KAUFMAN | DOLOWICH

Mansfield Rule Certified 2022-2023

Eleventh Circuit Furthers the Current Circuit Split: Finding Lack of Standing in Data Breach Actions Based on Claimed Increased Risk of Identity Theft

Litigation Alert: Another One Bites the Dust

By Avery A. Dial, Esq. , partner and co-deputy chair of KD's Data Privacy & Cybersecurity practice group, and Barbara R. Schabert, Esq. , KD attorney in Florida

The Eleventh Circuit recently affirmed the dismissal of a class action lawsuit against PDQ following a data breach that exposed PDQ's customers' personal financial information. The Eleventh Circuit joins the Second, Third, Fourth, and Eighth Circuits with its ruling that an [illegible] the requirements of Article III standing.

Tsao v. Captiva MVP Restaurant Partners, LLC,[1] arises out of I Tan Tsao's class action lawsuit filed in the Middle District of Florida wherein Tsao alleges that PDQ breached an implied contract by failing to safeguard customers' credit card data; was negligent in failing to provide adequate security for the credit card data; was per se negligent based on violation of Section 5 of the Federal Trade Commission Act (15 U.S.C. Section 45), which prohibits unfair practices that affect commerce; was unjustly enriched when it received payments from the customers but failed to provide those customers with adequate data security; and violated the Florida Unfair and Deceptive Trade Practices Act. Tsao claimed damages related to the cancelling of certain credit cards and other costs associated with his mitigation efforts against a claimed increased risk of identity theft.

PDQ accepts payments through a point of sale system where customers can insert credit or debit cards to pay. When customers pay with a debit or credit card, PDQ[2] collects some data from the cards, including the cardholder's name, the account number, the card's expiration date, the card verification value code (CVV), and PIN data for debit cards. PDQ then stores this data in its point of sale system and transmits the information to a third party for processing and for completion of the payment. Through an outside vendor's remote connection tool, a hacker was able to exploit PDQ's point of sale system and gain access to customers' credit and debit card information. PDQ notified customers that PDQ had been the target of a cyber-attack and that all PDQ locations in operation between May 19, 2017 and April 20, 2018 were affected by the cyber-attack.

Tsao, having been a patron at PDQ during the applicable time period of the cyber-attack, claimed that as a result of the data breach notice, he suffered damages stemming from mitigation efforts resulting from an asserted increased risk of identity theft. These mitigation costs included the cancellation of two credit cards which resulted in the loss of cash back or reward points, and lost time spent addressing the problems caused by the cyber-attack.

PDQ filed a Motion to Dismiss based on lack of standing, arguing that Tsao failed to identify any incident involving an actual misuse of credit card information and asserted that Tsao's claims were premised on a fear that his credit card information may be misused at some point in the future. PDQ further argued that any potential mitigation costs incurred would constitute a "manufactured standing" which would not be enough to satisfy Article III.

Holding

The Eleventh Circuit had not before addressed whether a plaintiff has standing based on an alleged increased risk of identity theft and other harm in the future as a result of the data breach and recognized the current circuit split on the issue. The Eleventh Circuit reviewed opinions issued in Sixth, Seventh, Ninth, and D.C. Circuits, all which recognized that a plaintiff can establish injury-in-fact based on the increased risk of identity theft. In the Court's review of those opinions, there were not only allegations of increased risk of identity theft, but there were also allegations of actual misuse or actual access to personal data. The Court found that Tsao failed to allege that the data breach created a "substantial risk" of identity theft or that identify theft was "certainly impending."[3]

The Court also reviewed opinions issued in the Second, Third, Fourth, and Eighth Circuits all which declined to find standing based on an alleged increased risk of identity theft. The Eleventh Circuit looked closely to the Eighth Circuit opinion in assisting its rendering of the opinion in this case based on the similarities in facts. The Court notes the Eighth Circuit's use of the June 2007 United States Governmental Accountability Office (GAO) report[4] on data breaches to reach its conclusions and finds that the GAO report demonstrates why there is no substantial risk of identity theft here.

The Eleventh Circuit also reiterated its holding in Muransky v. Godiva Chocolatier, Inc., that management-of-risk claims are bound up with arguments of risk of identity theft, and finding that mitigation costs were insufficient to establish standing where there was no substantial risk of identity theft.[5]

Overall, the Eleventh Circuit held that Tsao lacked Article III standing because it could not be demonstrated that there was a substantial risk of future identity theft or that identity theft was certainly impending, and because he cannot manufacture standing by incurring costs in anticipation of non-imminent harm.

Practical Implications

The specific factual details of the PDQ data breach were a significant factor in the Eleventh Circuit's analysis. Through the point of sale system data breach, the hackers would have been able to potentially obtain credit card numbers, cardholder's names, expiration dates, CVV, and PIN data. Notably, the data breach did not include the potential compromise of personal information such as social security numbers, dates of birth, or driver's license numbers. The Eleventh Circuit relies on the GAO report which states that compromised credit or debit card information, without additional personal identifying information, generally cannot be used alone to open unauthorized accounts. The Eleventh Circuit further notes that the GAO Report states that most breaches have not resulted in detected incidents of fraud on existing accounts.

Here, the Eleventh Circuit focused heavily on the lack of compromised personal identifying information in ruling that plaintiff lacked standing based on the GAO report and the finding that it is does not support the conclusion that the PDQ breach presented a substantial risk that plaintiff would suffer incidents of fraud. Accordingly, it still remains unknown how the Eleventh Circuit might rule on whether there is standing for claimed increased risk of identity theft should a data breach include not only the potential compromise of credit card information, but also the potential compromise of personal identifying information.

The Eleventh Circuit's ruling in this case provides defendants such as restaurants, retail stores, and other establishments that use a point of sale system, or similar payment method system, with a strong argument for the dismissal of lawsuits where a data breach results in only the potentially compromised information of a plaintiff's credit card information and no accompanying personal identifying information.

[1] 2021 WL 381948 (February 4, 2021).
[2] PDQ is a d/b/a of Captiva MVP Restaurant Partners, LLC.
[3] See Clapper v. Amnesty Int'l USA, 568 U.S. 398, 133 S.Ct. 1138 (2013) (Finding that a threatened injury must be certainly impending to constitute a concrete injury in fact and that a plaintiff must make a showing that there is a substantial risk that the harm will occur).
[4] GAO-07-737, Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (2007), http://www.gao.gov/assets/270/262899.pdf

[5] Muransky, 979 F.3d 931 (plaintiffs cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending).