UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA **Plaintiff,** **v.** **APPROXIMATELY 868,247 USDT** **Defendant.**	§ § § § § § § § § § §	**COMPLAINT FOR FORFEITURE *IN REM*** ***CIVIL ACTION NO.*** **25-cv-2967**

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

Plaintiff, the United States of America, through the U.S. Attorney for the District of Columbia, brings this verified complaint for forfeiture in a civil action *in rem* against approximately 868,247 USDT,[1] hereinafter "Defendant Property," and alleges as follows:

STATEMENT OF THE CASE

1. Criminals abroad, their associates, and conspirators together stole funds from at least three victims and laundered them through a convoluted web of cryptocurrency wallets to evade detection and obfuscate accountability. The Federal Bureau of Investigation ("FBI") Honolulu Division traced and seized the Defendant Property, which constitutes proceeds traceable to those thefts and property involved in, and traceable to, this nefarious money laundering scheme.

2. The United States of America seeks to lawfully forfeit the Defendant Property to punish and deter criminal activity by depriving criminals of property used in or acquired through

[1] USDT is a type of virtual currency called a "stablecoin." The price of a stablecoin is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. USDT is pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives. Tether Limited ("Tether") is the company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT tokens.

illegal activities; to promote and enhance cooperation among federal and foreign law enforcement agencies; and, most importantly, to recover assets that may be used to compensate victims.[2]

JURISDICTION AND VENUE

3. This Court has original jurisdiction of this civil action by virtue of 28 U.S.C. § 1345 because it has been commenced by the United States and by virtue of 28 U.S.C. § 1355(a) because it is an action for the recovery and enforcement of a forfeiture under an Act of Congress.

4. This Court has *in rem* jurisdiction over the Defendant Property under 28 U.S.C. § 1355(b).

5. Venue is proper in this judicial district under 18 U.S.C. § 3238 and 28 U.S.C. §§ 1355(b) and 1395(a), (b), and (c).

NATURE OF THE ACTION AND STATURY BASIS FOR FORFEITURE

6. The United States files this *in rem* forfeiture action to seek forfeiture of Defendant Property as constituting proceeds of wire fraud and wire fraud conspiracy offenses, committed in violation of 18 U.S.C. §§ 1343, 1349, 2, and 3, and as involved in money laundering and money laundering offenses, committed in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i), 1956(a)(2)(B)(i), 1956(h), 2, and 3.

7. Procedures for this action are mandated by Rule G of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions and, to the extent applicable, 18 U.S.C. §§ 981 and 983 and the Federal Rules of Civil Procedure.

8. 18 U.S.C. § 981(a)(1)(A) mandates forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of section 18 U.S.C. §§ 1956, 1957, or 1960, or any property traceable to such property.

[2] *See* United States Asset Forfeiture Program, *Our Mission*, https://www.justice.gov/afp.

9. 18 U.S.C. § 981(a)(1)(C) mandates forfeiture of property constituting or derived from proceeds traceable to wire fraud, conspiracy to commit wire fraud, or any offense constituting "specified unlawful activity" as defined by 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such offense. A violation of 18 U.S.C. § 1343, or a conspiracy to commit that offense, constitutes specified unlawful activity under 18 U.S.C. § 1956(c)(7)(A) as an offense listed in 18 U.S.C. § 1961(1)(B).

10. 18 U.S.C. § 1343 provides that whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, commits the violation of wire fraud.

11. 18 U.S.C. § 1349 provides that whoever attempts or conspires to commit a violation of 18 U.S.C. § 1343 shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

12. 18 U.S.C. § 1956(a)(1)(B)(i) provides in relevant part that whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity— . . . knowing that the transaction is designed in whole or in part . . . to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of "specified unlawful activity" is guilty concealment money laundering.

13. 18 U.S.C. § 1956(a)(2)(B)(i) provides that whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States—knowing that the monetary instrument or funds

involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part—to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity, commits international money laundering.

