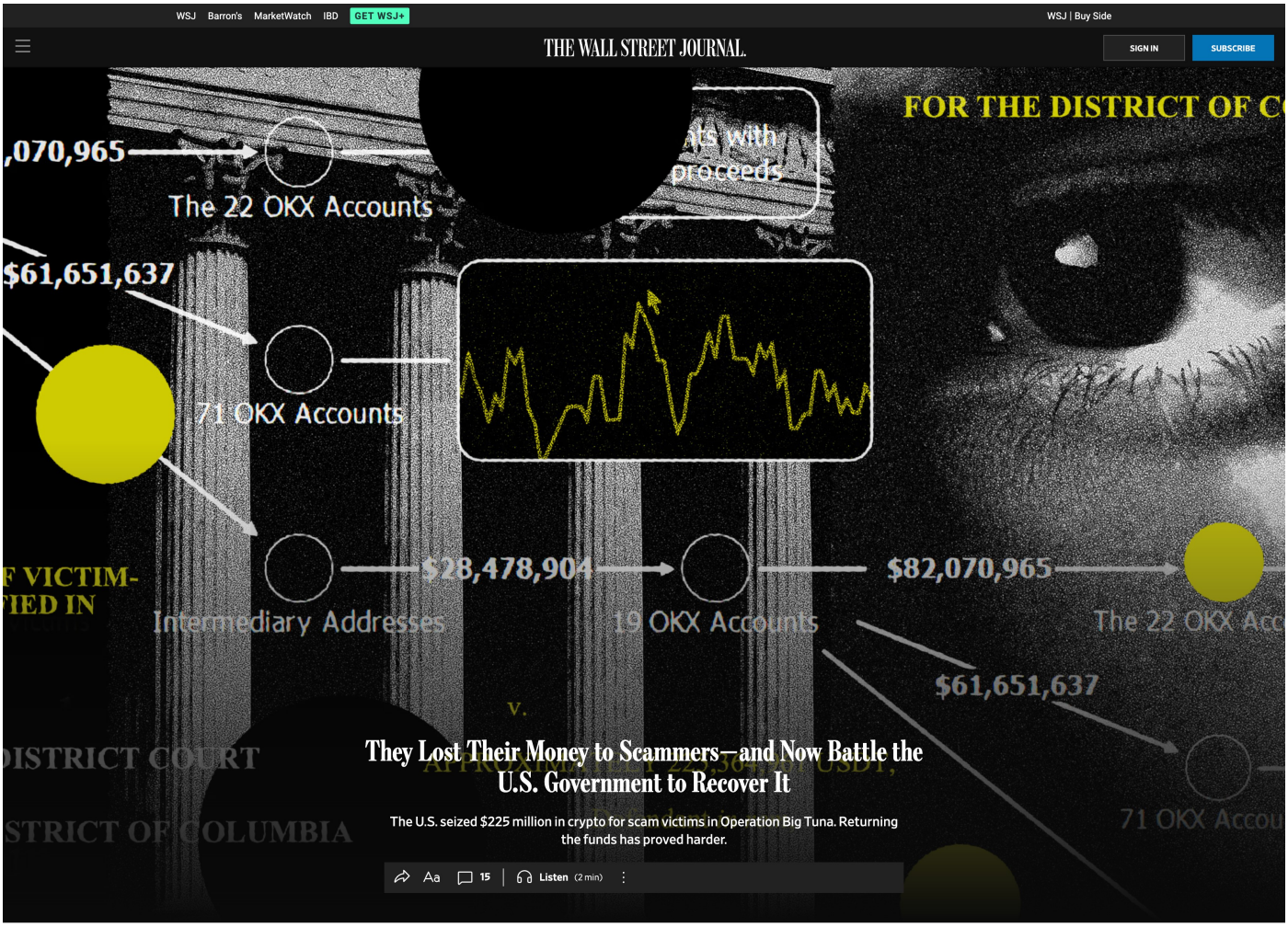
EXHIBIT D



By Dylan Tokar
Sept. 9, 2026 9:00 pm ET

RACHEL MENDELSON/WSJ; ISTOCK

In 2022, after Nivie Kaul lost more than $8 million in a cryptocurrency scam, she embarked on a quest to unmask the criminals and get the money back.

