Brian E. Frosh
Attorney General

Media Contacts:
Press@oag.state.md.us
410-576-7009

PRESS RELEASE

Attorney General Frosh Announces $17.5 Million Multistate Settlement with Home Depot Over 2014 Data Breach

BALTIMORE MD (November 24, 2020) – Maryland Attorney General Brian E. Frosh today announced a multistate settlement with the Georgia-based retailer The Home Depot stemming from its 2014 data breach, which exposed the payment card information of approximately 40 million consumers nationwide. Through the $17.5 million-dollar settlement, The Home Depot has reached a resolution with 46 states and the District of Columbia. The Home Depot has also agreed to a series of data security and good governance provisions designed to safeguard the personal information of consumers.

The breach occurred when hackers gained access to The Home Depot's network and deployed malware on The Home Depot's self-checkout point-of-sale system. The malware allowed the hackers to obtain the payment card information of customers who used self-checkout lanes at The Home Depot stores throughout the United States between April 10, 2014, and September 13, 2014.

"Far too often, companies fail to protect consumers' personal information from unlawful use or disclosure," said Attorney General Frosh. "As a result, consumers suffer harm personally and financially. The data security measures required by this settlement will help protect the personal information of Marylanders and other consumers throughout the country."

Under the settlement, The Home Depot has agreed to a series of provisions designed to strengthen its security practices. These include:

- Employing a duly qualified Chief Information Security Officer reporting to both the Senior or C-level executives and Board of Directors regarding The Home Depot's security posture and security risks;
- Providing the resources necessary to fully implement the company's information security program;
- Providing appropriate security awareness and privacy training to all personnel who have access to the company's network or responsibility for U.S. consumers' personal information;
- Employing specific security safeguards with respect to logging and monitoring, access controls, password management, two-factor authentication, file integrity monitoring, firewalls, encryption, risk assessments, penetration testing, intrusion detection, and vendor account management; and

- Consistent with previous state data breach settlements, the company will undergo a post-settlement information security assessment that will evaluate its implementation of the agreed upon information security program.

In addition to Maryland, the states participating in this settlement include Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, the District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, and Wisconsin.