COMMERCIAL & BUSINESS LITIGATION

SECTION OF LITIGATION

Fall 2017, Vol. 19, Issue 1

TABLE OF CONTENTS

COMMERCIAL & BUSINESS LITIGATION
SECTION OF LITIGATION

Fall 2017, Vol. 19, Issue 1

Practice Points »

Shop until the International Shoe Drops: SCOTUS Restricts Forum Shopping Against an Out-Of-State Employer

By Kathryn Dietrich Perreault

Out-of-state corporation must still have “continuous and systematic” contacts with forum state to be “at home” and subject to general personal jurisdiction.

Voices of Recovery Podcast Series

By ABA CoLAP

The ABA Commission on Lawyer Assistance Programs debuted the first of a series of podcasts that will address substance use disorders, mental health issues, addiction, and recovery issues. Episode 1 features attorney Laurie Besden, the Executive Director of Lawyers Concerned for Lawyers of Pennsylvania, who shares her battles with alcohol and drug addiction.

5 Billing Tips for Young Lawyers

By Michael S. LeBoff

Making the most of your time.

Payment Card Data Breach Class Actions: Who Foots the Bill?

By Shireen Meer, Claire MacKoul, and Robin Cantor – December 18, 2017

Payment cards are commonly used instead of cash to purchase goods and services at retail outlets. These transactions require the transfer of consumers' payment card information through a network of industry players. At each stage of transfer, consumers' information is potentially vulnerable to hackers. Given the ubiquity of payment cards, it should be no surprise that payment card data breaches are commonplace in today's data-driven economy. These breaches compromise sensitive information and ultimately can result in some form of harm to the parties whose information has been compromised. It is not surprising that litigation follows in the wake of such large data breaches. The large scale of potential losses that can result from these data breaches has stimulated questions regarding liability for the incidents—i.e., who should foot the bill?

Background

The Target data breach of December 2013 is an example of one of the largest breaches of payment card information in recent history. To place the Target breach in context with other business breaches in the same time period, the Identity Theft Resource Center reported 40 million exposed records from the Target breach, whereas the second largest data breach during this time period compromised only 2.9 million records. "Target Targeted in Data Breach," *Identity Theft Resource Ctr.* (last visited Dec. 2, 2017); "ITRC 2013 Breach List Tops 600 in 2013," *Identity Theft Resource Ctr.* (last updated Feb. 5, 2015). What further sets apart the Target data breach case from other cases, aside from the number of compromised accounts, is that it is the first data breach to date involving a certified class of financial institutions. *See* Memorandum & Order, *In re Target Corp. Customer Data Sec. Breach Litig.*, No. 0:14-md-02522-PAM (D. Minn. Sept. 15, 2015) [hereinafter Class Certification Order]. Notably, there are relatively few examples where payment card information breaches even reached the class certification stage.

Target Breach

The plaintiffs alleged that, in late 2013, Target failed to "adequately secure payment information on its systems," and this failure resulted in the compromise of sensitive financial and personal data of Target customers. Consolidated Class Action Complaint, *In re Target Corp. Customer Data Sec. Breach Litig.*, No. 0:14-md-02522-PAM (D. Minn. Aug. 1, 2014) [hereinafter Complaint]. Similar to prior cases related to the Heartland and TJX data breaches, the class action case against Target separated into two "tracks": a consumer class and a financial institution class. Class Certification Order, *supra*, at 1–2. The financial institution plaintiffs

alleged that Target's security failure resulted in substantial losses for the financial institutions that issued the debit and credit cards involved in the data breach. Complaint, *supra*, ¶ 2. These losses took the form of replacement cards, reimbursement of fraud losses, and other remedial actions in response to the data breach. Class Certification Order, *supra*, at 2. The plaintiffs sought certification of a class of "[a]ll entities in the United States and its Territories that issued payment cards compromised in the payment card data breach that was publicly disclosed by Target on December 19, 2013." *Id.* at 15. In September 2015, U.S. District Judge Paul Magnuson certified the class. *Id.*

