ECKERT SEAMANS
ATTORNEYS AT LAW

MARCH 2014

PRIVACY ALERT – DATA BREACH AND HIPAA UPDATES

SENATE COMMITTEE REPORT REVEALS THAT TARGET FAILED TO RESPOND TO EARLY WARNINGS

A March 26, 2014 report of the U.S. Senate's Committee on Commerce, Science and Transportation indicates that U.S. retail giant Target failed to take action in response to early warnings that attackers were intruding into Target's computerized systems and preparing to steal credit and debit card data. Over 40 million credit and debit card accounts were compromised as a result of the December 2013 cyber attack.

A key finding of the Senate Report is that Target appears to have failed to respond to multiple automated warnings from the company's anti-intrusion software that the attackers were installing malware on Target's system as well as warnings from the company's anti-intrusion software regarding the escape routes the attackers planned to use to exfiltrate data from Target's network. It is not clear why Target did not take action in response to these warnings.

Significantly, the Senate Report observes that in September of 2013, Target's payment card systems were certified as being compliant with Payment Card Industry Data Security Standards ("PCI-DSS"), but that despite meeting this industry security standard, hackers were able to circumvent Target's security and remove credit and debit card data from Target's system.

The clear message of the Senate Report is that companies that receive and maintain personal information (including credit/debit card data, social security number and bank account information, among other things), must not ignore early warning signs of a possible breach. Such companies must have adequate anti-intrusion software in place and must monitor and promptly respond to warnings of possible attacks generated by that software.

OCR PLANS ANOTHER ROUND OF HIPAA AUDITS

The Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services has announced that it will be sending surveys to approximately 800 covered entities and 400 business associates in preparation for a new round of HIPAA audits. This will be the first time that the OCR will audit business associates for HIPAA compliance. In the past OCR outsourced HIPAA audits to a third party but indicated that it will conduct the new round of audits on its own. Under HITECH regulations, OCR is required to conduct periodic audits. When an audit reveals significant noncompliance, the agency may open a separate investigation.

One of the items of top concern appears to be completion of a security risk assessment. OCR has discovered that many covered entities have not conducted the assessment which is mandated under HIPAA's security rules.

In addition to audits, OCR may investigate a covered entity or business associate based on a compliant or a breach of unsecured protected health information which is reported to the agency as required by HIPAA. Major breaches that affect 500 or more individuals have a significant chance of triggering such an investigation.

---

*This **Privacy Alert** is intended to keep readers current on developments in the data security & privacy world and in the law, and is not intended to be legal advice. If you have any questions, contact **Sandy B. Garfinkel**, Chair of the firm's Data Security & Privacy Group, at 412.566.6868, or sgarfinkel@eckertseamans.com or **Sandra Mihok,** Chair of Eckert Seamans' HIPAA Privacy Group, at 412.566.1903 or smihok@eckertseamans.com.*