Professional Perspective

Cybersecurity Liability for Web3 Platforms: Key Issues and Risk Mitigation Solutions

Sasha Rosenthal-Larrea, Benjamin Gruenstein and Evan Norris, Cravath Swaine & Moore
Daniel Barabander, Variant

Bloomberg Law

Read Professional Perspectives | Become a Contributor
Reproduced with permission. Copyright © 2024 Bloomberg Industry Group, Inc.
800.372.1033. For further use, please contact permissions@bloombergindustry.com

Cybersecurity Liability for Web3 Platforms: Key Issues and Risk Mitigation Solutions

*Contributed by **Sasha Rosenthal-Larrea**, **Benjamin Gruenstein** and **Evan Norris**, Cravath Swaine & Moore*
***Daniel Barabander**, Variant*

While hacks of web3 platforms have long been a threat, the liability landscape web3 platforms face in the wake of these hacks is maturing—and expanding—quickly. There has been an overall increase in consumer lawsuits brought against a wide range of web3 players, and plaintiffs' lawyers are showing expected creativity in the types of claims they bring. This development is occurring in the context of increased regulatory enforcement and scrutiny, as well as investor lawsuits, across the broader technology industry—trends that are likely to catch up with web3 players soon enough.

As the liability exposure faced by web3 platforms grows, security technology to prevent or limit hacks is improving. However, web3 platforms should be aware that the availability of these new solutions will be accompanied by higher expectations from consumers, users and service providers regarding cybersecurity standards, and, as in any industry, standards of care that determine legal liability will evolve alongside innovation. Platforms and developers would do well to proactively deploy available security features on their platforms and ensure that their governance and compliance procedures are adequate and regularly updated and improved. To best select solutions and implement procedures closely tailored to their risk profile, platforms should be mindful of the potential liability they face from private and governmental actors following a cybersecurity-related exploit.

Exploits Across the Web3 Ecosystem

Before addressing the liability landscape, it is important to appreciate the breadth of strategies employed by hackers and the various aspects of the web3 ecosystem vulnerable to attack. Hackers have targeted on-chain and off-chain protocols and end users, as well as platforms such as wallet apps and exchanges. Users have fallen prey to predatory transactions and fraudulent tokens imitating legitimate tokens. Among other methods, there have been numerous "**address poisoning attacks**" involving attempts to "poison" a user's list of recent transaction addresses with addresses controlled by the attacker to induce the user into mistakenly sending funds to a fraudulent address, and attacks on code vulnerabilities in underlying protocols or associated decentralized applications ("dApps") have led to lost user funds.

Both the variety and the pace of attacks have remained high, with more than $473 million **lost** to hacks and frauds so far in 2024—in May 2024, $52 million was lost across 21 reported incidents. Two entities alone accounted for a significant amount of that May total, demonstrating the magnitude of attacks. Gala Games, a blockchain gaming platform, **lost** $21 million worth of tokens in May 2024 when a malicious actor compromised a long-dormant account with poor security, with the platform's founder attributing the hack to insufficient internal controls. Sonne Finance, a cryptocurrency lending protocol, lost more than $20 million in a **hack** that same month, although certain users were able to recover funds due to prompt detection of the hack.

The Liability Landscape

Most web3 platforms are becoming acutely aware of the increasingly sophisticated and frequent attacks they face. But how fully do they understand the types of liability that might result following each type of attack? This understanding is critical to identifying the security, governance and compliance steps that can be taken in advance to mitigate legal exposure in the event of a hack.

Often, hacks occur through exploitation of a centralized point of control of the platform. In this way, the occurrence and specifics of a hack can call regulators' and potential consumer plaintiffs' attention to points of control on a platform. This attention may lead to unwanted scrutiny in areas where evidence of control could affect the regulatory analysis the platform has been relying on. An **argument** that web3 platforms have put forth to show that they are not issuers of securities, operators of exchanges or custodians of user tokens is that the underlying protocol is decentralized and not controlled by the corporate entity. In addition, when consumer lawsuits are brought against web3 defendants, evidence of control or sufficient influence is important in determining liability for the platform's legal wrapper, principals, developers and other key figures. In these ways, cybersecurity incidents can add complexity for defendants relying on arguments based on decentralization because plaintiffs and regulators can point to hacks as an indication of control or influence to advance their claims.

