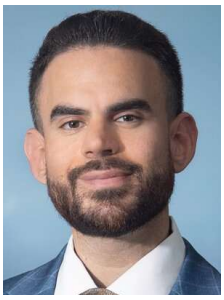
Where Crypto Mixing Enforcement Is Headed From Here

By **David Tarras** (November 17, 2025)



David Tarras

In August, a federal jury in the U.S. District Court for the Southern District of New York convicted Roman Storm, co-founder of the cryptocurrency mixer Tornado Cash, of conspiring to operate an unlicensed money-transmitting business that moved more than $1 billion in criminal proceeds.[1]

Prosecutors in U.S. v. Storm described Storm as having "provided a service for North Korean hackers and other criminals to move and hide more than one billion dollars of dirty money."[2] The Tornado Cash case unfolded against a dramatically shifting political backdrop.

Just four months earlier, Deputy Attorney General Todd Blanche issued his now-defining memorandum titled "Ending Regulation by Prosecution." The April directive fundamentally reshaped the federal government's approach to digital asset enforcement by declaring that the U.S. Department of Justice is not a financial regulator and that its role in the crypto space must focus on true criminal intent rather than regulatory noncompliance.[3]

The Tornado Cash case, therefore, stands as a turning point. It can be viewed as symbolic of the end to the Biden-era "war on crypto." But it also confirmed that enforcement against those who knowingly facilitate criminal conduct remains a central DOJ priority.

Tornado Cash as the First Test Case

As the U.S. Secret Service explained in its May "Public Advisory on Cryptocurrency Mixers," mixers, sometimes called "tumblers," are services that pool digital assets from many users and then redistribute them in random quantities to obscure the trail of ownership.[4]

The Tornado Cash mixer, founded in 2019, was a decentralized protocol that used zero-knowledge proofs to enable private transactions without revealing the identity of senders or recipients.

Users deposited cryptocurrency into Tornado Cash smart contracts, which then redistributed the same amount of value to a new address, effectively breaking the public blockchain link between the original wallets.

Because the protocol was open source and operated autonomously, it had no centralized custodian or identifiable "operator" in the traditional sense.

Nevertheless, prosecutors charged Storm and his co-founders with conspiring to commit money laundering, violating sanctions and operating an unlicensed money transmitting business.

They alleged that Tornado Cash had facilitated the laundering of more than $1 billion in criminal proceeds, including hundreds of millions stolen in the "Ronin hack" attributed to North Korea's Lazarus Group.

Initially, the indictment was filed under the pre-Blanche enforcement paradigm, treating Tornado Cash's failure to register with the Financial Crimes Enforcement Network as a

stand-alone crime.

After Blanche issued his memorandum, prosecutors quietly narrowed the case. By May 2025, the government had dropped the count alleging failure to register as a money service business under Title 18 of the U.S. Code, Section 1960(b)(1)(B), and proceeded only on the subsection that requires proof that the defendant knew the transmitted funds were derived from a criminal offense or were intended for unlawful use.

That revision aligned Tornado Cash with the DOJ's new philosophy. When the case went to trial, prosecutors focused on Storm's knowledge that Tornado Cash was being used to launder money. They presented evidence that he continued to operate the protocol after public reports linked it to North Korean hacking operations.

The defense argued that Tornado Cash was a neutral privacy tool, comparing it to encrypted messaging apps that can be used by criminals and law-abiding users alike.

After a four-week trial, the jury convicted Storm of conspiring to operate an unlicensed money transmitting business under Section 1960(b)(1)(C) but deadlocked on the money-laundering and sanctions-conspiracy counts, a significant victory for the defense.

The mixed verdict can be viewed as a reflection of a more narrow prosecutorial theory encouraged by Blanche's directive, where overt evidence of intent and knowledge are at the evidentiary forefront of the prosecution's case-in-chief.

The Shift From "War on Crypto" to "Targeted Accountability"

The federal government's tone toward digital assets has softened considerably. President Donald Trump's pardon of Binance founder Changpeng Zhao, who had served a short sentence for anti-money laundering violations, symbolized the administration's stated end to the so-called war on crypto.[5]

White House statements framed Zhao as a victim of overzealous regulation under the prior administration. The same period saw pardons for the founders of BitMEX and clemency for Ross Ulbricht of Silk Road fame.

