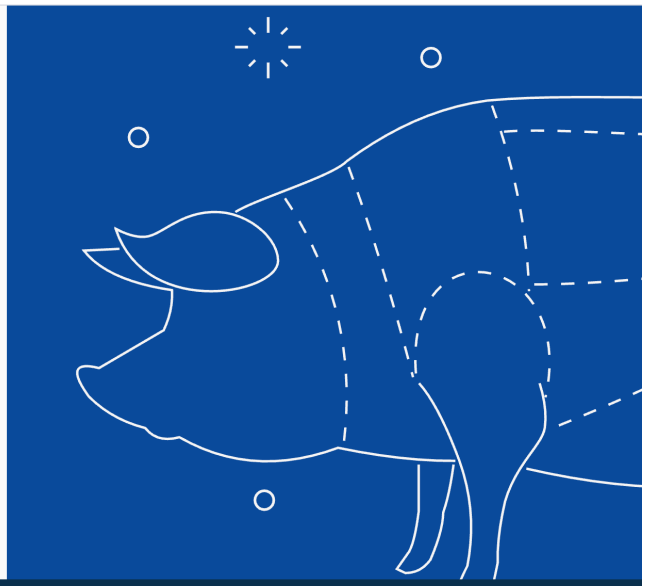
EXHIBIT E

USSS Pig Butchering Investigation Leads to $5M+ Seizure of Victim Funds

REQUEST A DEMO Download PDF →



US SECRET SERVICE

Region
North America

Industry
Law Enforcement

Product Used
TRM Forensics

Problem

A victim and several family members lost $5.5M through a romance scam turned investment scam

Results

- Recovery of $5 million in stolen funds
- Instant alert when funds moved from unhosted wallet to off-ramp
- Procurement of a seizure warrant within hours

Since its creation in 1865, the United States Secret Service (USSS) has been tasked with safeguarding the integrity of the nation's economy. In fact, early USSS investigations involved rampant counterfeiting taking place in the years following the American Civil War, a time in which as much as 30 percent of circulating currency was thought to be illicit. As the threat has evolved, so have USSS investigators, who now focus their efforts on modern financial crimes such as illicit credit card schemes, fraudulent wire transfers, computer fraud and abuse, and, most recently, the illicit use of cryptocurrencies.

To that end, over the last few years, the USSS has led efforts across the U.S. government to investigate fraud schemes involving virtual currency. In 2022, Secret Service launched its Cryptocurrency Awareness Hub and also runs the National Computer Forensics Institute (NCFI). The NCFI is a state-of-the-art, 40,000 square foot facility located in Hoover, Alabama, where it educates state, local, tribal, territorial law enforcement officers, prosecutors, and judges in cyber and electronic related threats.

As part of these initiatives, the USSS has focused its attention on a growing threat - "romance scams," also-known-as pig butchering. In pig butchering schemes, scammers encounter victims on dating sites, social media websites, 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 persuaded to invest money and once the money is sent to the fake investment app, the scammer vanishes with all the victim's money. The term "pig butchering" comes from the idea of "fattening" up the victim as much as possible before stealing the money. These cases often involve victims who have lost their life savings, leaving the victims devastated and desperate for help. The most recent FBI internet crime report states it received more than 30,000 complaints of cryptocurrency investment fraud, with total losses rising from $907 million in 2021 to $2.57 billion in 2022, an increase of 183 percent.

One of USSS' lead offices for cryptocurrency investigations is the San Francisco Field Office, which houses the Digital Asset Technology Alliance (DATA) and participates in the Rapid Enforcement Allied Computer Team (REACT) Task Force. Through the use of investigative tactics, blockchain intelligence and other tools, USSS, and their federal state and local partners, have been able to detect and disrupt a number of fraud schemes.

Unpacking a recent pig butchering case – August 2022

The following is a recitation of an actual case worked by USSS San Francisco. It's a great example of how law enforcement can leverage hard work and blockchain technology to disrupt these schemes and return misappropriated funds to victims.

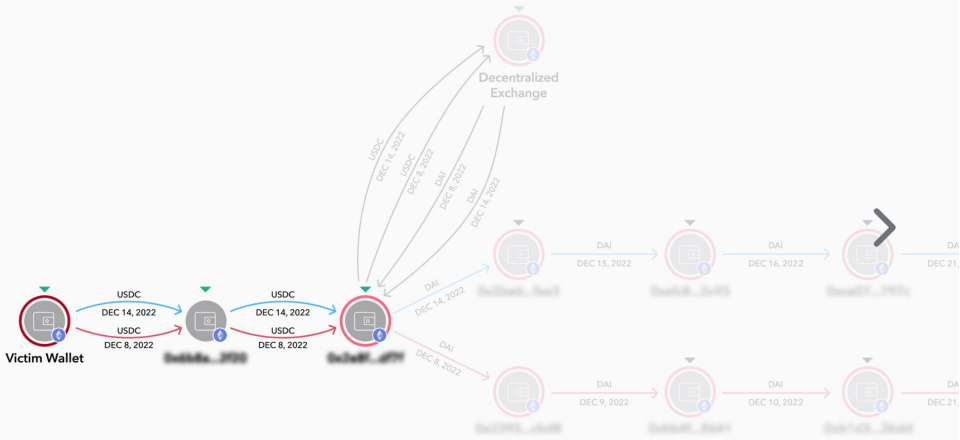
In the late summer of 2022, the soon-to-be victim was contacted by the scammer via the messaging feature of a real estate application. The scammer suggested moving the conversation onto a standard messaging app as the exchange between them became romantic in nature – a common feature of pig butchering scams.