©2024 Bloomberg Industry Group, Inc.

Consumer Lawsuits

Negligence of Web3 Platforms. Consumer class actions have been brought against web3 platforms—including exchanges, wallets, protocols and decentralized autonomous organizations ("DAOs")—in the aftermath of cybersecurity incidents. In class actions alleging negligence, plaintiffs must prove that a defendant owed a duty to its users (typically, a duty of care to protect user funds), that it breached its duty by acting unreasonably or failing to take reasonable protective actions, and that the platform's breach caused the loss of funds, information, or other assets. After large-scale hacks or breaches, consumer plaintiffs in negligence lawsuits often argue that defendants knew or should have known of specific vulnerabilities that had been identified by security auditors or other third-party reviewers. Plaintiffs then claim that the defendants had a duty to remedy those known vulnerabilities, and that these defendants breached that duty by failing to take reasonable measures such as deploying available detection and mitigation tools.

For example, in 2021, bZx protocol users lost approximately $55 million in crypto assets as a result of a phishing email that compromised a protocol developer's private key, enabling a hacker to transfer funds out of the protocol. Plaintiffs filed suit in California federal court, arguing that the bZx protocol and its partners owed users a duty to maintain the security of the protocol's funds, including security measures to prevent a multi-million-dollar theft from a phishing attack on a single developer. Plaintiffs alleged that the bZx protocol operators knew that security measures were reasonably necessary to protect the protocol, yet did not implement such measures, thereby breaching their duty. The court denied the defendants' motion to dismiss, and the parties ultimately reached a private **settlement**. *Sarcuni et al. v. bZx DAO et al.*, **664 F. Supp. 3d 1100** (S.D. Cal. Mar. 27, 2023).

In another ongoing case, consumer plaintiffs have relied on similar arguments about knowledge of necessary security measures. In June 2023, high volumes of unauthorized transactions were reported to the non-custodial decentralized wallet interface, Atomic Wallet. The hack breached at least 5,500 users' wallets and drained $100 million in crypto assets. Days later, Atomic Wallet users brought a consumer class action against the company in Colorado federal court. In their complaint, the plaintiffs emphasized that Atomic Wallet was put on notice of "serious 'existing security vulnerabilities' impacting the security of user wallets and funds" by security auditors, but did not take any measures to "inform users of those risks or protect against those risks." Among other issues, these vulnerabilities included a "lack of adherence to wallet system best practices and standards". The plaintiffs contended that Atomic Wallet owed a "duty to maintain the security of customer funds in Atomic Wallet wallets" and a "duty [to] secure against malicious attacks." The case is currently ongoing, with oral argument on motions to dismiss having recently been held on June 3, 2024. *Meany et al. v. Atomic Walletet al.*, 1:23-cv-1582 (D. Colo. June 21, 2023).

It is important to remember that the standard for establishing negligence is that a platform knew *or should have known* of security risks. So while the plaintiffs suing Atomic Wallet claimed the platform knew of specific vulnerabilities, Atomic Wallet would have been exposed to liability under a negligence theory even if it did not have that knowledge. A similar standard was applied in a separate class action brought against Coinbase. In that case, plaintiffs received phishing emails to change their Coinbase passwords, then had thousands of dollars drained from their accounts and transferred to hackers' wallets. As part of their negligence claim, plaintiffs alleged that Coinbase knew "or could readily determine" that the transactions in question were fraudulent. *Kattula v. Coinbase Glob., Inc.*, 1:22-cv-3250-TWT (N.D. Ga. Aug. 15, 2022). And indeed, in other cybersecurity-related lawsuits, plaintiffs have often **contended** that platforms should have known that their systems or data security practices were inadequate, regardless of whether they actually received notice of vulnerabilities.