14. 18 U.S.C. § 1956(h) provides that any person who conspires to commit any offense of 1956 or 1957 is subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy.

15. 18U.S.C. § 1957 makes it a crime to knowingly engage or attempt to engage in a monetary transaction in criminally derived property of a value greater than $10,000 where those funds are derived from specified unlawful activity.

PROPERTY INFORMATION

16. The Defendant Property is approximately 868,247.366804 USDT. That approximately 868,247.366804 USDT was associated with the following unhosted wallet addresses [3] : virtual currency address TC66d59uus8AWhYDvAgWM55T8NRa7KNWAN ("KNWAN"), which held approximately 465,514.638375 USDT, and virtual currency address TH4qXPSp3S5g3HnDr1pgnEq4XAoJh7McvZ ("7McvZ"), which held approximately 402,732.728429 USDT. The addresses together are hereinafter referred to as the "Subject Virtual Currency Addresses."

17. The FBI facilitated the transfer of the Defendant Property from Tether, and the Defendant Property is currently in United States Marshals Service custody.

[3] An unhosted wallet, also known as a self-hosted or non-custodial wallet, is a virtual currency wallet through which the user has complete control over storing and securing their private keys and virtual currency. Unhosted wallets do not require a third party's involvement (*e.g.*, a virtual currency exchange) to facilitate a transaction involving the wallet.

STATEMENT OF FACTS

Background on cryptocurrency

18. **Virtual currency:** Virtual currencies are digital tokens of value circulated over the internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies, such as the U.S. dollar, but are generated and controlled through computer software. Bitcoin ("BTC") and Ether ("ETH") are currently the most well-known virtual currencies in use.

19. **Virtual currency address:** Virtual currency addresses are the specific virtual locations to or from which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers.

20. **Private key:** Each virtual currency address is controlled through a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder(s) of an address's private key can authorize a transfer of virtual currency from that address to another address.

21. **Virtual currency wallet:** There are various types of virtual currency wallets, including software wallets, hardware wallets, paper wallets. A software wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet allows users to store, send, and receive virtual currencies. A virtual currency wallet can hold many virtual currency addresses at the same time. Wallets that are hosted by third parties are referred to as "hosted wallets" because the third party retains a customer's funds until the customer is ready to transact with those funds. Conversely, wallets that allow users to exercise total, independent control over their funds are often called "unhosted" wallets.

22. **Blockchain:** The code behind many virtual currencies requires that all transactions involving that virtual currency be publicly recorded on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by a decentralized network of computers and using that blockchain's technology, containing an immutable and historical record of every transaction. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

23. **Tron and TRX**: Tron is a blockchain that supports smart contracts and decentralized applications. Its native token is TRX, which developers can use in their applications. Unlike similar blockchain projects, TRX is not used on the Tron blockchain to pay transaction fees. Tron is maintained by the Tron Decentralized Autonomous Organization ("DAO"), a Singapore-based non-profit organization. Tron uses bandwidth points as payments. By default, each user has 600 bandwidth points, which represent 600 bytes of data. Transactions are measured in how many bytes they occupy in a block, so if a transaction is larger than the amount allowed by default, the user must purchase more bandwidth points. More bandwidth points can be acquired by staking TRX. In addition to query operations, any on-chain transaction will consume system resources. All types of transactions need to consume bandwidth. In addition to consuming bandwidth, smart contract deployment and calling transactions also consume energy. When the available bandwidth or energy in the account is insufficient, TRX needs to be burned to pay for the corresponding resource fee. In addition to resource fees, some special transactions require additional fees.

24. **Virtual currency exchanges (VCEs):** are trading and/or storage platforms for virtual currencies such as BTC and ETH. Many VCEs also store their customers' virtual currency in virtual

currency wallets. As previously stated, these wallets can hold multiple virtual currency addresses. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers (*i.e.*, "know your customer" or "KYC" checks) and to have anti-money laundering programs in place.

