"Navigating the Complex Intersection of Cryptocurrency, Cybercrime, and Privacy: Challenges and Solutions for Law Enforcement and Regulation"

Jason T. Ghetian, CryptoAware.ai, March 3, 2025

About the author:

With an extensive background in both cyber and law enforcement, Jason Ghetian bring over two decades of experience in tackling complex cases at the intersection of technology, fraud, and criminal activity. His academic qualifications include a Master of Science in Cybersecurity Engineering from the University of Southern California, alongside a Bachelor of Science in Mechanical Engineering from the United States Military Academy at West Point. He serves as the President of Cyber Asset Recovery Experts Inc. that focuses on cryptocurrency fraud investigations and Vice-President of Product Development for CryptoAware, an analytical software in the cryptocurrency space. As a Special Agent with the FBI, he led high-profile cybercrime investigations, including the "Pig Butchering" cryptocurrency scam, and established the Orange County Cyber Task Force. His expertise spans digital forensics, international cybercrime, and terrorism investigations, complemented by numerous awards and certifications in the cybersecurity field.

According to the Federal Bureau of Investigation's (FBI) 2023 Cryptocurrency Fraud Report, the Internet Crime Complaint Center (ic3.gov) received "*more than 69,000 complaints from the public regarding financial fraud involving the use of cryptocurrency, such as bitcoin, ether, or tether. Estimated losses with a nexus to cryptocurrency totaled more than $5.6 billion. While the number of cryptocurrency-related complaints represents only about 10 percent of the total number of financial fraud complaints, the losses associated with these complaints account for almost 50 percent of the total losses.*" Topping the list is cryptocurrency investment scams which equate to 71% of all losses related to cryptocurrency. However, hacks of exchange wallets are on the rise like those of Chainalysis and most recently, ByBit.

What exacerbates the situation—and is rarely reported—is that federal, state, and local law enforcement agencies are completely overwhelmed by the surge in cybercrime. Years ago, as cybercrime in the U.S. skyrocketed, the FBI's Cyber Division shifted most cyber-enabled financial fraud cases to the White Collar Division, which had more resources. This allowed Cyber Division to focus on more complex threats like ransomware and remote access tools (RATs).

However, this transition came with significant challenges. The Criminal Division, which oversees White Collar investigations, lacked the specialized training and tools needed to investigate cybercrime effectively. Likewise, federal prosecutors suddenly tasked with handling these cases were ill-prepared to prosecute highly technical, international cybercriminals. As is often the case, the U.S. government moves slowly, and the FBI was no exception—leaving law enforcement struggling to keep pace with cybercriminals who exploit these inefficiencies.

As any business leader knows, you get what you measure. For white-collar FBI agents and prosecutors, success is often quantified by indictments, arrests, convictions, and sentences. This measurement system creates a disincentive to pursue cyber-enabled crimes, which are far more complex and resource-intensive than traditional financial fraud.

Cybercriminals operate within a labyrinth of digital infrastructure, shielded by privacy laws that make identification exceedingly difficult. To convict an overseas perpetrator, prosecutors must prove beyond a reasonable doubt—including establishing *mens rea* (criminal intent)—that the person behind the keyboard committed the crime. However, in cybercrime cases, the usual investigative tools such as interviews, device seizures, surveillance, public databases, and search warrants are largely unavailable.

Further complicating matters, foreign cooperation is often elusive. In schemes like Pig Butchering, perpetrators often operate under the protection of corrupt governments—such as Cambodia—that refuse to assist in investigations. Even when cybercriminals are identified, extradition is rare and, when pursued, can take up to a decade.

Faced with these barriers, investigators and prosecutors naturally prioritize cases involving U.S.-based offenders, even if the financial impact of those crimes is significantly lower. In the eyes of government officials, an indictment is an indictment, and a sentence is a sentence—regardless of the crime's scope.

Unfortunately, the internet is filled with victims of cyber-enabled financial crime who receive little to no assistance from law enforcement—many don't even get a call back. With no recourse, they are forced to accept their losses. For the elderly, this often means losing a lifetime of savings and being forced back into the workforce. Others, overwhelmed by the shame and devastation of being deceived, see no way forward and take their own lives.

Blaming law enforcement alone is an oversimplification. While agencies could enhance their efforts through AI-powered investigative tools, they do not control their own staffing levels or resources. Investigating and prosecuting 69,000 cryptocurrency-related cases is an immense challenge, made even more difficult by the global nature of cybercrime.

On February 21, 2025, the Democratic People's Republic of Korea (North Korea) orchestrated the theft of approximately $1.5 billion USD in virtual assets from the cryptocurrency exchange Bybit. The FBI classifies this specific North Korean cyber operation as "TraderTraitor." [1] The TraderTraitor actors have been moving swiftly, converting portions of the stolen assets into Bitcoin and other cryptocurrencies, distributing them across thousands of blockchain addresses. These assets are expected to undergo further laundering before ultimately being converted into fiat currency. According to Glassnode, the breach triggered widespread panic withdrawals, resulting in total exchange outflows of approximately $4.3 billion across Bitcoin and stablecoins. Market sentiment declined sharply, leading to a broad sell-off. Bitcoin's monthly performance

[1] Federal Bureau of Investigation. (2025, February 26). *FBI issues PSA on the emerging threat of TraderTraitor*. Internet Crime Complaint Center. https://www.ic3.gov/PSA/2025/PSA250226#:~:text=The%20Federal%20Bureau%20of%20Investigation,TraderTraitor

plummeted -13.6%, while Ethereum (-22.9%), Solana (-40%), and Meme Coins (-36.9%) erased months of gains, effectively resetting market momentum to April 2024 levels[2].

