Client Update
Information Security Programs Play a Central Role in Target Data Breach Settlement

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Stephanie M. Cipolla
smcipolla@debevoise.com

WASHINGTON, D.C.
Luke Dembosky
ldembosky@debevoise.com

On May 23, 2017, Target Corporation ("Target") reached an $18.5 million settlement with the Attorneys General ("AGs") of 47 states and the District of Columbia. The agreement resolves the states' investigation into Target's 2013 data breach and is the largest ever multistate data breach settlement with regulators.

THE BREACH

In 2013, cyber criminals obtained network credentials from one of Target's third-party vendors and used the credentials to exploit weaknesses in Target's point-of-sale systems. The breach affected more than 41 million customer payment cards and exposed the contact information of over 60 million customers.

Prior to this settlement, Target had settled with a class of banks for more than $59 million in a final and approved settlement. Target had also reached a $10 million settlement with a consumer class impacted by the breach, but the 8th Circuit reversed the settlement, remanding to the District Court for consideration of class certification issues.

THE SETTLEMENT TERMS

Besides requiring Target to pay $18.5 million to the states, the settlement agreement requires Target to implement technical, administrative, and physical safeguards commensurate with the size of Target's technical infrastructure, types of personal information maintained, and nature of its business. Key provisions require that Target:

- encrypt cardholder and personal information;
- segment payment card data information from the rest of the computer network;

- implement greater controls over who can access its network, including requiring two-factor authentication for some accounts and mandating password rotation;
- develop a risk-based penetration testing program;
- employ a Chief Information Security Officer (CISO), who is responsible for reporting to and advising the corporation's CEO and Board of Directors on the corporation's security risks; and
- obtain an independent, third-party assessment of Target's information security program within one year of the settlement agreement.

Although the AG settlement mirrors the consumer settlement in many ways (e.g., in requiring the hiring of a CISO, implementation of a written information security program, monitoring of information security events, and provision of security training to employees), the AG settlement is notable for the granularity of its technical requirements including:

- encryption;
- multi-factor authentication;
- whitelisting;
- network access controls;
- active log monitoring;
- segmentation of production and development environments; and
- enhanced access control measures for service, vendor, and administrator accounts.

LEARNING FROM TARGET'S SETTLEMENT

Companies should take note of the level of technical specificity in the settlement, as it may help define what AGs consider the appropriate baseline security protocols that companies should employ. In fact, in announcing the settlement, Illinois Attorney General Lisa Madigan stated that it "establishes industry standards for companies that process payment cards and maintain secure information about their customers."

The settlement stresses the need for an information security plan that fits the actual risks of the entity and its customers. This risk-based approach will be familiar from the NIST Cybersecurity Framework (among other standards),

which continues to emerge as a *de facto* gold standard for cybersecurity assessments.

The settlement suggests entities:

- Conduct cybersecurity risk assessments.
- Implement a comprehensive information security program and incident response plan ("IRP").
- Stress test the information security program and IRP to ensure the policies and procedures are reasonable and appropriate given the entity's size, nature, and sensitivity of personal information maintained through, for instance, regular tabletop exercises.

These steps may help entities bolster their argument that they took reasonable measures to protect consumers' personal information, mitigating risk both by reducing the likelihood of a successful attack, and by positioning the company to succeed in regulatory investigations and private litigation.[1]

* * *

Please do not hesitate to call on any member of the Debevoise Cybersecurity & Data Privacy global practice team with questions or for assistance. Learn more about our practice at debevoisedata.com.

[1] The authors would like to thank HJ Brehmer, a Summer Associate at Debevoise & Plimpton, for her assistance and contributions to this client update.