While critics viewed these acts as politically motivated, they also aligned with the Blanche memo's principle that digital asset innovation should not be criminalized absent fraud, exploitation or willful misconduct.

Importantly, this leniency does not extend to all corners of the crypto world. The DOJ has continued to bring major cases where digital assets are used to enable serious crimes.

In October, the department announced the largest forfeiture in its history, roughly $15 billion in bitcoin, against Chen Zhi, the Cambodian chairman of the Prince Group, accused of running forced-labor compounds engaged in massive crypto investment scams.[6]

That case, which alleges human trafficking, torture and industrial-scale fraud, demonstrates that enforcement remains vigorous when crypto intersects with organized criminal activity.

Thus, the phrase "war on crypto is over" should not be misread as a blanket amnesty. Rather, it represents a narrowing of focus, from criminalizing the infrastructure of crypto itself to prosecuting those who knowingly weaponize it.

What the Data Show: Mixers Are Declining, Exchanges Are Rising

While Tornado Cash dominated headlines and constituted a significant win for the defense (avoiding convictions on all of the most serious charges), blockchain analytics reveal a larger shift in laundering behavior.

According to the 2025 Chainalysis Crypto Crime Report, the total volume of illicit cryptocurrency transactions in 2024 reached approximately $41 billion, though that figure represented only 0.14 percent of all on-chain activity.[7]

The report highlights two key trends. First, the use of mixers for ransomware laundering activities declined dramatically in 2024, when law enforcement actions dismantled or sanctioned several major services, including ChipMixer,[8] Tornado Cash and Sinbad.[9]

Mixers had historically processed 10% to 15% of ransomware proceeds, but by late 2024, that share had fallen sharply.

Second, and perhaps more importantly, centralized exchanges remain principal gateways for converting illicit crypto into fiat currency. As one October analysis from CoinDesk put it, "centralized exchanges are still criminals' favorite crypto money-laundering tool."[10]

Despite mandatory know-your-customer programs, these exchanges account for the majority of cash-out points for ransomware, scams and fraud schemes. Many are located in permissive jurisdictions with lax enforcement.

The same report observed that the DOJ's 2023 settlement with Binance exposed systemic compliance failures that allowed sanctioned and criminal entities to transact freely through the platform. BitMEX's $100 million penalty under the Bank Secrecy Act further illustrates the risks facing major exchanges that treat compliance as a formality rather than a core function.

The lesson for practitioners: While mixers have drawn the public's ire, centralized exchanges continue to represent the true bottleneck where illicit crypto becomes real-world money.

Takeaways for Attorneys in the Crypto Compliance Space

The evolving enforcement landscape carries several practical implications for lawyers representing digital-asset clients and for compliance officers in the industry.

Intent and knowledge are paramount.

In light of Blanche's policy, prosecutorial focus will be on cases in which they can prove beyond a reasonable doubt that defendants knew they were handling or transmitting illicit funds.

This elevates the importance of documenting compliance efforts and due diligence protocols. Developers of decentralized platforms should be able to demonstrate that they neither had control over nor knowledge of specific transactions involving criminal proceeds.

Technical registration failures are insufficient.

Failure to register as a money service business — once a DOJ focus due to ease of proof —

now lacks charging-decision weight unless accompanied by substantial proof of willfulness or knowledge.

For counsel defending digital asset clients, this provides new grounds to challenge indictments and negotiate favorable resolutions.

National security cases remain a top priority.

The Tornado Cash case and the Sinbad indictments both involved alleged links to North Korea's Lazarus Group, a designated foreign-terrorist entity.

Such cases fit squarely within Blanche's stated enforcement priorities, which target the use of digital assets in terrorism, cartel activity or human trafficking. Attorneys should anticipate robust coordination between the DOJ, the Office of Foreign Assets Control and international partners in these matters.

Asset forfeiture will remain aggressive.

Even as the DOJ narrows its charging focus, it is expanding its use of civil and criminal forfeiture to recover stolen crypto.

The Prince Group's $15 billion dollar bitcoin seizure demonstrates that asset recovery is now central to crypto enforcement strategy. Counsel must be prepared to navigate parallel civil forfeiture proceedings even when criminal exposure appears limited.

