KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

December 23, 2014

Consumers Permitted To Proceed With Data Breach Class Action Against Target

On December 18, 2014, the U.S. District Court for the District of Minnesota ruled, in a 46-page opinion, that a putative class of consumers could proceed with a majority of their claims against Target arising from the data breach Target sustained over the holiday season in 2013.[1] The plaintiffs allege financial losses after their credit- and debit-card information was stolen during Target's data breach.[2]

The plaintiffs asserted seven claims based on common-law theories and alleged statuory violations, in their 121-page complaint. Target moved to dismiss all claims under Rule 12(b)(6), contending that the plaintiffs lacked standing and that the complaint did not provide sufficient detail to support the allegations. The Court denied most of Target's motion given the early posture of the case. The Court's Order demonstrates the complexities of class action suits where the causes of action are subject to the distinct laws of all 50 states.

Standing Analysis

The Court first addressed the threshold issue of standing, a basis upon which many courts have dismissed proposed data breach class actions due to a lack of actual injury. In its Order, however, the Court held that the plaintiffs had sufficiently pleaded injuries that were "actual or imminent," including "unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees," which, the Court held, was "sufficient to plead standing."

The Court also held that "Article III standing analysis is best left to after the class-certification stage," denying as premature Target's motion to dismiss for lack of standing any claims brought under the laws of five states not associated with any of the 114 named plaintiffs.

In a third point of contention on standing, the Court held that the plaintiffs had pled sufficient injuries to seek injunctive relief, such as implementing stricter data security and the provision of extended credit-monitoring services.

Alleged Violation of State Consumer Protection Laws

Turning to the substance of the claims pleaded in the complaint, the Court analyzed many states' consumer protection laws. For purposes of analyzing a

For more information, contact:

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

Mark H. Francis
+1 212 556 2117
mfrancis@kslaw.com

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

New York
1185 Avenue of the Americas
New York, NY 10036
Tel: +1 212 556 2100
Fax: +1 212 556 2222

www.kslaw.com

motion to dismiss, the Court found that the plaintiffs had sufficiently alleged economic injury to satisfy the standard applied by states in which the consumer protection statutes require "pecuniary loss." Since neither party provided the Court with any legal authority regarding the type of allegations that are sufficient to establish a "duty to disclose" required under certain states' consumer-protection statutes, the Court held that the plaintiffs' allegations were sufficient under those statutes as well.

The Court, however, dismissed the plaintiffs' claims of consumer protection violations with respect to states that prohibited class-action treatment of such claims (Alabama, Georgia, Kentucky, Louisiana, Mississippi, Montana, South Carolina, Tennessee and Utah). The issue turned on a 2010 Supreme Court decision in *Shady Grove Orthopedic Assoc., P.A. v. Allstate Ins. Co.*, which had no majority opinion.[3] Citing other district courts acknowledging Justice Stevens' concurrence as the controlling opinion of that case, the Court held that the states' prohibition of class-actions in private rights of action is a substantive issue (not procedural), therefore, state law trumps Rule 23's federal class-action mechanism and the substantive class-action prohibition in those statutes requires dismissal.

Alleged Violation of State Data Breach Notice Statutes

Target contended that the plaintiffs' claims under state data breach notice statutes failed because they could not show damages flowing from the alleged violation of those statutes, but the Court found the argument to be premature. Thus, the Court denied Target's motion to dismiss those claims.

Target also contended that 29 of the 38 data-breach notice statutes asserted in the plaintiffs' claims provide no private right of action. Plaintiffs withdrew their claims under Florida, Oklahoma, and Utah law, but maintained that the other 26 states provided a right of action implicitly or explicitly through related consumer-protection statutes. The Court held that "the data-breach notice statutes of Arkansas, Connecticut, Idaho, Massachusetts, Minnesota, Nebraska, Nevada, and Texas allow for enforcement only by the state's attorney general or other government official, and the Rhode Island statute's silence on enforcement is to be construed as prohibiting private rights of action." However, for the remaining states with statutes containing (i) ambiguous language, (ii) non-exclusive remedies, or (iii) no enforcement provision, the Court declined to dismiss the plaintiffs' claims.

