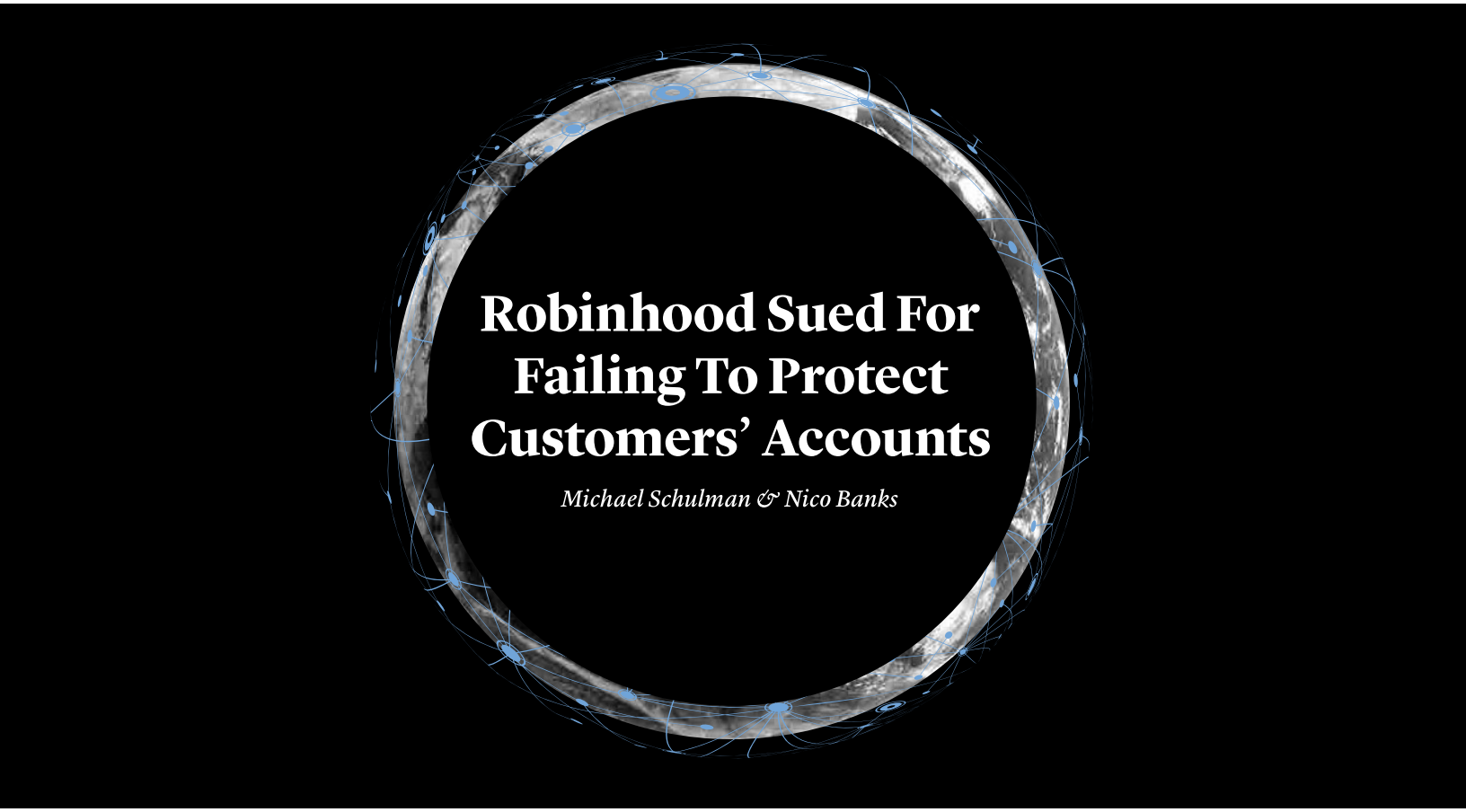


Robinhood Sued For Failing To Protect Customers' Accounts

Michael Schulman & Nico Banks

A class-action lawsuit in the Northern District of California against Robinhood Financial, LLC, a securities trading platform, alleges that unauthorized users accessed approximately 2,000 Robinhood customers' accounts storing the customers' sensitive personal information. The information included social security numbers, telephone numbers, bank account numbers, and tax information. The unauthorized users also looted the funds in the customers' accounts. The lawsuit seeks recovery for the looted funds as well as the time and money the class members spent attempting to cure the violations of their privacy.