Compliance programs are not optional.

Although the memo largely shields good faith actors, it also places a premium on proactive compliance.

Firms must maintain transaction-monitoring systems, screen wallet addresses against sanctions lists and establish escalation protocols for suspicious activity. In this new enforcement environment, ignorance may be a defense only if it is accompanied by diligence.

For attorneys advising clients in the digital asset sector, the key takeaway is that federal enforcement is becoming both narrower and deeper. It is narrower in that technical missteps no longer guarantee prosecution, but deeper because the cases that remain will be more complex, data-driven and often international in scope.

The Tornado Cash trial also reminds the defense bar that narratives matter. The government framed the case as one about protecting victims and national security, not about punishing privacy technology.

Defense counsel must be prepared to counter that framing with evidence of legitimate use, transparency and cooperation.

A New Enforcement Equilibrium

In many ways, Tornado Cash is the bridge between two philosophies. Under the old paradigm, the DOJ frequently charged digital-asset innovators with technical violations, using enforcement to shape industry norms. Under Blanche's directive, that approach is over. Now, enforcement targets knowledge and intent, not innovation itself.

However, Tornado Cash also underscores that ignorance cannot be feigned. Developers who become aware that their tools are being exploited for crime have a duty, legally or at least ethically, to take action.

Prosecutors will likely focus future cases on post-knowledge conduct: Did the developer update code, warn users or implement mitigation measures once illicit use became apparent?

Going forward, crypto enforcement will likely adopt a dual-track model.

The first track will pursue knowing facilitation of crime, such as laundering for ransomware groups, terrorist financing or human-trafficking rings.

The second track will focus on fraud and investor protection, targeting deceptive conduct that causes direct financial harm. Tornado Cash fits the first category, while the Prince Group and similar scams fall into the second.

The future of crypto enforcement is not deregulation but differentiation. The Tornado Cash verdict demonstrates that the DOJ's shift away from regulation by prosecution does not mean immunity for the crypto industry. Instead, it arguably reflects a more mature approach that balances innovation with accountability.

Developers who design privacy tools without criminal intent are unlikely to face prosecution merely for creating them. But those who knowingly enable the concealment of illicit funds will remain targets, regardless of how decentralized their technology appears.

In a post-Blanche world, the line between lawful innovation and criminal facilitation is no longer blurred by regulatory uncertainty. It is drawn clearly by intent, knowledge and response.

The "war on crypto" may be over, but the battle for integrity in digital asset markets has only just begun.

David Tarras is the founding attorney at Tarras Defense.

[1] U.S. Department of Justice, Founder Of Tornado Cash Crypto Mixing Service Convicted Of Knowingly Transmitting Criminal Proceeds (S.D.N.Y. Aug. 6, 2025).

[2] Internal Revenue Service, Founder of Tornado Cash Crypto Mixing Service Convicted of Knowingly Transmitting Criminal Proceeds (Aug. 6, 2025).

[3] Deputy Attorney General Todd Blanche, Memorandum: Ending Regulation by Prosecution (Apr. 7, 2025).

[4] U.S. Secret Service, Public Advisory on Cryptocurrency Mixers (May 2025).

[5] WIRED, "War on Crypto Is Over": Donald Trump Pardons Binance Founder CZ (Oct. 23, 2025).See United States v. Zhao, No. 23-cr-151 (W.D. Wash. Apr. 30, 2024).

[6] U.S. Department of Justice, Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes (E.D.N.Y. Oct. 14, 2025). U.S. Department of Justice, Operators of Cryptocurrency Mixers Charged with Money Laundering (N.D. Ga. Jan. 10, 2025).

[7] Chainalysis, 2025 Crypto Crime Report (Feb. 2025).

[8] U.S. Dep't of Justice, Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer That Processed Over $3 Billion in Transactions (Mar. 15, 2023), https://www.justice.gov/archives/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3.

[9] United States v. Ostapenko et al, No. 1:25-CR-001 (N.D. Ga. Oct. 2025).

[10] CoinDesk, Centralized Exchanges Are Still Criminals' Favorite Crypto Money Laundering Tool (Oct. 20, 2025).