25. **Blockchain analysis:** It is virtually impossible to look at a single transaction on a blockchain and immediately ascertain the identity of the individual behind the transaction. That is because blockchain data generally consist only of alphanumeric strings and timestamps. But law enforcement can obtain leads regarding the identity of the owner of an address by analyzing blockchain data to figure out whether that same individual is connected to other relevant addresses on the blockchain. To analyze blockchain data, law enforcement can use blockchain explorers as well as commercial services offered by several different blockchain-analysis companies. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions. "For example, when an organization creates multiple [BTC] addresses, it will often combine its [BTC] addresses into a separate, central [BTC] address (*i.e.*, a "cluster"). It is possible to identify a 'cluster' of [BTC] addresses held by one organization by analyzing the [BTC] blockchain's transaction history. Open-source tools and private software products can be used to analyze a transaction." *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020). Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

Overview of Confidence Scams

26. The FBI is investigating cryptocurrency investment fraud ("CIF") schemes, often referred to as "pig-butchering," a term derived from the Chinese-language word used to describe this scheme and its treatment of victims. In 2024, more than 41,000 complainants reported being

victimized by CIF schemes to the FBI, resulting in $5.8 billion in reported losses.[4] CIF schemes are largely run out of scam centers based in southeast Asia, but now they are now expanding into other continents.

27. CIF schemes often begin when criminals contact potential victims through seemingly misdirected text messages, dating applications, social media sites, or other online platforms. Next, using various means of manipulation, the criminal gains the victim's affection and trust. Under the so-called "pig butchering" scheme playbook, criminals liken victims to "pigs" at this stage because they concoct elaborate stories to "fatten up" their victims, or gain their confidence.

28. Once that trust is established, the criminal recommends cryptocurrency investment by touting their own, or an associate's, success in the field. Investment methods vary, but a common tactic is to direct a victim to a fake investment platform hosted on a website. These websites, and the investment platforms hosted there, are created by criminals to mimic legitimate platforms. The criminal assists the victim with opening a cryptocurrency account, often on a U.S.-based exchange, such as Coinbase, and then walks the victim through transferring money from a bank account to that cryptocurrency account. Next, the victim will receive instructions on how to transfer their cryptocurrency assets to the fake investment platform. On its surface, the platform shows lucrative returns, encouraging further investment. In reality, all deposited funds are routed to a cryptocurrency wallet address controlled by the criminals—the "butchering" phase of the scheme.

29. CIF schemes will often take victims down one of two paths. In path one, the criminals will encourage further investments until the victim has depleted their bank accounts. Oftentimes, the criminal will attempt to continue the scheme by coaching victims on taking out loans against their

[4] *See* Fed. Bureau of Investigation, *Internet Crime Report 2024* at 36, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

homes or to borrow money from friends and family. Inevitably, these victims eventually run out of money and make attempts to withdraw their funds. However, victims are unable to do so and are provided various excuses as to why. For example, criminals will often levy a fake "tax" requirement, stating taxes must be paid on the proceeds generated from the platform. This is just an eleventh-hour effort by criminals to elicit more money from victims; ultimately, victims are locked out of their accounts and lose all their funds. Even when victims procure enough funds to pay these "taxes," the criminals will continue to concoct new excuses and fees for victims to pay.

30. In path two, the victims are typically investing as part of a larger group where they are led to believe the group is leveraging their numbers to maximize profitability. Oftentimes, these victims will have been investing for a while before suddenly, and unexpectedly, they will lose all their money in one trade. The criminals will cast blame on the victim having made one of many small mistakes. Later, the criminals, and other "would-be" investors, encourage the victims to reinvest in the program to earn back their losses. In this variation of CIF, the victims never knew that the total loss of their entire balance was pre-planned. Therefore, some victims do not realize they have been scammed at all.