Kaul, who lives in California, has said in court filings that she gave up her work as a legal consultant and learned how to trace crypto across digital ledgers. When U.S. law enforcement said they couldn't help her, she filed a legal claim in Turkey, where she had tracked some of her money. That sparked a probe into what Turkish prosecutors have described as a professional money-laundering ring, a tributary to the vast shadow economy underpinning the global scam industry.

Few scam victims ever get their money back, but Kaul's dogged crusade appeared set to pay off. A Turkish court in 2023 ordered the seizure of a digital wallet holding more than $100 million, from which Kaul says her losses would have been repaid. But then a new obstacle arose.

Before Turkey could move to distribute the money, U.S. law enforcement took custody of the wallet sought by Kaul, along with other crypto holdings totaling $225 million, in an operation dubbed Big Tuna that aimed to disrupt an alleged scam compound in the Philippines.

Kaul is now one of several hundred victims who have filed claims on those funds, part of a giant legal battle that's demonstrating just how difficult it can be for victims to recover stolen funds.

The case highlights a harsh reality for the growing number of Americans left financially devastated by scammers: Even when the government is able to seize stolen crypto, with no clear standards around who gets what, the recovery process can turn into a bureaucratic mess.

The seizures represent only a small portion of the tens of billions siphoned from Americans each year—but they are growing. Since the scammers are abroad and not easy to arrest, law enforcement in recent years has focused on following the money. Agents have learned to painstakingly trace digital currencies, hop by hop, across blockchains—the decentralized ledgers stored on computers around the world that provide a public record of transactions between digital wallets. When money has moved beyond the reach of the U.S. legal system, agents in some cases have convinced foreign crypto companies to turn over allegedly stolen funds.

That approach, which often amounts to grabbing large sums of suspicious-seeming crypto without knowing who currently controls it, is being challenged in the case of

the government's $225 million seizure. Last year, an online gaming company named Infiniweb Technology showed up in court, saying that it owned the seized wallets and that it had nothing to do with the scam operation.

[advertisement omitted]

Three years after the launch of Operation Big Tuna—a reference to a nickname for John Krasinski's character in the TV sitcom "The Office"—the Justice Department in August said it was close to a settlement that could eventually lead to payouts for victims.

Even then, it may be many months before victims know what, if anything, they will receive from the case.

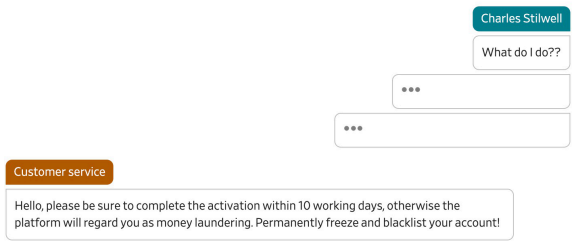
Defendant "1"

Global investment scams, sometimes called pig butchering, have exploded in recent years, thanks to sophisticated call centers in places like Southeast Asia where scammers spend months forging emotional ties with victims before luring them into seemingly lucrative crypto ventures.

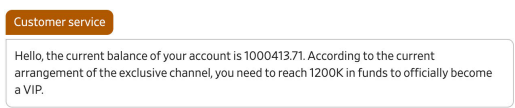
In 2022, Charles Stilwell began chatting with a user on Facebook Messenger who went by the name Amity Zhang and told him about a supposed crypto investment pool run by her uncle. The insurance business owner in Miami, who is in his 70s, started small, upping his investments only after the website for the fake cryptocurrency platform began showing big returns.

When his account reached $500,000, Stilwell was told by the investment platform's customer service that he had been flagged as a money launderer and needed to pay a hefty fee to prove he wasn't.

Advertisement



He was also told he needed to pay various fees and taxes to make any withdrawals. Stilwell added even more funds over the next two months, opening a line of credit on his Miami home, but the scammers continued demanding more fees.



As Stilwell began to realize he was being scammed, he reported his losses to the Federal Bureau of Investigation, Secret Service and even then-Sen. Marco Rubio. He also came across an online advertisement for a law firm dubbed the Crypto Lawyers.