Target contended that no class-wide proof supported the plaintiffs' negligence claims or Minnesota Plastic Card Security Act (PCSA) claims and damages had to be calculated on an individual basis. *Id.* at 6. Target also relied on the *TJX* decision to support its arguments against class certification, but the court noted that this reliance was not appropriate because the *TJX* claims of misrepresentation and consumer fraud required proof of individual reliance—different from the negligence and PCSA claims against Target. *Id.* at 10 n.4. In response to Target's claim that a choice of law analysis was required for each plaintiff, Judge Magnuson determined that Minnesota's contacts with the case were sufficient enough to allow application of Minnesota law to the claims of non-Minnesota class members. *Id.* at 5–6. The court noted that the "risk of future harm" injuries that Target used for its defense were not applicable to the financial institutions because the plaintiffs had already suffered harm. For this point, the court relied on a survey of banks cited by the plaintiffs' expert that noted large-scale card reissuance for alerted-on cards. *Id.* at 7.

Related to the costs of reissuance, the court rejected Target's defense that reissuance was a business decision. *Id.* at 7–8. Although the financial institutions were not required by contract, law, or regulation to reissue "alerted-on" cards, Judge Magnuson determined that "[s]ome action on the part of the financial institutions was certainly warranted." *Id.* at 8. Despite Target's argument that there was no class-wide proof as to which cards were affected by the breach or whether the banks' actions were reasonable, the court ruled that it was "self-evident that actions a financial institution took after being notified that its cards were involved in the Target breach were taken, at least in part, to protect the institution's customers' information and to provide service to those customers." *Id.* at 9.

One of the important factors raised by the plaintiffs' experts was how the regulatory environment for financial institutions drives them to take steps to protect consumer payment card information—indicating that all or nearly all of the affected institutions likely had to respond in some material way. The court specifically noted that the plaintiffs' banking expert was helpful in noting what "a reasonable bank should have done or would have done in

response to the Target data breach." Memorandum & Order at 4, *In re Target Corp. Customer Data Sec. Breach Litig.*, No. 0:14-md-02522-PAM (Sept. 8, 2015).

Research into the regulatory structure surrounding the payment card industry shows financial institutions operate in a highly regulated environment that shapes incentives and potential responses to risk events, such as those compromising payment card data. Different types of banks have different, and sometimes overlapping, regulators. Consumer protection regulations are part of the industry's compliance regulations. These regulations ensure that financial institutions treat consumers fairly in both lending and deposit activities. Technology requirements for financial institutions include rules regarding electronic banking, privacy, safeguarding customer information, information security, and more. Based on the attributes of its member financial institutions, regulators supervise compliance through regular, periodic examinations. If a financial institution is found to have problems or to be noncompliant, the regulator may use its authority to request that the bank correct the problems. In order for financial institutions to comply with regulatory requirements, and maintain acceptable examination ratings, they monitor and respond directly to notifications of data breaches in their customers' nonpublic personal financial information. This highly regulated environment is consistent with the court's findings that the financial institutions' actions were "self-evident" following the notification of the Target data breach. *See* Class Certification Order, *supra*, at 9.

Making a reference to the plaintiffs' economic expert's methodology and finding it reliable to support the plaintiffs' class-wide damages allegations, the district court in the *Target* case noted that "[d]amages can and often are left to determination after liability issues are resolved"; even if the damages ultimately could not be estimated on a class-wide basis, that would not preclude class certification if the other criteria are met. *Id.* at 10 n.5. The court noted that the plaintiffs, through their economic expert, were able to establish that "it is possible to prove classwide common injury and to reliably compute classwide damages resulting from reissuance costs and fraud losses." *Id.* at 13. The court further noted that, ultimately, if damages were not able to be worked out, the class would be decertified. *Id.*