Background on the LME Crypto Group's "Pig Butchering" Scheme

31. In or around September 2022, the FBI's Honolulu Division Cyber Squad initiated an investigation into a group impersonating the London Metal Exchange. The London Metal Exchange, a legitimate company, has offices in both the United Kingdom and Singapore, and primarily deals in financial trading of raw industrial materials. This impersonating group, herein referred to as the "LME Crypto Group," is believed to be operating a complex CIF scheme by cultivating long-term relationships with victims online and eventually enticing them to make investments in fraudulent cryptocurrency trading platforms. The FBI Honolulu Division opened an investigation after

receiving a complaint from a victim in Hawaii (the "Hawaii Victim") who was defrauded out of $1.3 million by the LME Crypto Group. The FBI has received additional victim reports from individuals located within the United States and abroad who have been defrauded by the LME Crypto Group in the same manner.

32. The FBI is aware that the LME Crypto Group operated, and continues to operate, numerous websites that impersonate the London Metal Exchange, as well as other entities, in furtherance of the scheme. The website of the legitimate London Metal Exchange is "https://www.lme.com/." The LME Crypto Group has created numerous webpages claiming to be a cryptocurrency trading arm of the legitimate London Metal Exchange. One of these websites—"lme-enterprises.com"—was used to trick the Hawaii Victim into depositing cryptocurrency into what the victim believed was a legitimate cryptocurrency exchange.

33. Based on an interview conducted with the Hawaii Victim, law enforcement knows that the Hawaii Victim was first contacted by the LME Crypto Group after receiving a "wrong number" message on WhatsApp in or around February 2022. The individual who contacted the victim used the name "Aileen." Aileen and the victim engaged in casual conversation for approximately one week before Aileen began to explain to the victim how much money she had made trading cryptocurrency on "lme-enterprises.com" (hereinafter referred to as the "LME Enterprises Site"). The victim had no prior experience purchasing or trading cryptocurrency. Aileen gave the victim detailed instruction on how to purchase cryptocurrency from legitimate cryptocurrency exchanges and how to transfer the cryptocurrency to wallet addresses found on the LME Enterprises Site. The victim initially deposited $5,000 into the fraudulent LME Enterprises Site. After seeing apparent gains to the initial investment, Aileen told the victim about increased profits from "quick trading." Aileen explained that to conduct quick trading on the LME Enterprises

Site, a minimum investment of $50,000 was required, as well as a "lock-up" period for the option. The victim deposited the required amount into a trading option because the victim understood (based on information from the website) that this option would generate a 2% daily gain for 90 days for the "locked-up" cryptocurrency. After the end of the 90-day lock-up period, the Hawaii Victim observed and believed that the initial $50,000 investment increased to $145,000 on the LME Enterprises Site.

34. Aileen then informed the Hawaii Victim that the most lucrative investments on the LME Enterprises Site came from investing in Initial Coin Offerings ("ICOs"). The Hawaii Victim trusted Aileen after seeing their previous deposits appear to grow significantly. The Hawaii Victim in turn deposited approximately $800,000 on the LME Enterprises Site, believing to be investing in an ICO. The Hawaii Victim observed that the total amount of available capital in the LME Enterprises Site grew to approximately $8,000,000 upon completion of the ICO investment.

35. The Hawaii Victim then attempted to transfer some of this apparent capital out of the LME Enterprises Site back to a legitimate cryptocurrency exchange to convert the cryptocurrency to U.S. dollars and other fiat currency. Instead, the Hawaii victim received an email from another LME-related address—"support@lme.show"—which stated that the Hawaii Victim needed to deposit money as collateral for the withdrawal, because such a large withdrawal was prevented by government regulations. The Hawaii Victim then transferred $550,000 worth of additional cryptocurrency to the LME Enterprises Site to unlock their funds and withdraw their investment and gains. To date, the Hawaii Victim has not been unable to withdraw any assets.

36. The perpetrators of this scam are primarily referred to herein as the LME Crypto Group because the investigation began with entities impersonating the London Metal Exchange.[5]

[5] There may be other fraudulent domains also impersonating the London Metal Exchange. This naming convention for the group does not imply that all LME spoofed domains are necessarily run by the same group.

