MINTZ

Privacy Monday - May 12, 2014

May 12, 2014 | Blog | By **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

Another busy week in the privacy/security world. We have some bits and bytes to start your week:

Verizon 2014 Data Breach Investigation Report - Something Old, Something New

Verizon is out with its 2014 edition of the comprehensive Data Breach Investigation Report (DBIR). You can get your copy **here** for your reading pleasure -- or heartburn. Retailers should take particular note of this report. "(2013) may be tagged as the 'year of the retailer breach,' but a more comprehensive assessment of the InfoSec risk environment shows it was a year of transition from geopolitical attacks to **large-scale attacks on payment card systems**," according to the report. Random-access memory (RAM)scraping -- a technique that was thought to be past its sell-by date -- appears to have increased with alarming intensity. Retail point-of-sale (POS) systems can be thwarted by weak or nonexistent passwords, allowing criminals to insert malware that will sit on a POS and collect card numbers. The bad guys grab the numbers from the RAM and dump them into a file then return and pick them up at a later date. New **PCI DSS rules** take effect in July that will shift the liability from banks and card issuers to the retailers. Time to review the security of your systems.

State Legislation Roundup

We recently updated **our Mintz Matrix** to include Kentucky as the 47th state to enact a data breach notification law, and to account for Iowa's amendment requiring notice to the state's Attorney General. We will likely need to make further updates as the state legislative calendars wind on. Minnesota is debating expansive amendments to its data breach notification law, described in our post **here**. A very expansive amendment to Florida's data breach notification law is sitting on the Governor's desk awaiting signature. SB 1524, the ***Florida Information Act,*** will repeal the existing data breach notification law and replace it with a law that expands the definition of personal information (to include medical information, health insurance information, user names and e-mail addresses), reducing the notification period from 45 days to 30 days, additionally requires notification to the Attorney General's office, and clarifies that if a vendor notifies individuals on a company's behalf, the company is deemed to have violated the law where the vendor fails to provide proper notice. The Act adds civil penalties for violations not exceeding $500,000: $1,000 for each day up to the first 30 days and $50,000 for each subsequent 30-day period up to 180 days. If the violation continues more than 180 days, the penalty shall not exceed $500,000. In the absence of Congressional action after the 2013 Target, Michaels, Neiman Marcus, et al, breaches -- the states are continuing to lead the way.

Canadian Anti-Spam Law (CASL) Compliance Deadline is Approaching

At last week's IAPP Canada Privacy Symposium, Canadian regulators held a jam-packed session on the **new anti-spam legislation** coming north of the border on July 1. The **basic message** was: this our last warning, and the compliance onus is on you. Warning to US marketers -- CASL applies to **any commercial email message** sent to a Canadian email address. It need not be "spam." If you are not preparing your compliance program and sorting your mailing lists, there is a maximum penalty of $10 million waiting.

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.