Platforms' actions are often assessed against a "reasonableness" standard, based on what other similarly situated players in the same industry do when faced with the same risk. As security tools continue to improve, platforms may be required to provide, or take efforts to provide, a heightened level of security in order to avoid liability in negligence actions. Increasing standards for security will also impact the expectations of third parties. As security standards in the web3 and DeFi space continue to evolve, third parties that support the web3 and DeFi ecosystem—including insurers, advertisers and other service providers—may begin to require compliance with heightened security standards before they engage with or promote a platform. For example, wallet companies have begun requiring certain security assurances before connecting with tokens and dApps they view as risky. While platforms may not otherwise be moved to implement heightened security measures, they may be required to do so in order to freely operate in the web3 and DeFi ecosystem.

Breach of Contract and Breach of Fiduciary Duty. In addition to lawsuits alleging negligent behavior, consumers have brought breach of contract and breach of fiduciary duty claims following large-scale hacks and cyberattacks. These claims can be based on platforms' terms of use and any fiduciary responsibilities that arise from agreements that provide assurances about account security to users or customers. This liability risk increases when platforms do not actually have the technical solutions in place to back their security guarantees, but instead solely rely on vague formulations that claim to, for instance,

©2024 Bloomberg Industry Group, Inc.

adhere to industry standards. The class action against Coinbase described above also involved a breach of fiduciary duty claim. Prior to the phishing attacks, Coinbase had represented itself as maintaining robust security protocols, stating that it followed "Payment Industry Best Practices" on its website.

Following the phishing attacks, Coinbase customers brought suit alleging that Coinbase breached the implied covenant of good faith and fair dealing arising from its User Agreement contracts. Customers must consent to Coinbase's User Agreement upon creating their accounts and wallets on the platform. The plaintiffs argued that by failing to protect customer accounts, transactions and assets, and failing to respond to and resolve customer complaints regarding security threats and hacks in a timely manner, Coinbase breached its contractual obligation to act in good faith. Customers also alleged that Coinbase breached its fiduciary duty because it had represented and agreed that it would act as the secure custodian of funds and assets held in customer accounts. In 2023, a Georgia federal judge granted Coinbase's request for arbitration.

As the Coinbase case makes clear, while negligence claims will be evaluated based on what measures are considered reasonable or standard in the industry, security standards that arise from contractual and/or fiduciary duties owed by platforms to their customers can form the basis for additional theories of liability based on the same incident, especially if promises or representations are made without actual security tools to back them up. As such, web3 platforms should carefully evaluate any representations they make or obligations they take on in their terms of use or public disclosures, including marketing materials. Platforms should also develop controls as part of their compliance infrastructure to ensure that such representations are accurate and, most importantly, obligations are fulfilled by implementing trustworthy security measures. If cybersecurity incidents occur despite these precautions, web3 platforms can more successfully argue that they nonetheless adopted reasonable mitigation and security steps to protect user assets.

Securities Law Claims. Unlike web2 hacks, in which the affected parties are users or consumers, web3 hacks may result in another layer of liability due to users often also being holders of the web3 platform's native token. Token-holders and regulators can bring suit against the token-issuing platforms for violations of securities law, alleging that token-holders are *investors* in securities. Plaintiffs in at least one securities lawsuit brought by token-holders have sought rescissory damages. See *Amanda Houghton, et al. v. Compound DAO, et al.*, 22-cv-07781-WHO (N.D. Cal. Dec. 8, 2022).

