Bloomberg Law News 2022-09-12T15:18:39651137589-04:00

Staying Ahead of Cryptocurrency Hacks and Legal Risks

2022-09-12T04:00:28000-04:00

Over $14 billion in cryptocurrency was lost to cybercrimes in 2021, followed by billions more this year. These staggering losses underscore the need to understand and stay ahead of security threats and legal risks facing the crypto industry.

Types of Threats

As blockchain technologies reduce friction for decentralizing financial infrastructure and other novel use cases, they also present an attractive target for threat actors that exploit the evolving industry's nascent security controls.

Private Key Theft. Many crypto holders store their own keys in hot (software) wallets or cold (physical hardware) wallets. Whoever holds the private keys controls the crypto asset. The security of the keys is only as good as the security of the person or entity holding them.

Blockchain immutability makes on-chain transactions irreversible, in contrast to transactions in the traditional financial system, which rely on financial institution intermediaries that can freeze funds and reverse transactions.

Even where a third-party exchange keeps custody of keys on users' behalf, hackers have penetrated systems to haul away funds. This March, for instance, hackers compromised private keys associated with the Axie Infinity crypto game and stole more than $600 million in crypto. The US Treasury Department linked the attack to North Korea's state-sponsored Lazarus Group and listed the wallet address used to steal funds in its Specially Designated Nationals List.

Software Exploitation. Traditional banks are no strangers to software exploits. Now, hackers are turning to crypto. Many crypto hacks in the last year took advantage of vulnerabilities in the code used to process smart contracts or underlying crypto software.

In the Poly Network attack, for example, a hacker exploited a smart contract vulnerability that allowed

them to change administrative permissions for executing blockchain transactions, allowing theft of hundreds of millions of crypto assets.

Scams and Fraud. Scammers have defrauded tens of thousands of consumers to the tune of more than $1 billion in crypto since 2021, according to the Federal Trade Commission. Such scams offer fake investment opportunities, prey on those seeking romance, or involve impersonation of legitimate businesses. Rug pulls are another scam where a creator will sell tokens, collect funds, promise a future launch, but then abscond with the funds.

Legal Risks and Practical Tips

Regulatory Scrutiny. Regulatory actions following software vulnerabilities have been brought with some frequency outside of the crypto industry.

Equifax, for example, settled with the FTC, Consumer Financial Protection Bureau, and 50 state attorneys general for more than $500 million for failure to resolve software vulnerability issues.

Regulators are now setting their sights on the crypto industry's cybersecurity controls. President Joe Biden's March 2022 crypto executive order directs the government to "prioritiz[e] ... security [and] combat[] illicit exploitation" of digital assets.

The FTC is monitoring crypto scams, foreshadowing potentially forthcoming enforcement actions. New York's Department of Financial Services recently emphasized that cybersecurity controls expected of traditional financial institutions apply to crypto businesses under DFS' jurisdiction.

In August, the Office of Foreign Assets Control sanctioned the Tornado Cash mixer, allegedly used to launder $7 billion from crypto hacks, after sanctioning Blender.io earlier this year. These OFAC actions create compliance challenges for entities that may have interacted with the sanctioned blockchain addresses or platforms.

Law Enforcement Prioritization. DOJ's efforts in crypto this year already resulted in its largest-ever financial seizure—$3.6 billion in crypto linked to a 2016 hack of the Bitfinex virtual currency exchange.

On June 30, the DOJ also announced charges against six defendants allegedly involved in an NFT rug-pull scam, and a fraudulent initial coin offering. The FBI, on the same day, added the "Cryptoqueen" to its Ten Most Wanted Fugitives list based on an alleged $4 billion fraud scheme involving "OneCoin."

In light of the regulatory and law enforcement focus, organizations would be prudent to develop policies and procedures for incident investigation, remediation, and response.

Scoping out risks and documenting a response plan can prepare an organization to act quickly and efficiently when an incident occurs. The $600 million Axie Infinity hack illustrates the benefits of optimizing detection and response, as the six days that passed before the attack was uncovered resulted in additional losses.

Due to challenges tracing transactions, law enforcement cooperation can pay dividends as well. Following victim cooperation, DOJ and the FBI have recovered funds transacted through blockchains in the ransomware context.

Private sector cooperation can help, too. Several vendor-built and community-driven tools exist for reporting hacks and malicious crypto attacks, and private sector efforts have led to successful law enforcement action against criminal hackers.

Civil Litigation Claims. Security incidents expose crypto platforms to litigation risk as well. Litigants have alleged that crypto exchanges were negligent in not preventing unauthorized account transactions or in identifying criminal proceeds that malicious actors were allegedly moving through an exchange.

Even traditional companies face litigation risk following cryptocurrency hacks.

Two major cellular providers, for instance, faced cases alleging that their purported negligence resulted in SIM-swap attacks that stole millions in crypto.

Takeaways for Crypto Businesses

Hackers are reaping billions of dollars in profits by attacking crypto organizations.

Regulators have long focused on enforcement against companies with inadequate cybersecurity protections, and are poised to bring such actions in the cryptocurrency context.

Given the wide-ranging threats, crypto organizations should focus on establishing a foundation of strong cybersecurity processes and innovations.

This article does not necessarily reflect the opinion of The Bureau of National Affairs, Inc., the publisher of Bloomberg Law and Bloomberg Tax, or its owners.

Write for Us: Author Guidelines

Author Information

Alex Iftimie is partner and co-chair of Morrison & Foerster's Global Risk + Crisis Management practice group. He is a former Department of Justice national security official. He is based in San Francisco.

Michael Burshteyn is an attorney at Morrison & Foerster in San Francisco. He is outside counsel to crypto companies, litigates crypto and data security disputes, and previously founded a cybersecurity startup.