The investigation has identified over 80 domains being operated by this group and the websites are nearly identical to one another, with names such as "lme-partners.com" or "lmedex.com," referencing LME. The websites also use the same back-end data set, which means that the login credentials for one website can be used to login to other LME associated websites. These domains can be further tied together by shared infrastructure such as a shared web host, shared support email addresses, and commingling of stolen cryptocurrency from multiple different domains. This group has impersonated other entities (such as CoinMarketCap,[6] the London International Financial Futures and Options Exchange ("LIFFE"), Tether, and the Chicago Mercantile Exchange) and runs a variety of web domains to facilitate CIF scams.

37. At least one victim of the LME group, interviewed by the FBI, resides in the District of Columbia ("DC Victim"), and was in the District of Columbia when they were in communication with and sent funds to the LME Crypto Group. The DC Victim reported "investing" $30,000 in cryptocurrency in an app called "LME" in or around October 2022 and stated that they "thought it was an investment to earn big profits in a short amount of time." The domains the DC Victim reported using during the scam were "lme-partners.com" and "lmedex.com," which, as noted above, have been identified and attributed to the LME Crypto Group by the FBI.

38. To date, the FBI is aware of at least 85 web domains which can be tied to the LME Crypto Group by shared infrastructure, such as application distribution domain, shared web host, shared support email addresses, and commingling of stolen cryptocurrency from multiple different domains.

[6] CoinMarketCap (www.coinmarketcap.com/) is website primarily utilized to check the market price of various cryptocurrencies.

The Illinois Victim

39. A victim located in Illinois ("Illinois Victim") lost approximately $60,000 worth of cryptocurrency to bull-tycoon.net ("Bull Tycoon"), which is a domain that law enforcement attributes to the LME Crypto Group. The Illinois Victim began proactively researching cryptocurrency investing and Bitcoin ("BTC") around May and/or June of 2024. Shortly thereafter, the Illinois Victim received a seemingly random message on their cell phone from Mikako Chiba ("Chiba"). Chiba quickly befriended the Illinois Victim, built rapport, and transitioned the conversation to the WhatsApp platform. The Illinois Victim and Chiba exchanged personal and semi-romantic messages, with the conversation eventually transitioning to the topic of cryptocurrency.

40. Chiba convinced the Illinois Victim to invest an initial $100 at Kraken.[7] Chiba advised the Illinois Victim to convert the investment into BTC and to keep at least $100 worth of assets in the Kraken account to avoid account closure. Chiba also suggested the Illinois Victim download the Strike[8] application. Chiba assisted the Illinois Victim in establishing accounts at Kraken and Strike, as well as purchasing BTC. Chiba then guided the Illinois Victim to transfer the BTC to Bull Tycoon for investment. The Illinois Victim believed Bull Tycoon was a legitimate cryptocurrency trading platform.

41. Chiba represented herself as working with a team of experts and a supercomputer to predict BTC prices and make money mining BTC. Chiba hosted weekly WhatsApp chats on Tuesdays which involved her providing advice on investments. Chiba claimed others were on these chats, however, the Illinois Victim was not sure who the other participants were. The Illinois Victim's

[7] Kraken (www.kraken.com) is a U.S. based cryptocurrency exchange.
[8] Strike (www.strike.me) is a U.S based company operating a mobile application platform to acquire cryptocurrency, primarily Bitcoin.

initial trading method with Bull Tycoon involved trading once per week and betting on whether the price of BTC would go up or down. This moved to another investment opportunity by putting BTC into accounts that would mine BTC. These accounts would gain interest over time, between 3% and 25% interest depending on how many days the mining position was held. Chiba claimed she did independent reviews of the BTC deals conducted on Bull Tycoon. Chiba claimed to have been called by the FBI and advised the Illinois Victim not to worry if the FBI called to discuss cryptocurrency.