According to the victim, cryptocurrency trading was introduced into the conversation almost immediately. The scammer shared information about a cryptocurrency exchange that offered crypto trading for beginners – a platform that would turn out to be fake. The scammer directed the victim to download a third-party application through a website to access the platform, which would end up being another huge red flag.

After installing the platform, the scammer convinced the victim to purchase approximately $200,000 worth of cryptocurrency from a well-known centralized exchange. After purchasing the cryptocurrency, the victim was directed to send it to an address she was told was associated with her trading account on the phony trading platform. Shortly thereafter, after seeing what she believed were instant gains of 20-30 percent, the scammer prompted her to follow up with an additional $1.1 million investment. Over the course of several weeks, the scammer lulled the victim into contributing even more additional funds. Based upon what she thought was a great investment platform, the victim subsequently shared the platform with several family members who also contributed funds. In total, about USD 5.5 million was sent by seven victims to the scam trading platform. The platform showed that the investment had doubled in value.

In late December 2022, the victim requested to withdraw a significant sum of her funds, at which point she was prompted to pay a $200,000 "withdrawal tax." Having earned what she believed to be millions of dollars from the trading platform, she made the additional $200,000 payment. This turned out to be one last payment that the scammer was able to misappropriate from the victim. Still unable to access her money even after paying the fee, the victim realized that she and her family members had been the victims of a scam. They eached out to the Secret Service for help.

The victim's report resulted in the USSS opening an investigation, led by the San Francisco Office team. Using information provided by the victim, the investigators were able to plot the flow of funds from the original investment platform address through dozens of addresses and multiple types of cryptocurrency. The cryptocurrency tracing showed the non-economic laundering of funds through several addresses on the Ethereum blockchain, then coming to rest in an unhosted wallet. The victim originally sent a cryptocurrency called USDC, which the scammer swapped into a different currency called DAI, prior to ultimately swapping the DAI for USDT (which you can follow from left to right in the visual):



1 Initial fund transfers from Victim's wallet to wallets controlled by Scammer

2 USDC is swapped for DAI through a decentralized exchange and then distributed between two wallets.

3 The funds move
December 2022
Investigators w
began to move

Investigators used an alert function that would notify investigators each time funds moved from monitored wallet addresses, including the unhosted wallet where the victims' funds sat.

Getting these alerts — which are often triggered even before the transaction is registered on-chain — is critical, as scammers often park stolen funds in unhosted addresses for days, weeks, or even months at a time. The moment when they transfer the funds out of the unhosted addresses to cash-out at an exchange can be a prime opportunity for law enforcement intervention, but it must be done quickly before the funds are allowed to pass through the exchange successfully.

In this case, when the funds finally moved from the scammer's unhosted address to an exchange, the USSS received an alert and was able to act in real time to prepare a seizure warrant.

Tracing on the address level enabled the team to quickly detail out the precise amount of funds that belonged to his specific victims; as opposed to entity-level tracing where funds are organized and tracked as movements between clusters of addresses and entities. Using data from the blockchain, combined with other evidence, the team secured a seizure warrant within hours and were ultimately able to seize about $5 million in stolen funds.

Luckily for the victim of this pig butchering scam, USSS team and prosecutors were able to identify and seize the majority of victim funds. As more investigators across the law enforcement community learn the fundamentals of blockchain tracing and investigative techniques, hopefully these types of disruptions will become the norm, not the exception.

Ready to

First Name*

Last Name*

get started?

Fill out the form to schedule a demo with our team.

Company Name*

Job Title*

Business Email*

Phone Number

United States of America

State*

Select the industry that most closely describes where you work.*

Where did you hear about TRM?

Services of Interest

- [ ] TRM Forensics
- [ ] TRM Triage
- [ ] TRM BLOCKINT API
- [ ] TRM Bulk Data
- [ ] TRM Entity Due Diligence
- [ ] TRM Transaction Monitoring
- [ ] TRM Wallet Screening
- [ ] TRM Know-Your-Asset
- [ ] TRM Real-Time-Supervision
- [ ] Professional Services
- [ ] Training Services
- [ ] Report a Personal Scam/Theft
- [ ] TRM Deconflict
- [ ] Partner Integrations
- [ ] Uncertain
- [ ] TRM MCP
- [ ] Privacy Support

- [ ] By submitting this form, you agree to allow TRM Labs to send you email communications and to store and process the personal information submitted. *

You can unsubscribe anytime using the link at the bottom of our emails or by contacting privacy@trmlabs.com. Unsubscribing won't affect our transactional communications with you. For more details, view our Privacy Policy here.

REQUEST DEMO

Subscribe to our latest insights

Enter your email* SUBSCRIBE

You can unsubscribe at any time. Read our Privacy Policy.

TRM

TRM Labs delivers blockchain intelligence to detect crypto-facilitated crime, ensuring compliance and safety worldwide

REQUEST A DEMO

PLATFORM
- Blockchain Intelligence
- Forensics
- Triage
- BLOCKINT API
- Entity Screening
- Transaction Monitoring
- Wallet Screening
- Entity Due Diligence

INDUSTRIES
- Law Enforcement
- National Security
- Regulator
- Banking
- Crypto Business
- Fintech
- Tax Authority
- Prosecutors

SERVICES
- TRM Academy
- Customer Success
- Incident Response

RESOURCES
- All Resources
- Blog
- Reports and White Papers
- Case Studies
- Webinars
- Guides
- TRM Talks
- Events
- Glossary

COMPANY
- Our Story
- Careers
- Press Center
- Company News
- Partners
- Compliance Center
- Contact Us

BACKED BY AMEX VENTURES BLOCK citi VENTURES PayPal salesforce VISA TIGERGLOBAL Bessemer Venture Partners Y

Terms of Use Privacy Policy Cookie Policy *Survey Methodology ©TRM 2026