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

Crypto Wallet Data Breach Leads to Class Action Litigation

Article By:

Kathryn M. Rattigan

Plaintiffs filed suit in the District Court for the District of Delaware against Shopify Inc. and TaskUs Inc., alleging that the companies failed to implement measures to prevent a data breach that resulted in a breach of their personal information and cryptocurrency portfolios.

The breach occurred in 2020 and affected Leger SAS cryptocurrency hardware wallets, which had contracted with third-party vendors Shopify and TaskUs to process its customers' personal information. The breach affected 272,000 individuals' names, email addresses, postal addresses, and phone numbers.

The complaint alleges that the affected personal information was published online. It was also alleged that some individuals were faced with physical violence or blackmail threats if they did not transfer their crypto assets to the cybercriminals, which led to millions of dollars in cryptocurrency stolen.

The complaint includes allegations of negligence, unjust enrichment, violations of Florida's Deceptive and Unfair Trade Practices Act, violations of the North Carolina Unfair and Deceptive Trade Practices Act, violations of the Arizona Consumer Fraud Act, and violations of the Kentucky Consumer Protection Act.

Furthermore, the complaint alleges that phishing attempts were made by hackers posing as Ledger support team members and asking Ledger customers to download a fake version of the Ledger Live software.

Plaintiffs are seeking injunctive relief requiring Shopify and TaskUs to implement security safeguards to protect consumers' personal information as well as direct damages, punitive damages, compensatory damages, statutory damages, and attorneys' fees and costs.

National Law Review, Volume XII, Number 97