42. In total, the Illinois Victim put $60,000 of BTC into Bull Tycoon and has been unable to withdraw any BTC. Chiba told the Illinois Victim that she put a million dollars into the Illinois Victim's Bull Tycoon account to allow for further trades, but the Illinois Victim now believes this was not the case. The account appeared to grow to $17 million worth of BTC, but the Illinois Victim was unable to withdraw money and was, for a time, attempting to send another $30,000 to the account to be able to withdraw money. The Illinois Victim last communicated with Chiba in mid-September 2024, when the Illinois Victim decided to exit Bull Tycoon. Upon exiting the Bull Tycoon platform, the Illinois Victim gave Chiba the password to their Bull Tycoon account. She came back to the Illinois Victim and advised she did not have full access to the account.

Analysis of Bitcoin Addresses Relevant to the Illinois Victim

43. The FBI obtained records from Kraken for the Illinois Victim's account. In total, the Illinois Victim made five BTC transactions from their Kraken account to Bull Tycoon BTC address bc1px0jrexmzlefw8slm3mxldz9sxchxxr58d02nc5udeu645e27awaq7ang6k ("ang6k"). The FBI also obtained records from Crypto.com for an account controlled by the Illinois Victim, and identified an additional transaction of approximately $10,103.60 to ang6k. These combined six transactions totaled approximately $90,056 worth of BTC, with the cost calculated at the time of each transaction. The Illinois Victim's BTC sent to ang6k comprised the entirety of BTC received by ang6k as of the

time of this application.

Transaction Hash	Date/Time	USD worth of BTC at the time of each transaction
6e8bf3694440b23e9fc95e2fc7cd8f1b869af323180db08c5edbae69819e1216	8/26/2024 13:55	$15,045.28
4b048a0ab9a1a9455fe52af170d2478e74dcf5c0021792d5d15903e8e4c92793	8/21/2024 17:32	$15,781.71
216a0312690f312b5c2d57558ae753a6dc5f8c0c90347a86e5aacfbf89f33d89	8/12/2024 15:43	$18,164.98
b87a17ed3779a108c61355e7d29f9285e8cdb63a785c45a0988c293352b4bf6b	7/15/2024 17:07	$25,700.37
4fed8ca6c780eb656212a473d8bc92b69be1b521d344f23308817e2756253936	7/10/2024 2:05	$4,844.47

(BTC transactions made from the Illinois Victim's Kraken account to ang6k)

