TRM

After the Scam: How Law Enforcement Restores Hope for Victims

SHAMROCK **Operation Shamrock**

Region
North America

Industry
Law Enforcement

Products Used
TRM Forensics, Chainabuse

Problem

A sophisticated "pig butchering" investment scam defrauded a victim of hundreds of thousands of dollars, using chain-hopping to obfuscate funds

Results:

- Connected the victim with an expert investigator within 24 hours
- Linked individual victim loss to USD 70 million frozen assets
- Placed the victim's funds in the federal queue for return

Global crypto transaction volume grew 56% last year to more than USD 10.6 trillion. That momentum has carried into 2025, and with it the sophistication and scale of criminals seeking to exploit it. In response to this rising threat, Operation Shamrock was established as a groundbreaking public-private sector collaboration with a clear mission: to educate the public, mobilize resources, and disrupt cryptocurrency fraud. By bridging the gap between victims and expert investigators at law enforcement agencies, the non-profit Operation Shamrock creates a unified front against transnational cybercrime networks.

At the heart of this initiative are the investigators of Operation Shamrock, law enforcement professionals who triage reports, support victims, and connect cases across jurisdictions. To scale this work and surface patterns that would otherwise remain hidden, they rely on a unified source of victim-reported intelligence. Chainabuse – operated by TRM Labs – the world's largest database of user-reported illicit cryptocurrency activity – serves as that critical intelligence layer, ingesting victim reports and enabling investigators to triage and support victims, instantly cross-reference new cases with known illicit actors to uncover additional victims, and map connections across scam networks. This synergy between Operation Shamrock's victim support network and TRM's blockchain intelligence capabilities enables rapid response, previously impossible for local agencies acting alone.

The rise of pig butchering scams

Among the most devastating threats targeting crypto users today is pig butchering (also commonly referred to as crypto investment scams or romance baiting) – a long-con investment fraud that has reached epidemic proportions. The global impact is in the hundreds of billions of dollars, including nearly USD 10 billion lost by Americans in 2024 alone. These schemes operate on an industrial scale, often run from compound-style operations overseas.

Unlike simple phishing attacks, pig-butchering scams rely on sustained psychological manipulation. Scammers spend weeks or even months grooming their targets, cultivating what appear to be genuine romantic or platonic relationships. Once trust is established, they introduce the victim to a fake cryptocurrency investment platform. These platforms are designed to look legitimate, complete with falsified growth charts and "customer support," convincing victims to invest increasingly larger amounts – often their entire life savings – before the scammers disappear.

The consequences extend far beyond financial loss. As Erin West, founder of Operation Shamrock, notes, these scams inflict a uniquely painful blend of emotional and monetary harm. "We understand romance scams. We understand investment scams," she explains. "But we have never seen what happens when you lead a human to believe that they are in the relationship of their life and that they are going to not just become rich, but maybe pay off debts or get rid of student loans. And then one day, that person comes to find out that it was all a lie."

A friendship turned financial ruin

For Mezemir, who goes by "Mez," a victim of one such scheme, the nightmare began with a simple friend request in October 2024. "I clicked on it. I wasn't suspicious about it. I thought it was just a normal friend that I met," Mez recalls. "And we started having a conversation."

Over time, the scammer, posing as a successful investor, manipulated Mez's trust. "She convinced him to begin investing in cryptocurrency," explains Detective Scott Simons of the Greenfield Police Department in Wisconsin, a key member of Operation Shamrock. "She was sending him photos of the fake investment website to deceive him and get his trust."

Enticed by the apparent profits and the relationship he thought he had built, Mez invested heavily. "I like how much she's making. I'm very attracted to it," Mez admits, reflecting on his mindset at the time. "I absolutely thought that my money was secured because it was going through legitimate apps. But, now I know that that is just a number. The actual asset is gone somewhere."

In total, Mez deposited approximately USD 240,000 into a cryptocurrency wallet, purchasing bitcoin and sending it to the scammer. It wasn't until he tried to withdraw his funds that reality set in. "The moment I realized that the money was gone [and] knew the fact that that person was actually a scammer… there was no hope at all."

Following the funds

Mez wasted no time. "So now I know that I'm in serious trouble. So I have to act quickly," he recalls. He navigated to Operation Shamrock's website, a resource hub for victims, and filed a report.

