



Portfolio Media, Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

'Pig Butchering' Seizure Is A Milestone In Crypto Crime Fight

By **David Zaslowsky** (August 4, 2025, 5:19 PM EDT)

The world of cryptocurrency, for all its revolutionary potential, has also become a fertile ground for sophisticated scams. Among the most insidious and financially devastating is the so-called pig butchering scheme, a form of investment fraud that preys on human trust and emotional vulnerability.

However, a recent operation, **announced** in June, led by the U.S. Secret Service and resulting in the seizure of over \$225 million in cryptocurrency, marks a significant turning point in the global fight against these elaborate criminal enterprises.

This landmark seizure of cryptocurrency, the largest in the U.S. Secret Service's history, not only represents a massive financial blow to scammers but also highlights the critical role of collaboration between law enforcement and the crypto industry.



David Zaslowsky

Understanding the Pig Butchering Scam

"Pig butchering," or "Sha Zhu Pan" in Chinese, is a long-con investment fraud in which criminals build fake romantic or business relationships with their targets over weeks or even months. The "pig" refers to the victim, who is "fattened" with fabricated trust and promises of high returns before being "butchered," or stripped of their assets.

Once a relationship is established, the scammers subtly introduce the idea of a lucrative cryptocurrency investment, often directing victims to sophisticated, yet entirely fraudulent, trading platforms.

Victims are initially encouraged to invest small amounts, which may even show fabricated profits, to build confidence. As trust deepens, victims are manipulated into investing increasingly larger sums, often their life savings, until suddenly, all access to their funds is cut off.

These operations are often run out of so-called scam compounds in Southeast Asia, where trafficked individuals are forced into cyber slavery to execute these frauds.

The devastating impact of these scams is evident in the staggering losses reported globally. In 2024 alone, cryptocurrency investment fraud, largely driven by pig butchering schemes, caused over \$5.8 billion in reported losses in the U.S., according to the complaint.

The anonymity and cross-border nature of cryptocurrency transactions have historically made these scams incredibly challenging to investigate and prosecute, allowing criminal syndicates to operate with relative impunity.

The Historic Seizure: A Collaborative Effort

This recent \$225 million asset seizure is a testament to the evolving capabilities of law enforcement and the crucial role that crypto companies are now playing in combating illicit activities. The operation involved a multipronged approach, leveraging advanced blockchain analysis and significant cooperation from major cryptocurrency players.

The investigation began in late 2023 when Tether, the issuer of the USDT stablecoin, proactively froze 39 wallet addresses containing \$225 million in stolen USDT after detecting suspicious activity.

This immediate action was critical in preventing further dispersion of the illicit funds. Paolo Ardoio, CEO of Tether, was quoted as saying, "Tether's work with the Department of Justice underscores our commitment to transparency, proactive engagement with law enforcement, and the protection of users across the digital asset ecosystem." [1]

A unique aspect of this seizure involved Tether's so-called burn and reissue mechanism. After freezing the stolen USDT, Tether burned the original tokens on-chain, effectively removing them from circulation.

An equivalent amount of new USDT was then minted and transferred to a wallet controlled by the U.S. Secret Service. This process, visible on the blockchain, provides a compelling real-time example of how blockchain's inherent transparency can be leveraged to aid law enforcement operations and facilitate asset recovery.

Following Tether's freeze, Coinbase played, in its words, a "key role" in the Secret Service's investigation. Between Feb. 26 and Feb. 29, 2024, Coinbase's team conducted extensive blockchain analysis to identify victims and trace the flow of millions in cryptocurrency transactions from illicit wallets back to their platform. [2]

Their efforts helped identify over 130 Coinbase customers who collectively lost at least \$2.3 million to the scam.

The Secret Service's investigation also involved collaboration with other cryptocurrency exchanges, including OKX. The seized funds were traced to over 140 accounts on the OKX exchange, many of which were held in the names of individuals allegedly operating from scam compounds in Southeast Asia.

Legal Ramifications and Future Implications

This massive asset seizure carries significant legal ramifications and signals a growing trend in how law enforcement is approaching crypto-related crime.

The U.S. Attorney's Office for the District of Columbia filed a civil forfeiture complaint in the U.S. District Court for the District of Columbia against the \$225.3 million in cryptocurrency, asserting that the funds are connected to the theft and laundering of money from victims of cryptocurrency investment fraud schemes. [3]

This legal mechanism allows authorities to seize assets linked to criminal activity, with the ultimate goal of returning them to the rightful owners. Special Agent in Charge Shawn Bradstreet of the U.S. Secret Service's San Francisco Field Office stated that this seizure "marks the largest cryptocurrency seizure in U.S. Secret Service history," and represents a "major milestone in their ongoing efforts to combat crypto-related scams." [4]

The U.S. Department of Justice has emphasized its commitment to returning the seized funds to the victims. The FBI has established the Internet Crime Complaint Center, or IC3, as a central hub for reporting cyber-enabled crimes. It provides a trustworthy and convenient reporting mechanism for the public to submit information about suspected internet-facilitated criminal activity.

Victims of internet crimes can file a complaint at www.ic3.gov, where their complaints are analyzed and may be referred to law enforcement agencies for investigation. [5] This focus on victim restitution is crucial for rebuilding trust in the crypto ecosystem.

This case also underscores the transformative impact of blockchain analysis in law enforcement. While the pseudonymous nature of crypto transactions can pose challenges, the immutable and public ledger of the blockchain provides a wealth of data for forensic investigators.

Tools that visualize complex transactions and identify patterns of illicit activity are becoming

indispensable in tracing stolen funds across multiple exchanges and identifying so-called cash-out points.

The success of this operation highlights the increasing necessity and effectiveness of collaboration between law enforcement agencies on the one hand and cryptocurrency exchanges and stablecoin issuers on the other.

As crypto-related crimes continue to rise, such partnerships will be essential for identifying, disrupting and prosecuting criminal networks.

It also underscores the importance of clear federal regulations that encourage legitimate exchanges to share data with law enforcement while respecting user privacy.

The message that law enforcement wants to send with this landmark \$225 million crypto seizure is clear: The days of operating illicit crypto schemes with impunity are numbered.

As blockchain forensics tools become more sophisticated, and cooperation between the private sector and law enforcement strengthens, the legal landscape for crypto-related crime will continue to evolve, offering greater protection to victims and posing significant challenges to those who seek to exploit the digital asset ecosystem for illicit gains.

David Zaslowsky is a partner at Baker McKenzie.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] <https://www.ccn.com/news/crypto/coinbase-secret-service-track-225-million-stolen-crypto-biggest/>.

[2] <https://www.coinbase.com/en-au/blog/consumer-protection-tuesday-how-coinbase-helped-secret-service-seize-stolen-crypto>.

[3] <https://www.secretservice.gov/sites/default/files/reports/2025-06/Verified-Complaint-25-cv-1907.pdf>.

[4] <https://www.secretservice.gov/newsroom/releases/2025/06/largest-ever-seizure-funds-related-crypto-confidence-scams>.

[5] <http://www.ic3.gov/>.

All Content © 2003-2025, Portfolio Media, Inc.