Target Corp. Cyber Breach Settlement Reflects Emerging Best Practices for Cybersecurity

May 30, 2017

Last week, Target Corp. reached a record $18.5 million settlement with 47 states and the District of Columbia to end investigations into Target's data breach in 2013. The settlement highlights the growing list of specific measures that companies are expected to have in place to mitigate the risk of cyber breaches.

In 2015, Target reached a class action settlement with consumers that required the company to implement certain measures to protect customer information. In re Target Corporation Customer Data Security Breach Litigation No. 14-2522 (D. Minn. Mar. 18, 2015). Comparing the measures that were required in the 2015 settlement with those in the 2017 settlement highlights the dramatic increase in expectations for cybersecurity over the last two years. Indeed, the requirements set forth in the recent Target settlement closely track the cybersecurity measures that were recently imposed by the New York Department of Financial Services ("DFS") through Rule 23 NYCRR 500, which New York Governor Cuomo described as "strong, first-in-the-nation protections," and which the DFS characterized as "landmark regulation."[1]

This chart lists some of the specific cybersecurity measures required in the 2017 settlement:

Specific Cybersecurity Requirement	Required by the 2015 Settlement	Required by the 2017 Settlement	Required by new DFS Cyber Regulations[2]
Maintain a written Information Security Program/Policy	✓	✓	✓
Periodically review sufficiency of safeguards	✓	✓	✓
Appoint a Chief Information Security Officer ("CISO") *with appropriate background or experience in information security*		✓	✓
Reporting by CISO to the board of directors		✓	✓
Periodic vulnerability assessments and penetration testing		✓	✓
User access control/privileges management		✓	✓
Maintain a third party service provider cybersecurity policy		✓	✓
Employ multi-factor authentication		✓	✓
Implement policies and procedures to monitor user activity and detect unauthorized access		✓	✓
Encryption or alternative control of personal information		✓	✓

[1] Press Release, New York Department of Financial Services, Governor Cuomo Announces First-in-the-Nation Cybersecurity Regulation Protecting Consumers and Financial Institutions from Cyber-Attacks to Take Effect March 1 (Feb. 26, 2017), http://www.dfs.ny.gov/about/press/pr1702161.htm.

[2] Pursuant to Rule 23 NYCRR 500, entities that are subject to the DFS cybersecurity regulations have grace periods before they are required to comply with the requirements, which take effect in stages ranging from August 2017 to March 2019. Certifications of compliance with those regulations are required in February of the year following the year in which the particular requirement became effective.

The significant overlap between the terms of the recent Target settlement, which included 47 Attorneys General, and measures required by the new DFS cybersecurity regulations illustrates the specific measures that appear to be emerging as industry best practices in cybersecurity.

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

John L. Douglas	**202 962 7126**	**john.douglas@davispolk.com**
Avi Gesser	**212 450 4181**	**avi.gesser@davispolk.com**
Reuben Grinberg	**212 450 4967**	**reuben.grinberg@davispolk.com**
Michelle Ontiveros Gross	**650 752 2073**	**michelle.gross@davispolk.com**
Joseph Kniaz	**202 962 7036**	**joseph.kniaz@davispolk.com**
Jon Leibowitz	**202 962 7050**	**jon.leibowitz@davispolk.com**
Neil H. MacBride	**202 962 7030**	**neil.macbride@davispolk.com**
Antonio J. Perez-Marques	**212 450 4559**	**antonio.perez@davispolk.com**
Gabriel D. Rosenberg	**212 450 4537**	**gabriel.rosenberg@davispolk.com**
Margaret E. Tahyar	**212 450 4379**	**margaret.tahyar@davispolk.com**