Crypto tokens' potential designation as securities opens platforms up to this broad source of legal liability, which can be wielded directly by individual token-holders. For example, a lawsuit brought by token-holders against Uniswap alleged that the exchange facilitated dozens of scams by providing and allowing scam token issuers to engage in unlawful transactions by "soliciting, offering, and selling securities without registering the Tokens as securities and without Uniswap registering with the SEC as an exchange or a broker-dealer," in violation of securities law. *Risley v. Uniswap*, 1:22-cv-02780 (S.D.N.Y. Apr. 4, 2022). Two common types of crypto scams are "rug pulls"—wherein issuers of a new token place tokens into a pool in exchange for platform-issued liquidity tokens, then "pull" all their tokens from the pool, leaving other investors with now-worthless tokens—and "pump and dumps"—wherein issuers first send millions of new tokens to themselves, "pump" or promote their new token to investors, then "dump" their holdings at the highest possible valuation. Both of these common scams, as well as many other varieties, decrease the value of the tokens at issue, resulting in losses for investors who hold those tokens. These investor losses are the damages on which securities law claims are based and that expose platforms to potentially significant liability.

In addition, while rare right now, web3 platforms that go public can face securities law claims on behalf of their public investors based on insufficient or inaccurate disclosures relating to cybersecurity risk and mitigation measures. The investment community has been increasingly focused on cybersecurity, in part spurred by the SEC's 2023 rules on disclosure of cybersecurity risk, which required public companies to separately disclose material cybersecurity incidents and describe the company's process for managing material cybersecurity threats, as well as the SEC's recent enforcement actions. These risks have become more salient given the SEC's continued enforcement actions against companies engaging with tokens that have been alleged to be securities following its 2017 Report on DAO Tokens, in which the SEC **determined** that DAO Tokens were securities partly because "[w]hen the Attacker exploited a weakness in the code and removed investor funds, Slock.it and its co-founders stepped in to help resolve the situation."

As one example of enforcement, in 2023, the SEC settled charges with Blackbaud, a software provider, for misleading investors about a cybersecurity incident. The settlement included a cease-and-desist order and a $3 million civil penalty—three times the amount of a similar settlement in 2021. *In re Blackbaud Inc.*, Mar. 9, 2023 (Sec. Exch. Comm.). While Blackbaud had represented that the incident did not compromise bank account information or Social Security numbers, it discovered days later that these claims were erroneous—and failed to make corrective disclosure. As the SEC ramps up its cybersecurity scrutiny, elevated industry standards and rising civil penalties will likely follow. Web3 players would do well to implement effective

©2024 Bloomberg Industry Group, Inc.

cybersecurity governance measures, including an incident response plan and regular assessments—to effectuate prompt detection of incidents and accurate reporting—as well as proactive security solutions.

Other Regulatory Enforcement. In addition to the SEC, agencies at the state level are beginning to regulate cybersecurity risk aggressively, a development which has begun to impact the web3 ecosystem. The New York Department of Financial Services ("NYDFS") has been particularly active in bringing regulatory enforcement actions against web3 platforms for cybersecurity and consumer protection violations, as well as for having inadequate transaction monitoring systems. Regulated entities under the NYDFS's Cybersecurity and Virtual Currency Regulations—including web3 players with Virtual Currency and Money Transmitter licenses—are **required** to implement risk-based cybersecurity programs, report certain cybersecurity events and certify annual compliance with the regulations. In 2023, the NYDFS reached a settlement with bitFlyer USA, a custodial wallet provider, for failing to implement an adequate cybersecurity program and for failing to customize its policies to the platform's needs and risks. As part of the settlement, bitFlyer committed to a $1.2 million penalty and a significant remediation of its cybersecurity program. *In re Bitflyer USA, Inc.* (N.Y. Dep't Fin. Serv. May 1, 2023).

