The Year of the Breach: California Attorney General Releases 2013 Data Breach Report

October 30, 2014

On Tuesday, the California Attorney General released the second annual data breach report, summarizing the 167 data breaches reported to the Attorney General's office in 2013, and providing privacy and security recommendations for businesses. According to the report, the retail, finance, and healthcare industries reported over 60 percent of the 167 breaches, over half of which were the result of malware and hacking. The breaches affected 18.5 million California residents – a 600 percent increase over the 2.5 million records breached in 2012, and 84 percent of those records were the result of retail industry breaches.

The report provides several recommendations for businesses directed towards improving security and notification measures, including the following three non-sector-specific recommendations: (1) conduct risk assessments at least annually and update privacy and security practices based on the findings; (2) use strong encryption to protect personal information in transit; and (3) improve the readability of breach notices. Additionally, the report recommends that the healthcare industry consistently use strong encryption to protect medical information on laptops and other portable devices, and consider it for desktop computers. Importantly, the report also includes the following six recommendations specific to the retail industry, suggesting that the Attorney General considers the security measures and breach response actions of the retail industry, to date, inadequate:

1. Update point-of-sale terminals so that they are chip-enabled and install the software necessary to operate this technology.

2. Implement appropriate encryption solutions to devalue payment card data, including encrypting data from the point of capture until the completion of transaction authorization.

3. Implement appropriate tokenization solutions to devalue payment card data, including in online and mobile transactions.

4. Respond promptly to data breaches and notify affected individuals in the most expedient time possible and without unreasonable delay.

5. Improve substitute notice, such as by placing a prominent and conspicuous link to the notice on the website homepage, leaving the link and notice up for at least 30 days, publishing the notice in the most expedient time possible and updating it as the business learns more, and telling consumers what they can do to protect themselves.

6. Work with financial institutions to protect debit card holders in breaches of unencrypted payment card data.

Finally, the report suggests that the state consider legislation (1) to amend the breach notification statute to strengthen the substitute notice procedure, clarify the roles and responsibilities of data owners and maintainers, and require a final breach report to the Attorney General; and (2) to provide funding to support system upgrades for small California retailers. As it appears no longer a question of “if” but rather “when” a breach will occur, businesses should continue to evaluate and modify their privacy and security practices to ensure compliance with these recommendations and all legal obligations.