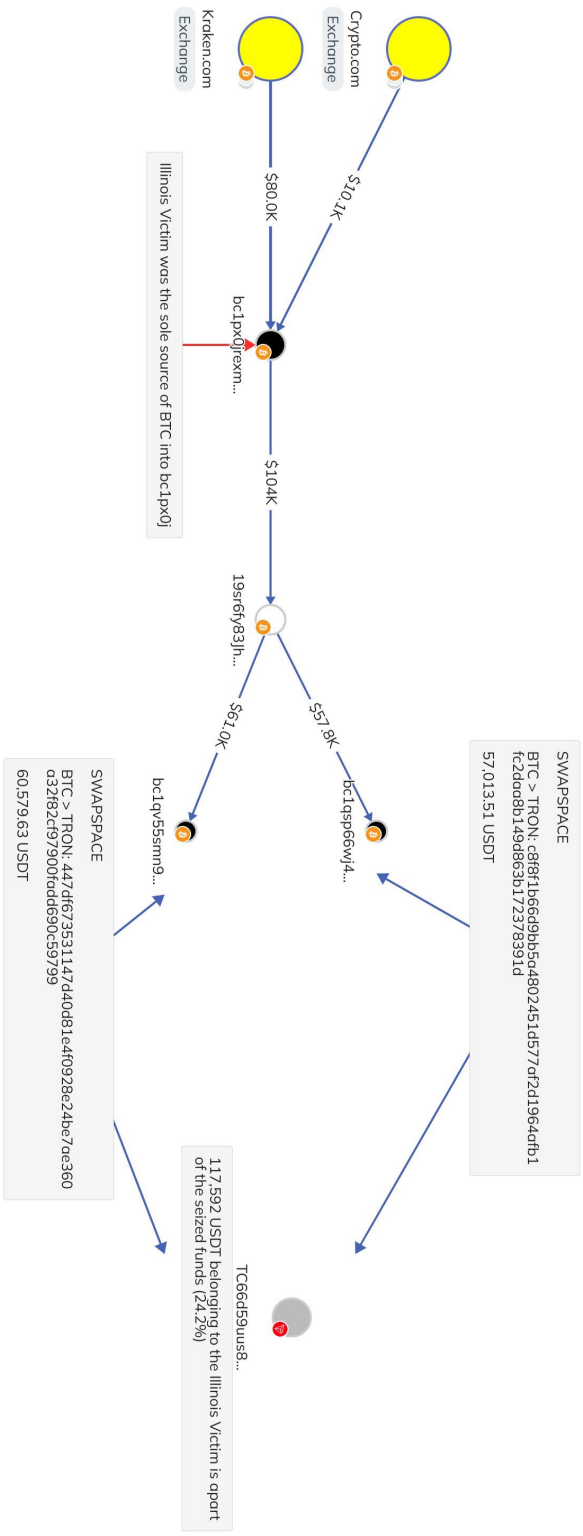
44. On or about October 29, 2024, the entirety of the BTC balance (1.47075503 BTC worth approximately $104,308.23) of ang6k was sent to 19sr6fy83JhYoTUmmTigXkh6AKp1oMMBz6 ("MMBz6"). This was one of thirteen transfers made of BTC into the MMBz6 address. Evidence from similar situations suggest that the actors making the transactions were consolidating funds into the MMBz6 address in order to prepare to move them together into another address. Stolen cryptocurrency is often consolidated in one address in preparation to launder the stolen funds through multiple external accounts. In total, 5.36532379 BTC worth approximately $380,672.97 was received by MMBz6 on October 29, 2024.

45. Shortly after the last inbound transaction, MMBz6 sent six outbound transactions to BTC addresses controlled by SwapSpace.[9] These six transactions occurred on or about October 29, 2024, between 7:57 AM UTC and 12:37 PM UTC. The six transactions consisted of approximately

[9] SwapSpace (swapspace.co/) is a cryptocurrency exchange aggregator which allows users to swap between two different cryptocurrencies.

5.1 BTC worth approximately $360,666.41, nearly all the BTC received by MMBz6. The entirety of the BTC sent from MMBz6 to SwapSpace was swapped from BTC to USDT on the Tron Network. In total, 359,217.08 USDT_TRX (USDT which resides and is transacted on the Tron Network) was sent to Tron address TC66d59uus8AWhYDvAgWM55T8NRa7KNWAN ("KNWAN") (one of the Subject Virtual Currency Addresses). The SwapSpace transfers from MMBz6 to KNWAN had a listed email address of lingxingyu999@gmail.com and all login IP addresses were geolocated to Cambodia. In addition, the FBI has previously seized approximately 327,146.95 USDT from a Binance account that was registered with the same email address lingxingyu999@gmail.com pursuant to a seizure warrant issued by a District Court in the District of Hawaii on February 21, 2024.

46. The 359,217.08 USDT received via the SwapSpace transfers on October 29, 2024, made up approximately 73.98% of all USDT_TRX received by KNWAN to date. Shortly after these transfers, there were two withdrawals of 10,000 USDT_TRX from KNWAN on or about October 30, 2024 and on or about November 2, 2024. On or about November 4, 2024, Tether froze KNWAN at the request of the FBI. At the time of the freeze of KNWAN, approximately 24.2% of all USDT_TRX located at KNWAN was traceable to the Illinois Victim.