Investigations revealed that the breach originated from a supply chain attack targeting Safe{Wallet}, a multisignature wallet platform used by Bybit. The attackers compromised a developer's machine within Safe{Wallet}, enabling them to manipulate the wallet's functionalities. During a routine transfer from Bybit's Ethereum cold wallet to a hot wallet, the attackers exploited their access to execute unauthorized transactions. They crafted a malicious transaction, which was inadvertently signed by Bybit, allowing them to siphon approximately 401,000 ETH—valued at nearly $1.5 billion at the time—into wallets under their control.

Following the theft, the hackers employed sophisticated laundering techniques to obscure the stolen assets' origins. They dispersed the ETH across a web of intermediary wallets, converting large portions into Bitcoin (BTC) and DAI. The laundering process leveraged decentralized exchanges (DEXs), cross-chain bridges, and no-KYC instant swap services, further complicating asset tracing.

Despite the overwhelming cyber-crime losses involving cryptocurrency, U.S. regulators appear to be going in the wrong direction. On the same day as the Bybit hack, Coinbase announced that the Securities and Exchange Commission (SEC) would be dropping its enforcement action against the company—the largest case against a cryptocurrency exchange for alleged failure to meet registration requirements[3]. That same day, OpenSea, the largest NFT marketplace, revealed that the SEC had also decided to drop its investigation into its operations. Three days later, Robinhood announced that the SEC had likewise closed its investigation into the company.

The tradeoff between security and privacy is a longstanding debate, particularly in areas such as cybersecurity, financial regulations, and law enforcement. Striking the right balance between the two is crucial, as prioritizing one often comes at the expense of the other. Security measures are designed to protect individuals, businesses, and governments from threats such as cybercrime, fraud, and terrorism. However, implementing stringent security often requires compromising privacy, as it involves increased surveillance, data collection, and monitoring of personal and financial activities. On the other hand, prioritizing privacy means limiting the extent to which security agencies, corporations, or governments can monitor individuals. While this ensures greater personal freedoms and data protection, it may also create loopholes that criminals can exploit.

In the case of financial institutions (FIs) and crypto exchanges, implementing strict Know Your Customer (KYC) and Anti-Money Laundering (AML) measures enhances security by preventing fraud and illicit transactions. However, these measures require individuals to reveal personal information, reducing their financial privacy. Some crypto users argue that excessive regulation

---

[2] Glassnode. (2025, February 26). *The week on-chain: Week 08, 2025*. Glassnode Insights. https://insights.glassnode.com/the-week-onchain-week-08-2025/#:~:text=,the%20realized%20supply%20"air%20gap"

[3] Sullivan & Cromwell LLP. (2025, February 26). *SEC withdraws from prominent crypto enforcement amid regulatory shift*. Corporate Securities Law Blog. https://www.corporatesecuritieslawblog.com/2025/02/sec-withdraws-from-prominent-crypto-enforcement-amid-regulatory-shift/

undermines the decentralized and anonymous nature of blockchain technology. Similarly, governments use surveillance programs, such as mass data collection and AI-powered monitoring, to detect and prevent threats like cybercrime and terrorism. While this improves security, it also raises concerns about personal freedoms, data misuse, and potential government overreach. Messaging apps like Signal and WhatsApp use end-to-end encryption to ensure privacy. However, law enforcement agencies argue that encryption makes it difficult to track criminal activities, leading to debates over whether companies should provide "backdoor" access to authorities.

Finding a middle ground between security and privacy is the burden of our times. It involves ensuring security measures are clearly defined and do not excessively infringe on individual rights. Companies and governments should be selective in collecting only necessary data rather than mass surveillance. Exploring privacy-focused security measures, such as Zero-Knowledge Proofs in crypto transactions, which allow verification without exposing personal information. Finally, educating individuals about best practices in both cybersecurity and data privacy to empower informed decision-making. Ultimately, the balance between security and privacy depends on context—whether in cryptocurrency, law enforcement, or technology. A thoughtful approach is needed to ensure both safety and personal freedoms are protected.

Private and government entities should, at the very least, implement advanced software capable of quickly and efficiently analyzing public blockchains and private exchange records, obtained through legal processes, to track stolen cryptocurrency assets in real time. Additionally, no-KYC instant swap services should be made illegal, as they violate basic AML laws. Even the most staunch privacy advocates would likely change their stance if they personally became victims of cybercrime and found that nothing could be done to recover their stolen assets.

In conclusion, the rapid growth of cryptocurrency-related fraud and cybercrime poses significant challenges for law enforcement, regulators, and victims alike. While cryptocurrency's decentralized nature offers privacy and security benefits, it also creates fertile ground for exploitation by cybercriminals. The overwhelming number of cases and the complex international landscape hinder effective prosecution and recovery efforts. The tradeoff between security and privacy remains a critical issue, as stricter regulations could either help prevent cybercrime or undermine the principles of decentralized systems. To strike an appropriate balance, both private and government entities must adopt more advanced technologies, enforce stronger anti-money laundering measures, and ensure that privacy protections do not shield criminals. Ultimately, finding a middle ground that fosters both security and privacy will require thoughtful collaboration and innovative solutions to address the growing threat of cybercrime in the cryptocurrency space.