The firm, which provides a range of crypto-related services, is part of a small but growing industry of lawyers and forensic blockchain investigators who say they can help scam victims get their money back. In a phone call with Stilwell, one of the partners explained the firm's strategy. The first step was to have an in-house investigator trace the crypto that Stilwell had sent to the scammers.

Stilwell decided to pay the initial $15,000 fee. The Crypto Lawyers say their fees vary depending on the client's situation, and that it often is paid as a percentage of recovered losses.

Advertisement

Most of Stilwell's money had ended up in wallets hosted on the crypto exchange Binance. The lawyers contacted Binance's legal department, and were told that Binance would freeze the money if they could get a court order.

In May 2023, the lawyers filed a racketeering complaint in Miami federal court against the anonymous holder of the wallets, dubbed defendant "1," which the firm described as an individual in China who had tricked Stilwell into sending money. They gave notice of the lawsuit by sending the wallets a special type of crypto token with a link to the legal papers.

Fifteen months later, a magistrate judge denied Stilwell's motion, saying he needed to serve the same notice to other anonymous co-conspirators who may have been part of the scam. By then his lawyers realized that the funds traced to Binance had disappeared.

"It was deflating," Stilwell said.

He didn't know it at the time, but U.S. law enforcement was already on the trail of a trove of stolen crypto that would give him another chance to reclaim his lost funds.

Operation Big Tuna

Around December 2022, the crypto platform OKX received a tip from a private investigator about a suspicious wallet hosted on its platform. A small team at OKX dug in. They soon discovered dozens of wallets they suspected were moving billions in scam proceeds, the company said.

Advertisement

OKX turned over its findings to the Secret Service's San Francisco field office. That January, the agency launched Operation Big Tuna.

OKX requires identification and a matching selfie to open a wallet on its platform. When OKX's investigators examined the pictures linked to the suspicious OKX accounts, many appeared to have been taken at the same facility, with someone else holding the camera.

In all, OKX found 144 suspicious wallets on its platform that had processed 263,000 transactions worth $2.94 billion.

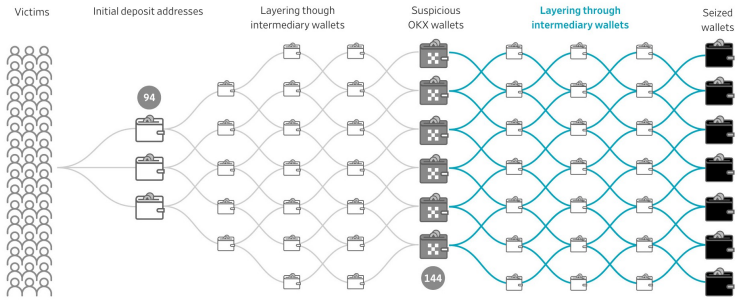
Nearly all of the accounts were accessed via IP addresses in the Philippines and some account holders wore lanyards with the name ITECHNO Specialist Inc., a call center in Manila, according to court documents. The company couldn't be reached for comment.

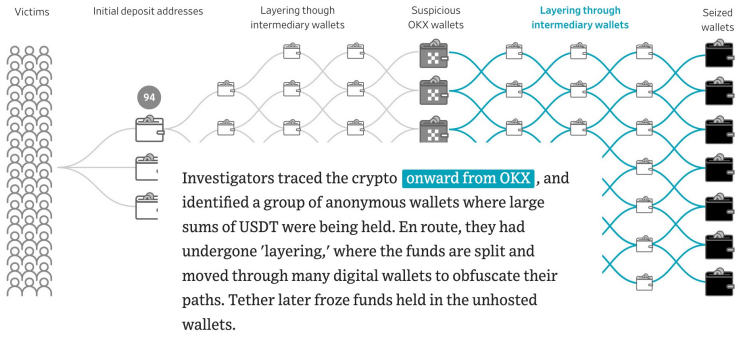
Large amounts of crypto were being routed from OKX to a group of anonymous wallets, investigators found. The crypto in the wallets was USDT, a type of digital coin that is centrally controlled by the company Tether. USDT can be frozen and reminted no matter where it is—presenting law enforcement with a rare opportunity to grab the funds, with Tether's cooperation.