Networks such as Visa and MasterCard have developed processes and guidelines for calculating operational reimbursement and fraud recovery owed to financial institutions that fall victim to data breaches. *See* MasterCard, Account Data Compromise User Guide (2016); "Global Compromised Account Recovery Program Modified to Reflect Increased Response Costs," *Visa* (May 14, 2015). Based on these guidelines, networks use data routinely collected on credit card transactions to estimate the operational and fraud costs faced by financial institutions with accounts compromised in merchant data breaches. This common information could potentially be used for a reliable damage methodology, at least in the cases of reissue and fraudulent charges, because these data are collected by the networks.

Additionally, academic literature points to approaches for quantifying the costs associated with data breaches. For example, scholars have conducted cost-benefit analyses of reissuing compromised cards by financial institutions by comparing estimates for the cost of reissuing and the cost of not reissuing cards. *See, e.g.*, James T. Graves et al., "Should Payment Card Issuers Reissue Cards in Response to a Data Breach?" (June 2014). The cost of reissuing cards was estimated based on survey responses of credit card issuers and estimates reported by analysts or unnamed issuers. *Id.* at 7. The cost of not reissuing cards was estimated based on the expected cost of fraud on an account due to a data breach, and the sources used to calculate this value ranged from publicly available data breach databases to identity theft survey reports. *Id.* at 7–10, 18–20. As data breaches become more prevalent and the financial industry and consumers become more aware of resulting operational and fraud costs, the scholarly inquiry into quantifying the costs associated with data breaches will continue to develop and can provide a basis for reliable damages models.

Conclusion

The court's decision in the *Target* matter likely set a new precedent because it was the first time a class of financial institutions was certified in a data breach litigation. During the time between the *TJX* and *Target* class action litigations, the economics of data breaches have come into clearer focus. The plaintiffs' economic expert in the *Target* matter examined the regulatory structure of the financial industry as the foundational support for common impact and developed a systematic, data-driven approach to analyzing damages. Although courts previously have rejected existing industry dispute resolution mechanisms to measure damages in data breach class actions, the data upon which these mechanisms rely can be used for class-wide analysis. Recognition of the data available from the payment card networks was influential in the *Target* certification decision.

Following the certification decision, Target settled with the financial institutions for $39 million. Christie Smythe, "Target Settles with Banks over 2013 Breach for $39 Million," *Bloomberg Tech.* (Dec. 2, 2015). It remains to be seen whether the certification of the class in the *Target* matter influences the proceedings of subsequent data breach litigations. A subsequent data breach matter between Home Depot and a proposed, but not yet certified, class of financial institutions settled for $25 million in March 2017. Jeff John Roberts, "Home Depot to Pay Banks $25M in Data Breach Settlement," *Fortune* (Mar. 9, 2017). Clearly, financial institutions are continuing to pursue compensation for data breaches that far exceeds the amounts offered by the payment card networks through their alternative dispute resolution mechanisms. The recent Equifax breach has prompted renewed interest into the economic consequences of data breaches, and developments will be closely watched. *See* Bloomberg Politics, "FTC Opens Investigation into Equifax Breach," *Bloomberg Pol.* (Sept. 14, 2017).

Shireen Meer is an associate director and Claire MacKoul is a consultant at Berkeley Research Group in Washington, D.C. Robin Cantor is a managing director at the same office and was the economic expert retained by the plaintiffs' counsel in the Target financial institution class action.
The authors wish to thank Michelle Anderson of DLA Piper for helpful comments on an earlier draft.

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the opinions, position, or policy of Berkeley Research Group LLC or its other employees and affiliates.

EDITORIAL BOARD

The views expressed herein are those of the author(s) and do not necessarily reflect the positions or policies of the American Bar Association, the Section of Litigation, this committee, or the employer(s) of the author(s).

ABA Section of Litigation Commercial & Business Litigation Committee
http://www.americanbar.org/publications/litigation-committees/commercial-business