisition LLC, bought from Supervalu last year. According to a press release issued by AB Acquisition, those systems were also believed to have been breached.

Third-Party Guidance for Merchants – Payment Card Industry Security Standards Council

The organization known as the PCI-DSS Council has released a useful guidance document for merchants accepting credit cards. The spate of data breaches is not the only reason that merchants should be paying attention to the guidance and reviewing it with care. The other reason is liability: when a merchant signs an agreement with a payment card processor (a "merchant agreement"), that merchant enters into a contract that includes an agreement to comply with the PCI-DSS rules. All of them.

Most often small and medium-sized enterprises outsource the payment card processing functions to a service provider, thus taking credit card collection out of their hands and keeping the cardholder data out of their systems. But, also most often, these businesses are the "merchant of record" with no diligence on that service provider. The latest PCI-DSS guidance document provides recommendations on how to implement a third-party review program to meet due diligence

requirements that are a part of PCI DSS (see Requirement 12.8).

Remember – all businesses that handle payment card data (whether directly or through third parties) must become PCI DSS 3.0 compliant by December 31, 2014.

Aol Will Not Honor Do-Not-Track Requests

Joining Yahoo, Aol issued a revised privacy policy last week (effective September 15) that inserted new language relating to so-called “do-not-track” signals. “There is no standard that governs what, if anything, websites should do when they receive these signals. AOL currently does not take action in response to these signals. If and when a standard for responding is established, we may revisit the policy on responding to these signals.”

California’s amendment to its Online Privacy Protection Act (described here) requires operators of commercial websites and online services that collect personal information to disclose whether they honor “do-not-track” signals.

Back in 2007, Aol was one of the first to let users opt out of online cookie-based advertising.

National Law Review, Volume IV, Number 230