AUGUST 3, 2020

Data Breach Class Actions – Florida District Court Rules Threat of Future Injury Too Speculative to Support Standing

by Jeffrey H. Fisher

Takeaway: Data breach cases often turn on whether the threat of future identity theft suffices to establish Article III standing. In yet another data breach case, *In re Brinker Data Incident Litig.*, 3:18-CV-686-J-32MCR, 2020 WL 4287270, at *2 (M.D. Fla. July 27, 2020), the Middle District of Florida found that named plaintiffs who did not incur an unauthorized charge, but instead immediately cancelled their compromised debit cards, failed to allege a substantial likelihood that they would suffer future injury. Brinker International owns the Chili's chain of restaurants. Hackers accessed Brinker's network and obtained access to the payment card information of customers who had dined at Chili's in March and April of 2018. Several named plaintiffs filed a putative class action, and Brinker moved to dismiss for, among other reasons, lack of standing.

In its first ruling, the court found that five plaintiffs who alleged they had incurred unauthorized charges on their cards alleged concrete injuries sufficient to confer standing. *In re Brinker Data Incident Litig.*, 3:18-CV-686-J-32MCR, 2019 WL 3502993, at *6 (M.D. Fla. Aug. 1, 2019). The court took a broad view of Article III standing, concluding that an unauthorized charge was sufficient to confer standing even if the plaintiff did not allege that the losses were unreimbursed.

The court, however, found that two of the named plaintiffs who alleged only an increased risk of future injury failed to establish Article III standing. Although an increased risk of future injury can be sufficient to establish Article III standing, the risk must be "certainly impending—not merely possible—and cannot be too speculative." The court applied a three-part test – (1) whether there was a criminal motive by the hacker; (2) whether the information contained Personally Identifiable Information ("PII") (social security numbers, driver's license numbers, birthdates, etc.), or merely payment card information; and (3) whether there was evidence a third-party had already accessed or used the information. Pointing out that the plaintiffs had canceled their cards, and finding that only the first factor supported standing (because there was a criminal motive), the court dismissed the two named plaintiffs' claims for lack standing.

The plaintiffs amended their complaint, and Brinker once against moved to dismiss for lack of standing. The amended allegations asserted that, although they had cancelled the debit cards they used at Chili's, their card information remained on Brinker's system, and hackers could steal the old card information and use it to get the replacement card information. In support, the plaintiffs cited articles describing arrangements between credit card companies and merchants like Netflix where, if a hacker had added a stolen payment card to a merchant account, the card information would be automatically updated when the card was reissued after being cancelled.

The court found this scenario too implausible to establish Article III standing. 2020 WL 4287270, at *3. It

explained that, for plaintiffs to suffer injury, (1) Brinker would have to be hacked again, (2) plaintiffs' stolen cards would have to be serviced by a merchant that automatically updates new card information, (3) the hackers would have to find a merchant with an agreement with the stolen credit card's processor, and (4) the processor would have to send the replacement card information to the merchant. Pointing out that the plaintiffs had suffered no harm since the lawsuit was filed more than two years earlier, the court found this string of events too speculative to support Article III standing. It dismissed the named plaintiffs' claims for lack of Article III standing.

Brinker adds to a growing body of case law rejecting Article III standing in data breach cases based on the threat of future injury. Although the plaintiff in *Brinker* offered a particularly creative injury theory, the decision follows other authorities in holding named plaintiffs who cannot at least show evidence of an unauthorized charge face dismissal for lack of standing. It also demonstrates that the passage of time can work in a data breach defendant's favor, as the court viewed the risk of future injury especially speculative given that more than two years had passed since the data breach and the plaintiffs still had not suffered any injury.