Data privacy class actions

MATTHEW S. MULQUEEN
Baker Donelson, Bearman, Caldwell & Berkowitz, PC

MATTHEW G. WHITE
Baker Donelson, Bearman, Caldwell & Berkowitz, PC

MORE FROM BAKER DONELSON

Baker Donelson represents many community and regional financial institutions in connection with organization, governance, capital raising, mergers, acquisitions, branching, regulatory and governmental compliance, and more. For more information, contact Steven Eisen at *sjeisen@bakerdonelson.com*.

Over the last several years, corporate counsel have consistently identified data privacy class actions as a top concern.[1] The worry stems from the steadily increasing manner that commerce is conducted through the internet and the apparently endless ingenuity of individuals intent on stealing customer data for financial gain. Financial institutions are at particular risk because of the multiple ways that a data breach can impact their bottom line.

Financial Institutions as Defendants

Like any other entity that stores customer financial information electronically, a bank can find itself named in a putative class action following a breach of its computer systems. Plaintiffs in such cases typically assert state law claims, including negligence, based on the breached entity's alleged failure to implement adequate measures to protect customers' data.

In many early data breach cases, defendants challenged plaintiffs' claims—sometimes with success—on the grounds that the plaintiffs had only alleged speculative future injuries from the release of their personal information. As a result, plaintiffs have increasingly sought to identify tangible damage resulting from the theft of their data, including actual fraudulent use of the stolen information, costs associated with ongoing monitoring, and damages from the time and effort spent addressing the breach. Plaintiffs have also asserted claims based on defendants' alleged delays in notifying customers of breaches.[2]

Financial Institutions as Claimants

The risks to banks are not limited to breaches of their own systems. When a breach occurs at a nonbanking commercial entity, and customers of the bank and the entity suffer losses, those customers often look to the bank to make them whole. Banks may be obligated to indemnify customers for unauthorized transfers pursuant to statute[3] or contract. After incurring financial liability to their customers, banks may have a cause of action against the entity that suffered the breach.

In 2013, for example, Target announced that hackers had gained access to the credit and debit card data of approximately 40 million customers. The financial institutions that had issued the cards were forced to replace them, reimburse fraud losses, and take other remedial steps to address their customers' injuries. The banks asserted claims of negligence against Target and successfully moved to certify the case as a class action.[4]

Because the losses that financial institutions experience in such circumstances are tangible and immediate, they have sometimes been more successful than consumers in striking settlements with breached entities. In the Target litigation, for example, the banks ultimately settled their claims for $39.4 million—almost four times the amount that Target's customers settled for.[5]

Potential Hurdles to Recovery

Other banks, however, have not been so lucky. After a massive data breach at the retailer Schnucks, several card-issuing banks that suffered resulting losses brought suit. The U.S. Court of Appeals for the Seventh Circuit affirmed the district court's dismissal of the banks' complaint, holding that the economic loss doctrine barred their state law tort claims. That doctrine limits tort liabilities for purely economic losses inflicted by one business on another where those businesses have already ordered their duties, rights, and remedies by contract. The court concluded that the banks' claims effectively sought

remedies above and beyond those set out in the network of contracts that linked Schnucks, card-processors, the banks, and card brands.[6]

The banks argued that the economic loss doctrine did not apply because the banks did not directly contract with Schnucks. That did not matter, said the court. It was enough that the network of contracts set out standards and remedies for data breaches and that the multiple contracts tied together all the parties participating in the card payment system.

On the Horizon

Data breaches, and resulting lawsuits, are unlikely to slow down in the coming years. With potential interests as both defendants and plaintiffs in data breach litigation, banks should stay tuned for further developments as the courts work through the complicated legal issues at stake in these cases.

Endnotes

1 See The 2018 Carlton Fields Class Action Survey: Best Practices in Reducing Cost and Managing Risk in Class Action Litigation.
2 See, e.g., Complaint, LeRoy, et al. v. SunTrust Bank Inc., No. 1:18-cv-02200-MHC (N.D. Georgia, May 16, 2018).
3 See, e.g., 12 C.F.R. § 205.6.
4 In re Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482 (D. Minn. 2015).
5 See Decl., ECF No. 653-1, In re Target Customer Data Sec. Breach Litig., MDL No. 14-2522 (PAM) (D. Minn. Dec. 2, 2015); Order, ECF No. 364, In re Target Consumer Data Sec. Breach Litig., MDL No. 14-2522 (PAM) (D. Minn. March 19, 2015).
6 Cmty. Bank of Trenton v. Schnuck Markets, Inc., 887 F.3d 803, 807 (7th Cir. 2018).