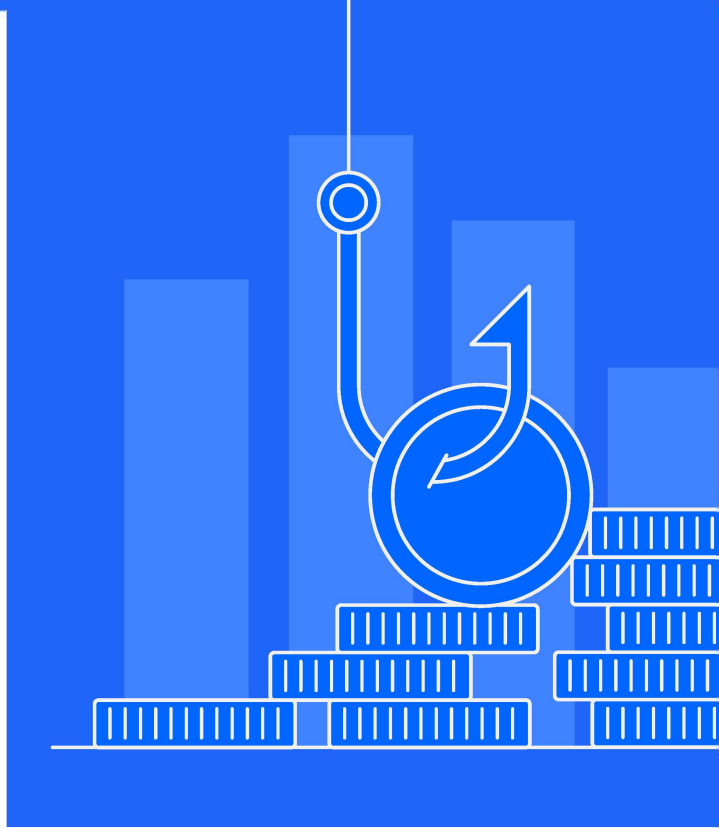




DOJ and FBI Phoenix Seize \$112M in Proceeds from Crypto-related Scams



FBI & DOJ



Region:
North America



Industry:
Law Enforcement



Products Used:
TRM Forensics

Problem

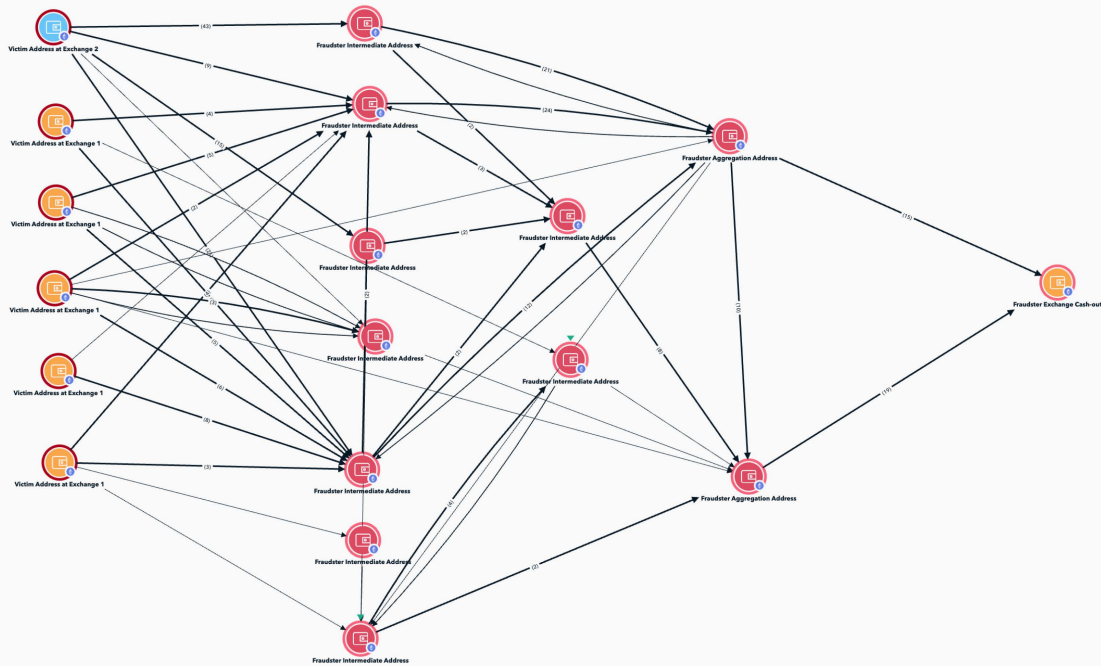
Victims of “pig butchering” lost millions in investment scams and fraud

Results

- Seizure warrants amounting to \$112M
- Cross-agency, cross-jurisdiction coordination

Earlier this year, the Department of Justice announced that it seized cryptocurrency worth an estimated \$112 million linked to “pig butchering” and other crypto-related investment scams. TRM Labs is proud to have assisted law enforcement in the investigations that led to the seizure.

The investigation and prosecution team were able to unwind a huge, commingled network of transactions and follow the proceeds of fraud to cash-out points at exchanges where the government was able to seize proceeds for the victims.



“While ever-evolving technology has allowed drug traffickers and other criminal actors to expand into the digital world and use the darknet to engage in their illegal activity, we are working diligently with our law enforcement and private sector partners to harness the power of technology to mitigate these risks,” said Assistant United States Attorney Seth Goertz, the lead prosecutor on the seizure.

“These cases are very important for protecting the citizens of Arizona and the United States writ large.”

According to [TRM's Illicit Ecosystem Report](#), \$9.04 billion was sent to various types of fraud schemes, including “pig butchering” scams in 2022.

In pig butchering schemes, scammers encounter victims on dating sites, social media platforms, or even random texts masquerading as a wrong number. Scammers initiate relationships with victims and slowly gain their trust, eventually introducing the idea of making a business investment using cryptocurrency. Victims are then persuaded to invest money. Once the money is sent to a fake investment app, the scammer vanishes, taking all the money with them, often resulting in significant losses for the victim.

The term “pig butchering” comes from the idea of “fattening” up the victim by gaining their trust before stealing the money. These cases often involve victims who have lost their life savings not to mention undergone significant psychological trauma.

Seizure warrants for six virtual currency accounts amounting to \$112 million were authorized by judges in the District of Arizona, the Central District of California, and the District of Idaho. These cases are the result of the tireless, coordinated efforts of FBI Phoenix, the U.S. Attorney’s Offices, and the Computer Crime and Intellectual Property Section’s (CCIPS) National Cryptocurrency Enforcement Team (NCET), Fraud Section, and Money Laundering and Asset Recovery Section (MLARS). This is a great example of the Department of Justice, working across judicial districts, to seize and disrupt fraud in the crypto ecosystem.

In addition, the District of Arizona recently announced, together with Homeland Security Investigations, IRS-Criminal Investigations, DEA, United States Postal Inspection Service, the creation of a Darknet Marketplace and Digital Currency Crimes Task Force. The mission of the Task Force is to disrupt and dismantle criminal organizations that are exploiting the appearance of anonymity on the darknet or using digital currency to facilitate criminal activities, such as drug trafficking, money laundering, theft of PII, and child exploitation. The goal of the DNMDCC will be to provide increased collaboration, enhance resources, and disrupt and dismantle criminal organizations that are using these new and emerging technologies.

The Task Force formalizes work that law enforcement partners have been doing since 2017 targeting darknet drug vendors and cryptocurrency-related crimes. The release announcing the Task Force provides a list of key cases.