Published on *The National Law Review* https://natlawreview.com

Mint Gets Data Breach Claims Dismissed

Article By:

Alyssa M. Sones

California federal Judge William Alsup dismissed various claims against Mint Mobile LLC based on a data breach that exposed personal information of Mint customers. Plaintiff Daniel Fraser alleged that Mint, a mobile virtual network operator using the T-Mobile network infrastructure, was hit with a data breach in June 2021. According to Fraser, the breach resulted in disclosure of his and others' personal information, including names, addresses, email addresses, phone numbers, account numbers, and passwords.

Fraser alleged that within a few days of the data breach, his phone number was ported out, or switched from one service provider to another. Fraser alleged that less than two hours after the SIM port-out, cryptocurrency drained from his ledger account. Ultimately, he alleges $466,000 in cryptocurrency was stolen from him.

Fraser's allegation that Mint had a role in helping the hacker gain control of his phone number sets this case apart from the typical data breach case. Usually, plaintiffs allege that disclosing their information in a breach resulted in later fraudulent activity or a risk of future fraud against the plaintiff. Often, plaintiffs allege no causal connection between the breach and the fraud.

Fraser alleges that Mint allowed Fraser's number to be ported out because it approved the porting out of his number. In doing so, he alleges Mint bypassed the access PIN Fraser had set up just days before to enhance the security on his account. In Fraser's theory, that would allow the hacker greater access to his accounts, such as the ability to bypass multi-factor authentication. Mint thus allegedly took steps after the breach that helped the hacker complete a fraud using the disclosed information.

Based on this series of events within just a few days of the breach or less, the Court allowed Fraser's negligence and breach of implied-in-fact contract claims past a motion to dismiss.

However, the Court dismissed Fraser's claim under California's Unfair Competition Law. The only available remedy that Fraser sought under the UCL was restitution. The Court held that restitution is unavailable in a situation like this because any stolen money went to a third-party criminal. As is common when data breaches lead to theft by the hacker, the defendant, Mint, acquired no money or other benefit from the alleged fraud. The Court similarly dismissed Fraser's request for punitive damages as to all claims.

The Court held that Fraser's federal claims required damage to a computer system. Fraser only

alleged financial loss flowing from the disclosure. The Court dismissed Fraser's federal claims under the Computer Fraud and Abuse Act and Federal Communications Act.

Putting it in Practice: With data breaches becoming more common, courts are becoming sophisticated at understanding the roles of the different players. Courts are also showing they will closely examine the harm alleged by the plaintiff early in a case. Companies defending against data breach claims may greatly limit the exposure early by asking a court to dismiss claims or remedies where the plaintiff's harm does not logically flow from the defendant's actions.

National Law Review, Volumess XII, Number 133