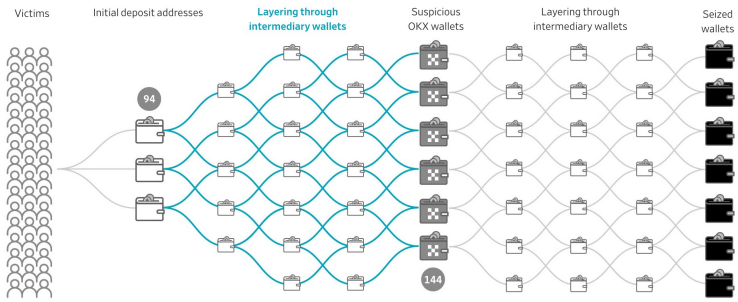
El Salvador-based Tether initially declined a request to freeze the USDT held in two suspicious wallets, according to Justice Department attorneys. Agents kept an eye on the funds. In the months that followed, with USDT's reputation as the crypto of choice for money launderers growing, pressure built on Tether to do more to police its digital currency. By November, the company told the government it was ready to help.

Advertisement

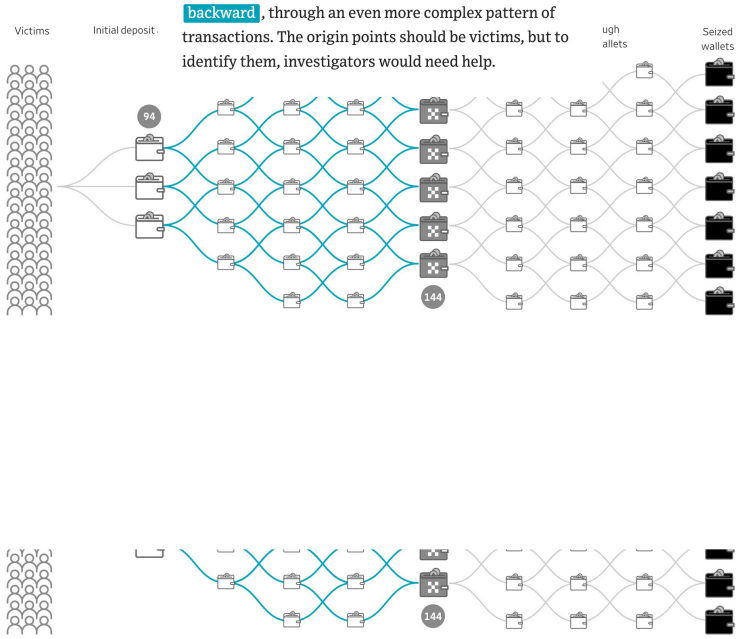
A spokesman for Tether said the company "didn't refuse the freeze. We remained available to collaborate further on the matter, resulting in one of the best coordinated examples of enforcement action and maximizing the result of the freeze."







Investigators suspected the wallets were holding the proceeds of scams. But before Tether could remint the crypto, investigators needed to trace the money backward, through an even more complex pattern of transactions. The origin points should be victims, but to identify them, investigators would need help.



Alana Pipe/WSJ

In February 2024, Secret Service convened representatives from several crypto exchanges in the suburban office building outside San Francisco that served as its regional field office.

Getting account information from a crypto exchange can take days or weeks. At the gathering—one of what the Secret Service has dubbed "sprints"—a Justice Department attorney could merely write up a subpoena, walk it over to a desk where a representative from a crypto exchange sat, and quickly get a response.

The two sides worked together for two days. Anytime a victim was identified, there was a burst of excitement, said Samantha Rodriguez, an in-house investigator for crypto exchange Coinbase who attended the sprint.

Advertisement

But the most grueling step came when Secret Service agents called the suspected victims. In many cases, the account holders hadn't yet realized they were being scammed, people who participated in the sprint said.

The Secret Service was able to contact around 60 victims whose cumulative $19 million in losses could be traced to the seven unhosted wallets—just a slice of the total $225 million ultimately seized by the Justice Department. Agents believed there were some 374 other victims but were unable to either identify or contact them, lawyers for the government later said.