Shareholder Derivative Claims. Finally, any company that has crypto-related offerings or functionalities (and not just web3 platforms themselves) may face increasing shareholder derivative litigation over their cybersecurity governance and for failures to maintain adequate cybersecurity measures around these specialized offerings. In the cybersecurity context, shareholder derivative suits allow the shareholders of a company to sue corporate directors and officers for damages to the company that they allege flowed from their failure to adequately oversee cybersecurity risks. Web2 companies have faced claims from derivative plaintiffs that allege the board failed to take action with respect to "red flags" showing that internal controls were inadequate to prevent a data breach. In a Home Depot hack in 2014, malicious actors compromised email addresses and credit card accounts of around 56 million Home Depot customers. *In re Home Depot, Inc., Customer Data Sec. Breach Litig.*, 1:14-md-02583-TWT (N.D. Ga. May 17, 2016). In a subsequent lawsuit, shareholders alleged in a derivative suit that the company's current and former directors and officers breached their duty of loyalty by failing to institute internal controls sufficient to monitor cybersecurity risk. *In re The Home Depot, Inc. S'holder Derivative Litig.*, No. 1:15-cv-2999-TWT (N.D. Ga. Nov. 30, 2016). In recent years, shareholder derivative suits have continued, with shareholders alleging that the company in which they were invested failed to maintain an effective control system even after hackers repeatedly exploited cybersecurity weaknesses, ranging from software bugs to unrestricted access to servers. In settling lawsuits alleging data breaches, some companies have committed to address cybersecurity vulnerabilities that resulted in the breach. *In re T-Mobile Customer Data Sec. Breach Litig.*, 4:21-md-03019-BCW (W.D. Mo. July 22, 2022). These lawsuits highlight the need to improve cybersecurity across the board: technology, governance and compliance.

Emerging Solutions

We have described the cybersecurity risks and liabilities that web3 platforms face in the event of a cybersecurity incident. So, how can parties mitigate their risk?

Naturally, the best way to avoid liability is to prevent the exploits in the first place, through tools that allow companies to proactively scan for malicious actors. Security tools like Blockaid can now identify malicious dApps, tokens, transactions and wallet addresses using a combination of on-chain and off-chain data, and web3 platforms such as Coinbase and MetaMask have begun integrating such security features to enhance user safety. Centralized exchanges can also scan for malicious wallet addresses to block withdrawals to such addresses following phishing attacks targeting exchange users.

More sophisticated hacks may do more than divert assets to malicious wallet addresses—bad actors can take advantage of loopholes or other vulnerabilities in existing smart contracts to execute transactions that do not match what is displayed to the user. To protect against such hacks, wallets and dApps can integrate solutions that simulate transactions dictated by the smart contract code, which can thereby warn the user of potential dangers before the user signs a transaction that executes in a way unintended by the user. Platforms can even integrate solutions that differentiate between legitimate and potentially harmful tokens so that such tokens are flagged and not shown to the user. These preventative security detection capabilities are made possible through security vendors conducting advanced scanning and analysis of on- and off-chain data. By leveraging such security measures, platforms can not only enhance user safety, but also demonstrate their active efforts to prevent harmful exploits in the face of potential risks.

Integration of proactive security solutions will mitigate many of the most common crypto hacking and fraud tactics. In terms of liability, these measures also allow web3 platforms to argue that they have met the duty of care owed to their users, and have adopted reasonable security measures to mitigate against cybersecurity risk as standards of care continue to evolve. If

©2024 Bloomberg Industry Group, Inc.

exploits nevertheless occur, platforms may be able to argue that assets were lost due to negligence on the part of users who did not heed the warnings, or that the hacks were beyond the level of protection reasonably expected from the company.

Conclusion

Web3 companies are currently operating in an uncertain regulatory environment, where hacks can act as a lightning rod for litigation and regulatory enforcement. Unlike traditional web2 platform hacks that primarily lead to consumer cybersecurity lawsuits, web3 platform hacks can also attract securities claims brought by private litigants, and regulatory enforcement by state and federal regulators, in addition to the typical cybersecurity consumer lawsuits seen in web2. The wisest course of action available for web3 and DeFi platforms is to implement strong, preventative measures to protect the security of the platform and the safety of its users.

©2024 Bloomberg Industry Group, Inc.