On May 6, 20201, Judge Susan Van Keulen granted in part and denied in part Robinhood's motion to dismiss the Plaintiffs' claims. One of the claims that survived was the alleged violation of the California Consumer Privacy Act ("CCPA"). The CCPA is a comprehensive state-level data privacy legislation that took effect in January 2020. It creates a private right of action for a consumer whose personal information is subject to unauthorized theft or disclosure as a result of a data breach resulting from a company's failure to implement and maintain reasonable security procedures and practices. A "consumer" is not limited to individual purchasers of goods or services, but includes any California resident. Furthermore, the law does not just govern California-based companies, but extends to many other entities, including any entity doing business in California with annual gross revenues in excess of $25 million.

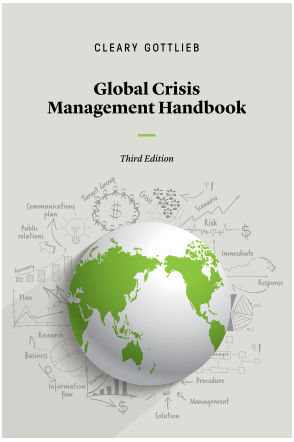
Robinhood argued that Plaintiffs' claim for a violation of the CCPA should be dismissed because the origination of the data breach was not on Robinhood's network; instead, outside identity theft by third parties led to access of the accounts. The court, however, allowed the claim to proceed because Plaintiffs had alleged that Robinhood failed

to implement and maintain standard security measures that could have prevented unauthorized users from transferring funds from an account or accessing sensitive personal information without substantial verification.

The court did dismiss Plaintiffs' claim for a violation of the Consumer Records Act ("CRA"), but it allowed Plaintiffs leave to amend. The CRA is a California law that creates a private right of action when a person or business that conducts business in California fails to disclose a breach of their security system in the most expedient time possible after discovering the breach of a California resident's data. The court noted that Robinhood allegedly only offered an email address—not a phone number—for customers to reach its customer service, and customer-service representatives allegedly failed to respond to emails promptly. As a result, customers who realized their accounts had been hacked allegedly waited days or weeks for Robinhood to respond to their emails regarding the breach and depletion of their funds. Plaintiffs also alleged that Robinhood took remedial action, such as alerting its customers about the breach, only after the breach was reported by the media. Despite those allegations, the court dismissed the CRA claim because Plaintiffs failed to specifically allege when Robinhood first learned of any incident for which it should have notified Plaintiffs sooner.

The Robinhood data breach, and Judge Van Keulen's decision, highlight the importance for companies that control or process personal data to implement and maintain systems that suitably protect that data from unauthorized disclosure. The Cleary Gottlieb Global Crisis Management Handbook discusses the CCPA in more detail and provides guidance to companies for ensuring proper data security. For example, organizations should ensure that employees have updated their machines with the latest security software, and that an organization's network blocks non-essential internet services that may cause vulnerabilities. The Handbook also recommends that an organization's IT staff has sufficient expertise and training in detecting and mitigating security issues and responding to new challenges. Organizations should also ensure that any third-party providers have been vetted against internal security standards, and internal recordkeeping memorializes that such due diligence was taken.

And while the CRA claim here was dismissed, the breach still highlights the importance of prompt communication and proactive rectification following a data breach. The European Union's General Data Privacy Regulation ("GDPR") mandates that companies ensure that they promptly notify supervisory authorities and implicated data subjects of a data breach in some circumstances. For organizations operating in the United States, it is best practice to do so, including because prompt communication and remedial action may lessen litigation risk, especially for organizations doing business in California, where the broad CCPA takes a page from the GDPR.



For more information, request a copy of the Global Crisis Management Handbook here.

13000000_062521