KING & SPALDING

Client Alert

Data Privacy & Security Practice Group

December 15, 2014

Financial Institutions' Claims in Data Breach Litigation Survive Target's Motion to Dismiss

In a much anticipated decision, a United States District Court in Minnesota denied Target's attempt to dismiss financial institutions' putative class action claims relating to losses they suffered as a result of last year's holiday-season security breach that affected approximately 110 million Target customers.[1] At this early stage in the litigation, the court concluded that the financial institutions ("FIs") had sufficiently stated claims against Target for negligence, a violation of Minnesota's Plastic Security Card Act ("PSCA"), and negligence per se as a result of Target's violation of the PSCA.[2]

The more than 100 lawsuits filed in the weeks following the massive hacking of consumer information were consolidated by the Judicial Panel on Multidistrict Litigation into two distinct types of claims, those brought by consumers and those brought by FIs.[3] The Minnesota court's recent decision involved claims by the FIs. The FI plaintiffs are primarily issuer banks who issued credit and debit cards and provided credit to affected consumers.

While acknowledging that third-party hackers' criminal activity caused the harm to the FIs, the court noted that "Target played a key role in allowing the harm to occur." The FIs allege that Target failed to maintain appropriate data security measures, disabled certain security features that could have prevented the breach, and failed to heed the warning signs as the attack began. The court found that those allegations sufficiently pleaded a claim of negligence against Target. The court rejected Target's argument that it did not owe the FIs a duty of care, concluding that Target owes a duty to safeguard its customers' credit and debit card data. The court concluded that imposing this duty on Target is consistent with Minnesota's policy of punishing companies that do not secure consumers' credit and debit card information and the legislature's endorsement of other remedies in addition to those available under the PSCA, which provides that the remedies available for violations of the PSCA are "cumulative and do not restrict any other right or remedy otherwise available" to the FIs.[4]

The court also ruled that the FIs had sufficiently alleged that Target's actions violated the PSCA, which prohibits the retention of the card security code data, the PIN verification code number or full contents of any track or magnetic stripe data subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.[5] The PSCA provides that an entity that has violated the

For more information, contact:

Barry Goheen
+1 404 572 4618
bgoheen@kslaw.com

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

Sarah E. Statz
+1 404 572 2813
sstatz@kslaw.com

Julia C. Barrett
+1 404 572 3562
jbarrett@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

www.kslaw.com

PSCA's retention requirements must reimburse the issuer banks for the costs of reasonable actions undertaken by the FIs to protect consumer information following a data breach, including the notification of cardholders affected by the breach, and any refund or credit made to a cardholder to cover the cost of any unauthorized transaction relating to the breach, among other things. Again, despite the fact that the hackers' illegal activity caused the harm to the FIs, the court allowed the PSCA claim to proceed on the basis that Target stored data for longer than the PCSA allows, which played at least some role in enabling the hackers to access some of the stored data.

The FIs also alleged that Target's violation of the PSCA proves negligence per se against Target. Target moved to dismiss the negligence per se claims on the basis that the PSCA applies only to transactions that occur in Minnesota. The court rejected that argument and found that the PSCA applies to the data retention practices of entities that conduct business in Minnesota, regardless of where the transaction actually occurs. The court also rejected Target's argument that it was the hacker's activities, and not Target's retention of data, that caused harm to consumers. The court permitted the negligence per se claim to proceed because Target's activities played at least some role in enabling the hackers to access the consumer data.

The court granted Target's motion with respect to the claim that Target's failure to inform the FIs of its insufficient security constituted a negligent misrepresentation by omission. The court found that Target had breached a duty to the FIs because it knew facts about its ability to repel hackers that the FIs could not have known, and yet made misleading representations regarding its data security practices. Nevertheless, the claim for negligent misrepresentation was dismissed without prejudice because the FIs had failed to plead any reliance on Target's alleged omissions. The court granted the FIs thirty days to file an amended complaint to address the deficiency in pleading reliance.

The court has yet to decide Target's motion to dismiss the consumer class action claims. While the consumer class action raises many different claims and distinct issues, the court's imposition of a duty on Target to protect customer's credit and debit card data could carry over into the analysis of similar negligence claims pled in the consumer class actions. This decision comes at a very early stage in the litigation; the court was only required to assess whether the issuer banks have "plausibly alleged" Target's negligence, and did not reach the ultimate merits of the banks' legal theories. Nevertheless, the holding carries important ramifications. The imposition of a duty of care on Target to protect debit and credit card data carries implications for all businesses that accept credit or debit card payments. It sends a signal to retailers to review their data security policies and ensure they have in place reasonable security measures to protect sensitive customer information.

* * *

King & Spalding's Data, Privacy and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and data security law. Our Data, Privacy & Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 50 Data, Privacy & Security lawyers in offices across the United States, Europe and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property

rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy.

---

[1] *In re Target Corp. Customer Data Security Breach Litigation*, MDL No. 14-2522, 2014 WL 6775314 (D. Minn. Dec. 2, 2014).
[2] The court did dismiss the claim that Target's failure to inform the Plaintiffs of its insufficient security constitutes a negligent misrepresentation by omission, because the Plaintiffs had not sufficiently pled they relied on Target's alleged omissions.
[3] Specifically, the MDL created by the Judicial Panel on Multidistrict Litigation consists of more than 80 actions filed by consumers, nearly 30 by financial institutions, and four shareholder derivative actions. *See Target, Class Attys Fight Banks' Bid to Sever Breach Suit*, Law360, New York (July 16, 2014).
[4] The court did not address the causation and damages elements of a negligence claim because Target did not challenge the allegations with respect to those elements.
[5] Minn. Stat. § 325E.64, subd. 2, 3.