ALERT MEMORANDUM

Recent Developments Highlight Measures To Mitigate Litigation and Regulatory Exposure From Cyber-Attacks

June 21, 2017

Late last month, Target Corporation ("Target") reached an $18.5 million settlement with the Attorneys General ("AGs") of 47 states and the District of Columbia, resolving the AGs' investigation into Target's 2013 data security breach. Target, like other victims of cyber breaches, has faced intense regulatory inquiries based on the incident, along with extensive civil litigation by consumers, shareholders, and financial institutions.

Target's multistate settlement with regulators – the largest such data breach settlement to date – brings the total amount paid by the company to settle legal claims arising out of the breach to over $130 million, including settlements paid to private litigants. This amount represents only a fraction of Target's total loss arising from the incident, including the reputational harm the company suffered, lost revenue following the announcement of the breach, and the expense of implementing remedial measures.

Target's experience serves as a vivid reminder of the potential exposure that can result from a cyber breach. However, as we examine below, Target's recent settlement, when viewed in conjunction with other recent developments, also provides a roadmap for prophylactic measures that companies may implement to limit the likelihood that cyber criminals will successfully obtain sensitive data and potentially limit liability if such an attack occurs.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

NEW YORK

Jonathan S. Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Daniel Ilan
+1 212 225 2415
dilan@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

NEW YORK
One Liberty Plaza
New York, NY 10006-1470
T: +1 212 225 2000
F: +1 212 225 3999

Background

In late 2013, Target suffered a significant data breach at the hands of sophisticated cyber criminals. The hackers infiltrated Target's systems and obtained personal and financial data for up to 110 million customers – including names, contact information, payment card numbers, expiration dates, card verification codes, and encrypted PINs. The immediate fallout from the breach included a decline in Target's quarterly profits and was followed by the resignation of Target's CEO. The company also promptly became a target for civil plaintiffs and regulators seeking to hold the company liable for losses stemming from the breach.

Civil Litigation

Following a cyber incident, a company faces potential litigation from numerous interested parties, including customers, other affected third parties, and shareholders. Each of these litigants brought claims against Target in the aftermath of the 2013 breach.

Consumer Litigation. Dozens of plaintiffs seeking to represent a class of consumers commenced suit against Target claiming that they had suffered losses from the incident. In March 2015, Target agreed to pay $10 million and implement enhanced data security measures to settle the consumer class action. The District Court approved the settlement and certified the settlement class. However, the settlement is currently in limbo after the Eight Circuit found that the District Court's class certification analysis was insufficiently rigorous and ordered further analysis before ruling on whether the settlement would be affirmed.[1]

Financial Institution Litigation. Numerous financial institutions also brought suit against Target for the costs they had incurred on behalf of Target's customers due to the breach, including amounts paid to cover fraudulent charges and reissuing payment cards. The financial institutions alleged that Target had failed to implement adequate data protection measures. In 2015, Target entered into two settlements with financial institution plaintiffs, agreeing to pay approximately $108 million to reimburse card issuers for costs resulting from the breach. These settlements are now final.

Shareholder Litigation. Various shareholders also brought derivative actions against the company and certain of its officers and directors, alleging that the Target Board and management had breached their fiduciary duties in failing to implement sufficient data protection and cybersecurity measures. In order to investigate the shareholders' allegations, Target established a Special Litigation Committee, which conducted an investigation over 21 months and ultimately concluded that Target should not pursue the derivative claims. The District Court later affirmed this conclusion as an appropriate exercise of the Board's business judgment.

Regulatory Action

In addition to the civil litigation exposure stemming from a cyber breach, various state and federal regulators have jurisdiction over such incidents. A range of agencies and authorities have been conducting investigations with respect to the Target breach.