Negligence

The Court preserved most of the plaintiffs' common-law negligence claim, except with respect to five states (Alaska, California, Illinois, Iowa, and Massachusetts) that impose the economic loss rule, which bars a plaintiff from recovery of purely economic losses under a tort theory of negligence.

Breach of Contract and Implied Contract

The Court dismissed *without* prejudice the plaintiffs' breach-of-contract claim for REDcard debit cardholders. The complaint alleged that in the cardholder agreement, Target claimed to "use security measures that comply with federal law," and the Court held that in order to sufficiently plead a viable claim for breach of contract, the complaint would need to identify the federal law(s) with which Target allegedly failed to comply.

The Court did preserve the plaintiffs' claim for breach of implied contract. The plaintiffs contended there was an an implied contract in which they agreed to use their credit or debit cards to purchase goods and Target agreed to safeguard their personal and financial information. Target contended that the plaintiffs failed to allege any meeting of the minds sufficient to establish an implied contract. In consideration of differing prior decisions, the Court concluded that the alleged breach of implied contract was sufficiently pled, and a determination of the terms of an alleged implied contract was left as a factual question for a jury to determine.

Bailment

The plaintiffs' claim of bailment (*i.e.*, delivery of property that must be returned after the purpose has been fulfilled) was dismissed *with* prejudice because, according to the Court, the plaintiffs did not allege that Target wrongfully retained any information.

Unjust Enrichment

The plaintiffs' final claim, for unjust enrichment, was pled with two theories. First, they argued that Target "overcharged" consumers by selling goods at a price that was presumed to include a premium for adequate data security. The Court rejected this theory, noting that all consumers paid the same price regardless of whether the payment method required security (*i.e.*, cash or credit). The Court, however, did find plausible merit in the plaintiffs' second theory, which posited that consumers "would not have shopped" at Target had they been notified after Target knew or should have known of the breach.

Impact

The Court's decision is a mixed bag for data breach plaintiffs and defendants. Most data breach class actions have foundered because the plaintiffs have been unable to plead an "actual or imminent" injury sufficient to establish Article III standing; a recent District Court decision out of Illinois **dismissing a data breach class action against P.F. Chang's** exemplifies these decisions.[4] The Target consumers arguably pleaded more "actual or imminent" injuries than many prior data breach class plaintiffs, and it is likely their allegations will become a model for future data breach plaintiffs seeking to escape immediate dismissal.

One the Court found standing, it was easier for the plaintiffs to survive dismissal of most of their claims given the liberal Rule 12(b)(6) standard. Nevertheless, even under that standard, the Court dismissed some of the plaintiffs' claims, and in several other instances in emphasized that Target would be free to renew its arguments—particularly with regard to actual damages—at the summary judgment stage. Still, defendants in future data breach cases can expect their consumer-plaintiffs to cite the Target order in their effort to avoid immediate dismissal.

For a copy of the District Court's Order, please click **here**.

* * *

King & Spalding's Data, Privacy and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information 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 30 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] *See* Memorandum and Order, *In re: Target Corporation Customer Data Security Breach Litigation* (Consumer Cases), MDL No. 14-2522-PAM-JJK, Dkt. 281, 2014 WL 7192478 (D. Minn. Dec. 18, 2014) ("Order").
[2] An order denying Target's motion to dismiss all cases filed by financial institutions was recently issued by the same Court. *See* Memorandum and Order, *In re: Target Corporation Customer Data Security Breach Litigation* (Financial Institution Cases), MDL No. 14-2522-PAM-JJK, Dkt. 261, 2014 WL 6775314 (D. Minn. Dec. 2, 2014).
[3] 559 U.S. 393 (2010). Justice Scalia wrote the *Shady Grove* opinion for himself and three other Justices, while Justice Ginsburg dissented with three other Justices. Justice Stevens concurred with Justice Scalia's judgment for a different reason viewed as "narrower" and thus supported by five justices.
[4] *Lewert, et al. v. P.F. Chang's China Bistro, Inc*., Nos. 1:14-cv-4787; -4923, Dkt. 35, 2014 WL 7005097 (N.D. Ill. Dec. 10, 2014) (on appeal).