Users of 'especially secure' crypto network sue over $55 million theft

2022 DPDBRF 0080 • By John Fitzgerald

WESTLAW Data Privacy Daily Briefing • May 4, 2022

(May 4, 2022) - Users of a cryptocurrency network have filed a proposed class action alleging its founders created a protocol that was hacked despite their having "repeatedly and prominently" touted its superior security features.

Sarcuni et al. v. bZx DAO et al., No. 22-cv-618, *complaint filed*, 2022 WL 1434198 (S.D. Cal. May 2, 2022).

Christian Sarcuni and 13 other named crypto investors filed suit May 2 in the U.S. District Court for the Southern District of California over the theft of about $55 million in digital currency at bZx DAO, a decentralized autonomous organization.

The creators of bZx told users that they had no reason to "ever worry about … getting hacked," but the plaintiffs say that is exactly what happened.

The companies that control bZx owed users a duty of protection from malicious attacks such as the one that resulted in the theft, the suit says.

Suit: Phishing attack leads to hack

bZx is a cryptocurrency trading and lending platform that allows users to lend cryptocurrency and earn interest, according to the lawsuit.

The site touts its "World Class" security features, stating that users maintain control of their assets because accounts can only be accessed by user-generated passwords, the suit says.

The "non-custodial" nature of the features "supposedly, makes the platform especially secure," according to the suit.

However, on Nov. 5, 2021, a bZx developer opened an attachment to a phishing email that allowed hackers access to every digital wallet that contained cryptocurrency using the Polygon and Binance Smart Chain blockchains, the complaint says. The third blockchain used by bZx, Ethereum, was unaffected, the suit says.

The as-yet-unknown developer employed by bZx, who had access to private passwords, was acting within the scope of his employment at the time of the hack, according to the complaint.

Who gets sued?

A DAO lacks a corporate structure. Each person who holds digital currency issued by a DAO can suggest actions that are then voted on by everyone else. Typical suggestions involve organization hires, distribution of funds and changes in organizational policy.

In late November, the bZx DAO voted on and approved a compensation plan for those affected by the hack, the complaint says.

For the first part of the plan, unassigned bZx digital currency — BZRX tokens — from the DAO's "treasury," or shared bank account, will be used to reimburse victims with a new token or with tokens that vest over time, according to the complaint.

The second part of the plan involves issuing debt tokens that would be paid back using 30% of future revenue, the suit says. On this schedule, full repayment would take thousands of years, the complaint alleges.

In December, users were encouraged to transfer from the bZx platform to the Ooki platform, and many of the BZRX tokens were "transformed" into OOKI tokens, the suit says. The complaint asserts that the Ooki DAO is the successor to the bZx DAO.

Although a DAO lacks a corporate structure by design, the suit notes that "there is another phrase in American law for that kind of arrangement: general partnership," in which two or more people carry on as co-owners of a business for profit.

The lawsuit names as defendants bZx co-founders Kyle Kistner and Tom Bean, bZx investors Hashed International LLC and AGE Crypto GP LLC, as well as the bZx and Ooki DAOs.

The plaintiffs, represented by Gerstein Harrow LLP, allege bZx was negligent in maintaining security for those who deposited funds with the DAO. They seek to represent a class of everyone who had cryptocurrency stolen in the Nov. 5 hack. They ask for compensatory and punitive damages, attorney fees and costs.

By John Fitzgerald

End of Document

Related topics

Data Privacy and Security
Corporate Governance
Investor Relations
Online and Mobile
Apps
Data Breach
Consumers
Product and Service Development
Security Providers
Cyber Threats and Attacks
Data Theft
Phishing
Litigation
Class Actions/MDL
Risk Management
Information Security Risk Assessment
Enforcement
Cybercrimes
Class Actions and MDL
Class Actions
Banking Finance

Electronic Funds Transfer
Online Banking
Litigation
Class Action
California
Related filings
Complaint: 2022 WL 1434198
Attorney profiles
Jason Harrow and Charles Gerstein; Gerstein Harrow LLP for Plaintiffs

