Proskauer

Circuit Split Deepens as Eleventh Circuit Rejects "Risk of Identity Theft" Theory of Standing in Data Breach Suit

Minding Your Business Blog on **February 18, 2021**

On February 4, 2021, the Eleventh Circuit affirmed the dismissal of a customer's proposed class action lawsuit against a Florida-based fast-food chain, PDQ, over a data breach. The three-judge panel rejected the argument that an increased risk of identity theft was a concrete injury sufficient to confer Article III standing, deepening a circuit split on this issue.

The case, Tsao v. Captiva MVP Restaurant Partners, LLC, stemmed from a data breach at PDQ, in which a hacker exploited the restaurant's point of sale system to gain access to customers' credit or debit card information. When PDQ became aware of the breach, it posted a notice saying that the following customer data "may" have been accessed during the May 19, 2017 to April 20, 2018 time period: cardholder names, credit card numbers, card expiration dates, and card verification value codes. According to the opinion, the notice emphasized that it was impossible "to determine the identity or exact number of credit card numbers or names that were accessed or acquired," and that customers' information may have been exposed or compromised.

Upon learning of the data breach, plaintiff and PDQ customer I Tan Tsao cancelled the two credit cards he had used at PDQ locations during the relevant time period. Tsao also filed suit against Captiva MVP Restaurant Partners, LLC (the owner of PDQ) alleging negligence, breach of contract, unjust enrichment, and violation of the Florida Unfair and Deceptive Trade Practices Act. Tsao sought damages stemming from the loss of credit card cash back or reward points; loss of the use of his cards; and lost time and costs associated with cancelling the cards and taking other measures to protect himself against possible identity theft.

PDQ moved to dismiss the complaint for lack of standing, arguing that although customer financial data may have been compromised in the breach, Tsao had failed to identify "a single incident involving an actual misuse of the credit card information, much less any misuse . . . causing any of the customers any actual injury." PDQ reasoned that because Tsao's lawsuit was premised on a fear that his credit card information may be misused at some point in the future, he was foreclosed from alleging damages because he cancelled the cards before any misuse had occurred. Finally, PDQ argued that Tsao could not "manufacture" standing by pointing to the costs he apparently incurred in cancelling his credit cards following the breach.

The District Court granted the motion to dismiss, rejecting Tsao's argument that he and the other class members had standing because of (i) an increased risk of identity theft as a result of the breach and (ii) the costs related to mitigating that risk. Instead, the District Court found that the allegations of harm were conclusory and speculative, and that evidence of a data breach was, by itself, insufficient to confer standing.

In affirming the District Court's dismissal of Tsao's proposed class action, the Eleventh Circuit acknowledged the circuit split on the issue of whether the risk of identity theft could confer standing. But in summarizing decisions on this issue from other circuits, the court noted that the cases that conferred standing included at least some allegations of actual misuse or actual access to personal data. Here, Tsao alleged neither, and therefore the court found that he failed to demonstrate that the PDQ data breach placed him at a "substantial risk" of identity theft or that identity theft was "certainly impending" – particularly because he had already cancelled the credit cards in question.

In rejecting Tsao's second theory of standing – that he suffered an injury because of the time and costs spent mitigating the risk of identity theft – the Eleventh Circuit relied in large part on its en banc opinion in Muransky v. Godiva Chocolatier Inc. In that case, customers of Godiva chocolate stores alleged that Godiva printed too many digits on credit card receipts in violation of the Fair and Accurate Credit Transactions Act, thereby exposing customers to an increased risk of identity theft. The plaintiffs in that case, like Tsao, argued that they suffered injuries by mitigating the risk of identity theft – namely, by spending time "destroying or safeguarding" receipts. Citing the Supreme Court's decision in Clapper v. Amnesty International USA, the Muransky court explained that where a hypothetical future harm is not "certainly impending," plaintiffs are unable to create standing by inflicting harm on themselves. The panel in Tsao adopted this reasoning, finding that any costs incurred or time lost through Tsao's efforts to mitigate the risk of future identity theft did not confer standing.

Critically, the type of data compromised in the PDQ data breach also played an important role in the court's analysis. Here, the hacker may have accessed credit card numbers and the names of the cardholders, and other related credit card information. By itself, this information could enable hackers to commit credit card fraud, but the court explained that there is a much lower chance of identity theft where other personally identifiable information – like social security numbers, birthdates, or drivers' license numbers – is not also compromised. This leaves open the question of how the court would rule in a situation where personally identifiable information is part of the breach, and whether the reasoning in Tsao would still apply.

With this ruling, the Eleventh Circuit joins the Second, Third, Fourth and Eighth Circuits in rejecting the theory that an increased risk of identity theft is, by itself, a concrete injury that confers standing. Although this decision will provide some comfort for retailer or restaurant defendants seeking to dismiss similar lawsuits, businesses should take note of the particular facts of any data breach, including the type of data that has been compromised, and the law in their circuit. Unless and until the Supreme Court weighs in on this issue, it is unlikely that this will be the last time a plaintiff proffers this theory of standing following a data breach.

View Original