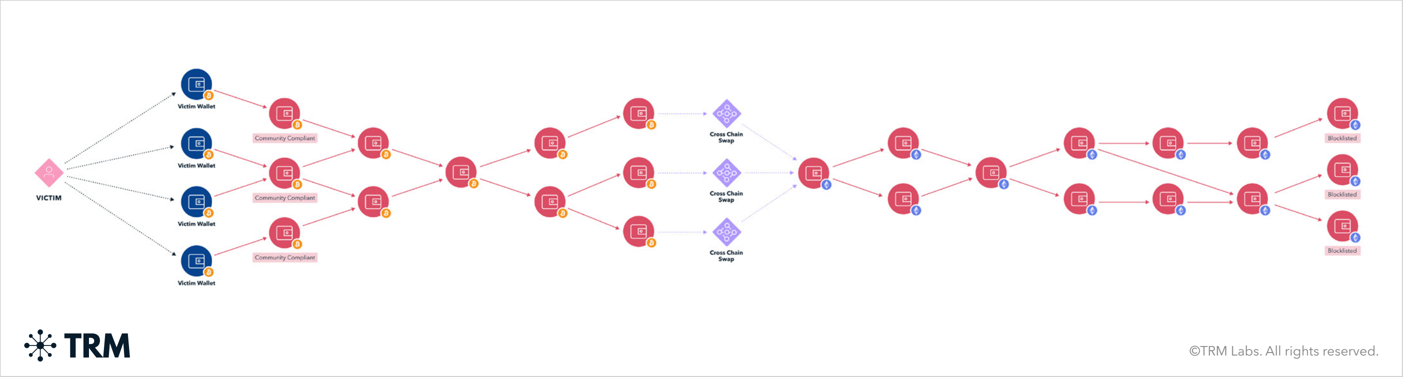
"If someone thinks they're scammed, the first thing they have to do is to go straight to operationshamrock.org, where they can automatically send a report to [the law enforcement teams that are part of Operation Shamrock], like Detective Scott [Simons]," Mez explains.

This report was automatically ingested into Chainabuse, where it was immediately flagged for Detective Simons. "I think within a day, he sent me an email," says Mez.

Detective Scott Simons began his investigation using TRM Forensics to trace the flow of funds. However, the scammers had employed advanced obfuscation techniques. "The scammer was very sophisticated in this investigation, even moving the cryptocurrency to other blockchains," Simons notes. "This is very common by scammers to make it more difficult for law enforcement to trace."

Despite the "chain hopping," TRM's cross-chain tracing capabilities allowed Simons to follow the money. The breakthrough came when his analysis revealed the destination of Mez's funds. "TRM immediately identified the wallet as a frozen wallet by federal law enforcement," Simons reveals.

Mez's USD 240,000 had been swept into a massive laundering network that federal authorities had already targeted. "Mez's scam was part of a much larger scam, in which at least USD 70 million was stolen and frozen," explains Simons. The swift reporting and connection provided by Chainabuse linked Mez's individual loss to a major federal seizure.



Justice served and hope restored

This case stands as an example of what's possible when law enforcement agencies are empowered with the intelligence and capabilities to respond effectively to victim reports. Organizations like Operation Shamrock and platforms like Chainabuse help law enforcement teams unlock immense potential to return funds and restore justice for victims. "In the amount of time that Operation Shamrock has partnered with TRM, our experienced investigators have seized or frozen millions of dollars in cryptocurrency for victims," Detective Simons states proudly.

For Mez, the news was life-changing. "I am so blessed and happy right now. Very happy. I'm so blessed to have Detective Simons on my case," he says.

Beyond the financial recovery, the case highlights how Operation Shamrock can support local law enforcement in restoring justice for victims. "I've been able to help victims, but at the same time build up my knowledge base by working these different cases," Detective Simons says. "Being able to help victims such as Mez, it's a great feeling."

Are you a victim of a crypto scam?

If you believe you or someone you know has been the victim of a cryptocurrency scam, time is of the essence. Acting quickly can increase the chances of recovery and helps law enforcement disrupt these criminal networks.

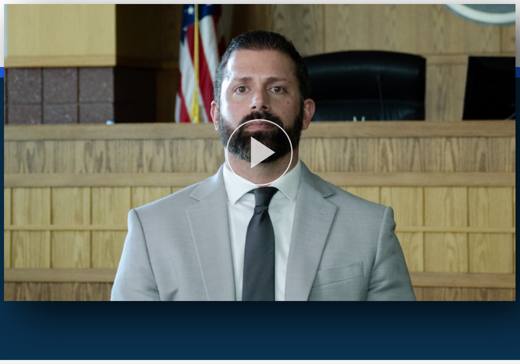
What to do:

- **Stop all communication:** Do not send any more money to the scammers, even if they promise it will unlock your account.
- **Report immediately:** Go to operationshamrock.org to file a report through Chainabuse. Your information will be securely shared with crypto experts and investigators who can take action.
- **Preserve evidence:** Keep records of all communications, transaction hashes, and wallet addresses associated with the scam.

Your report not only helps your own case, but also contributes to the global intelligence needed to stop these scams for good.

Watch Det. Scott Simon's story

Looking for more? Explore all our case studies.



TRM provides blockchain intelligence tools to help financial institutions, crypto businesses, and governments combat cryptocurrency fraud and financial crime.

Request a demo: contact@trmlabs.com
www.trmlabs.com |