Federal Investigations. At the federal level, the Federal Trade Commission ("FTC") has the authority to oversee corporate cybersecurity practices and has brought a number of cases alleging that companies have not lived up to their data security promises and thereby deceived consumers. The Consumer Financial Protection Bureau ("CFPB") entered its first cybersecurity enforcement order last year against an online payment platform, alleging that the platform overstated its data security practices. The Securities Exchange Commission ("SEC") may also impose penalties on companies that fail to properly disclose

[1] *In re Target Corp. Customer Data Sec. Breach Litig.*, 847 F.3d 608, 615 (8th Cir.), amended, 855 F.3d 913 (8th Cir. 2017).

breaches. Target has disclosed that both the SEC and the FTC are investigating events related to the 2013 data breach.

State Investigations. At the state level, AGs and other regulators, like the New York Department of Financial Services ("DFS"), have jurisdiction to enforce state cybersecurity laws and have shown marked interest in such matters. As part of Target's recent settlement with the AGs, in addition to paying $18.5 million, Target is required to adopt heightened data security measures, including enhanced data encryption practices, two-factor authentication practices, data segmentation policies, the appointment of an executive to oversee information security, and the hiring of outside consultants to conduct security assessments.

An Emerging Data Security Standard

In announcing the settlement, one of the AGs described it as establishing "industry standards" for cybersecurity practices.[2] The settlement comes on the heels of several other recent developments in this area, including the promulgation of new cybersecurity regulations by DFS, the recent consumer settlement in the Home Depot cyber breach case, and Target's own settlements with consumers and financial institutions. When viewed together, these agreements and regulations contain an emerging set of best practices for cybersecurity. For example, these sources suggest that companies would be well-served to:

- Establish a Chief Information Officer position;
- Conduct routine risk assessments and intrusion testing;
- Develop a service provider program to reduce third-party cyber security risks;
- Train employees on IT security issues;
- Encrypt personally-identifiable and other sensitive data (both in transit over external networks and at rest) and use multi-factor authentication as necessary; and
- Develop policies and procedures to monitor activity, detect unauthorized access and address any such issues, including incident response plans.

While specific requirements will vary by industry, this catalogue of cybersecurity practices provides a helpful roadmap to companies in several respects.

First, such measures can help guard against costly and disruptive cyber-attacks like the one that was suffered by Target by making it more difficult for hackers to obtain access and disseminating any information that hackers might obtain. Second, in the event of an attack, a company that already has such measures in place, has a potentially powerful line of defense against litigants and regulators. Courts and regulators will continue to be sympathetic to the fact that cybercriminals are ever more sophisticated and may bypass almost any security measure because of technical or human shortfall. A company that has implemented industry standard cybersecurity measures, including protections along the lines set forth above, will be better situated to convince courts and regulators that the company should not be liable because hackers were able to override well-designed measures. Third, and finally, as more regulators become active in monitoring data protection compliance, implementing the measures that have been part of the recent agreements and regulations (and creating a record to that effect) can help establish that a company has adequate data protections in place.

Conclusion

Target's recent settlement, amid a wave of cybersecurity-related litigation, reveals the increasing exposure faced by companies that collect large troves of personally-identifiable or other sensitive data. As another AG stated in announcing the Target settlement: "This [settlement] should send a strong

[2] Press Release, Lisa Madigan, Illinois Attorney General, Attorney General Madigan Announces $18.5 Million Settlement With Target Over Data Breach: Agreement Establishes Industry Standards for Collecting and Protecting Consumer Data (May 23, 2017), http://www.illinoisattorneygeneral.gov/pressroom/2017_05/20170523b.html.

message to other companies: you are responsible for protecting your customers' personal information. Not just sometimes – always."[3]

Going forward, companies would be well-served to implement data security best practices, as set out in recent settlements and regulations and to be attentive to continued improvements (as well as new regulations) in this area. Doing so will not only help protect a company's valuable data, but could also help to limit litigation and regulatory liability in the event of a cyber incident.

…

CLEARY GOTTLIEB

[3] Press Release, Xavier Becerra, California Attorney General, Attorney General Becerra: Target Settles Record $18.5 Million Credit Card Data Breach Case: Multi-State Settlement Requires Target to Implement Specific Measures to Protect Customer Information from Cybersecurity Threats (May 23, 2017) https://oag.ca.gov/news/press-releases/attorney-general-becerra-target-settles-record-185-million-credit-card-data.