One victim was Shan Hanes, the former chief executive of Heartland Tri-State Bank, a tiny community bank in Elkhart, Kansas. After Hanes lost all of his own money in a crypto investment scam, he began sending scammers the bank's deposits, according to prosecutors. The losses secretly grew until the bank was forced to close, leaving its small-town investors and depositors in shock.

In 2024, Hanes was sentenced to more than 24 years in prison for embezzling $47.1 million in bank funds. A lawyer for Hanes declined to comment.

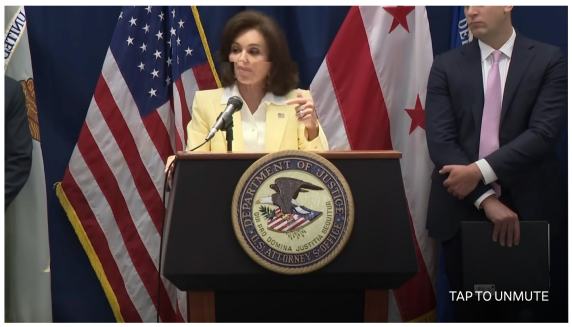
A giant legal battle

U.S. Attorney Jeanine Pirro announced the $225 million seizure at a press conference in June 2025. The DC's attorney's office was taking a lead on fighting crypto scams with an "eye toward making victims whole," Pirro said in a press release at the time.

Advertisement

The announcement kicked off a chaotic tussle over the funds.

In October, Infiniweb, an online gaming company registered in the British Virgin Islands, challenged the Justice Department's $225 million seizure.



U.S. Attorney Jeanine Pirro announced the $225 million seizure at a press conference in June 2025.

Lawyers for the government have yet to respond to Infiniweb's claim, or explain how the alleged scam proceeds ended up in the company's possession. Casinos and gaming companies have long been a favored venue for laundering illicit funds. But without evidence that Infiniweb knowingly played a role in the scam, the Justice Department could be forced to return all or some of the seized funds.

Infiniweb declined to comment, citing the active litigation.

Quickly stacking up against Infiniweb's claim were those filed by law firms representing hundreds of victims. The Crypto Lawyers sifted through its blockchain analyses and found 118 clients, including Stilwell, whose losses it believed could be tied to the seized crypto.

Soon after, a second law firm filed a similar claim on behalf of another 147 scam victims.

The Justice Department initially moved to strike the claims filed by the Crypto Lawyers, saying victims would need to apply directly to the department to get funds back. And lawyers for the government say a judge must first approve the forfeiture before it can return money to victims.

Advertisement

But last month a Justice Department attorney said the department was close to striking a deal with both Infiniweb and victims that could involve appointing an administrator to oversee claims and giving preference to victims who could trace their funds to the suspicious wallets identified in the Big Tuna case.

One victim whose claim to the seized funds remains in contention is Kaul, whose efforts kicked off a sprawling investigation in Turkey.

Justice Department attorneys have said Kaul's funds aren't traceable to the wallets seized in the Big Tuna case, though they have said she can still apply along with other victims when the case concludes.

Since Kaul took her legal crusade to Turkey, prosecutors there have filed a 1,548-page indictment describing a money-laundering operation they say operated out of Istanbul's Grand Bazaar—a 500-year-old shopping market stretching back to the Ottoman Empire. As of July, the Turkish investigation, which is ongoing, had yielded more than 130 arrests.

The U.S. hasn't filed any criminal charges connected to Big Tuna.

Kaul launched an organization called the Digital Defenders Group, aimed at helping other victims recover their funds, and has said she identified more than 200 other scam victims who were victims of the Turkish money laundering ring.

Kaul recently asked the judge overseeing the Justice Department's $225 million seizure to set aside the wallet targeted by Turkish prosecutors, arguing that the Turkish court's seizure order gave her special status over the funds. Justice Department attorneys have dismissed the Turkish order as a basis for any claim over the wallet.

"I have had no income for more than three years," Kaul wrote in a recent court filing. "I have funded my investigation, the Turkish proceedings, and DDG's work from my own savings."

[related links, author note, "Up Next" panel and advertisement omitted]