WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

Target Data Breach AG Settlement Establishes "New Industry Standards" for Collecting and Protecting Consumer Data

May 25, 2017

AUTHORS

Elizabeth J. Bower | **Daniel K. Alvarez** | **James C. Dugan**

Target Corporation, the second-largest discount retailer in the United States, agreed to an $18.5 million settlement yesterday to resolve an investigation by 47 state attorneys general ("AGs") into the company's 2013 data breach. The states' investigation revealed that the breach "affected more than 41 million customer payment card accounts and contact information for more than 60 million customers." Hackers obtained such extensive access to Target's information systems using only the stolen credentials of a third-party HVAC vendor.

Target's settlement with the states calls for it to implement and maintain a cybersecurity compliance structure that the AGs are touting as "industry standards." The "industry" includes all companies that process payment cards and store customers' personal information. The "standards" require:

- **Comprehensive Information Security Program**: Target must implement within 180 days a comprehensive information security program that is "reasonably designed to protect the security, integrity, and confidentiality" of personal information it collects from consumers. The written program must consist of safeguards consistent with Target's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information it maintains. Target may satisfy this requirement by reviewing and updating an existing cybersecurity program.

- **Ensure Vendor Compliance**: Target must develop and implement risk-based policies and procedures for auditing vendor compliance with its comprehensive security program.
- **Responsible Executive or Officer**: Target must employ "an executive or officer with appropriate background or experience in information security" to implement and maintain its comprehensive information security program. Target's designated executive or officer must advise the Chief Executive Officer and Board of Directors on Target's information security posture and the security implications of its decisions.[1]
- **Segmented Cardholder Data Environment**:[2] Target must scan and map connections to its Cardholder Data Environment and segment that environment from the rest of its computer network. Target must also implement a risk-based penetration testing program to identify vulnerabilities in its network, and must take steps to separate its production and development environments.
- **Access Controls and Management**: Target must implement risk-based access controls appropriate to Target's business and environment. These controls must manage access to individual accounts, service accounts, and vendor accounts, and must incorporate strong passwords, password-rotation policies, and two-factor authentication. Target must also restrict or disable any network program that provides access to the Cardholder Data Environment or the compromise of which Target believes would affect the security of the Cardholder Data Environment.
- **Payment Card Security**: Target is required to (i) comply with the Payment Card Industry Data Security Standard ("PCI DSS"), (ii) reasonably review and implement improved industry-accepted payment card security technologies appropriate to Target's business and technology environment, and (iii) take measures to protect payment card information, including by encrypting payment card information at the point of sale.
- **Third-Party Security Assessments:** Target must obtain within one year of the settlement agreement an assessment from an independent third-party professional concerning the appropriateness of safeguards in its comprehensive security program and its implementation of those safeguards.
- **Data Security Software**: Target must deploy and maintain data security software on its network, including (i) a file monitoring solution, (ii) an application whitelisting solution,[3] (iii) access restricting mechanisms, such as firewalls, and (iv) a security information and event management tool for logging and monitoring events.

---

1 The settlement agreement does not address whether Target's existing designated Chief Information Security Officer satisfies this requirement.

2 The settlement defines "Cardholder Data Environment" as "technologies that store, process, or transmit payment card authentication data, consistent with the Payment Card Industry Data Security Standard ('PCI DSS')."

3 The National Institute of Standards and Technology ("NIST") defines an "**application whitelist**" as "a list of applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on a host according to a well-defined baseline."

- **Encryption Policies**: Target must maintain and implement data encryption policies and procedures concerning the encryption of individuals' (i) Social Security numbers, (ii) driver's license numbers, (iii) state-issued identification card numbers, and (iv) financial account numbers and credit or debit card numbers, in combination with any codes or passwords that would provide access to financial accounts. Target's encryption policies must apply to data stored on desktops that process cardholder data, laptops and other portable devices, and any data that is transmitted wirelessly or across public networks.
- **Change Control Policies**: Target must develop and maintain policies and procedures concerning changes to network systems.

While many companies that process payment cards will have already implemented many of these policies and practices in connection with a PCI DSS compliance program or internal cybersecurity program, the Target settlement puts all companies on notice that these are the standards expected by at least 47 AGs. Failure to implement these standards proactively may therefore put companies at risk of costly enforcement actions when a data breach occurs.

If you have any questions regarding this memorandum, please contact Elizabeth J. Bower (202-303-1252, ebower@willkie.com), Daniel K. Alvarez (202-303-1125, dalvarez@willkie.com), James C. Dugan (212-728-8654, jdugan@willkie.com) or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

May 25, 2017

"**Whitelisting**" is the practice of using technologies to control which applications are "permitted to be installed or executed" on a system. *See* NIST Special Publication 800-167 (Oct. 2015).