Fallout from Target's 2013 Data Breach includes an $18 Million Multistate AG Settlement

Alyssa Z. Hutnik

May 25, 2017

Target Corporation agreed to an $18.5 million settlement with 46 State Attorneys General and the Attorney General of the District of Columbia this week, resolving allegations that the company failed to provide reasonable data security to its customers, as demonstrated by the Target's 2013 holiday data breach that affected more than 60 million customers.

Background. In November 2013, hackers accessed Target's customer service database using legitimate credentials stolen from a third-party vendor. The breach affected the personal information of over 60 million customers and the payment card accounts of over 41 million customers. The information accessed included full names, telephone numbers, email and mailing addresses, payment card numbers, expiration dates, card-validation value codes, and encrypted debit PINs.

Settlement Terms. The conditions of the settlement agreement, some of which will be effective for a five (5) year period, require Target to:

- **Implement a comprehensive information security program**. Target must develop, implement, and maintain a comprehensive information security program and employ an executive for that purpose that will advise Target's CEO and Board of Directors.
- **Encrypt and protect Cardholder data**. Target must maintain encryption protocols and policies, and comply with the Payment Card Industry Data Security Standard.
- **Implement other technological safeguard measures.** Target must implement specific safeguards including: implementing reasonable access restricting mechanisms and appropriate systems to collect logs and monitor network activity; managing and documenting changes to network systems; adopting improved industry-accepted payment card security technologies and; using encryption or similar masking techniques to devalue payment card information.

The $18.5 million settlement is the largest multistate data breach settlement to date and yet another multistate settlement concerning a breach more than three years old. Companies can review FTC guidance on protecting personal information, as well as the California Data Breach Report, and this settlement for general guidance on legal expectations to protect customer financial and personal information and the potential fallout for failing to do so.