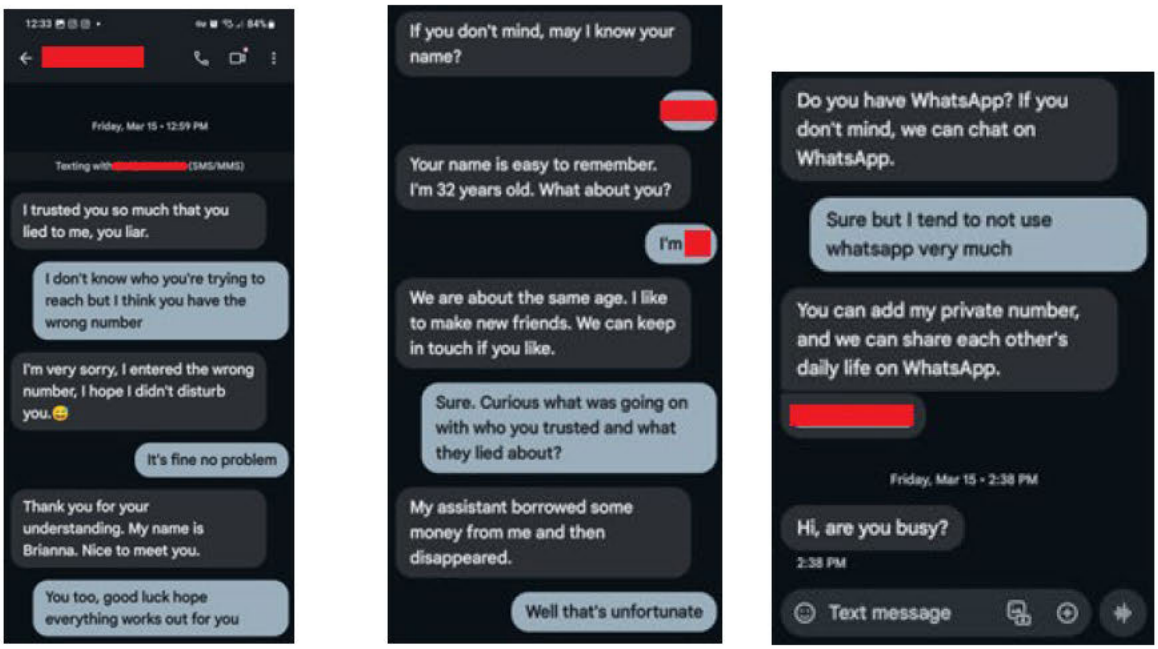
(Visual Aid detailing funds stolen from the Illinois Victim sent to KNWAN)

The Texas Victim

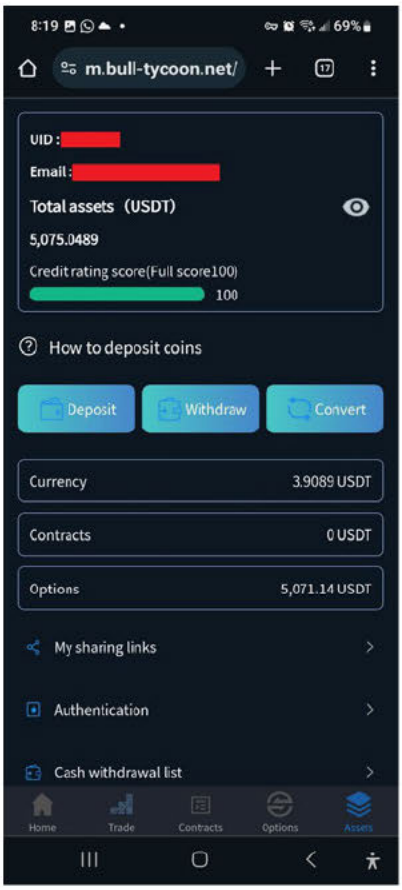
47. In or around July 2024, the FBI received a report via IC3 from an individual located in Texas ("Texas Victim"). The Texas Victim reported losing approximately $5,000 of cryptocurrency to m.bull-tycoon.net ("Bull Tycoon"),[10] which is a known domain operated by the LME Crypto Group. The Texas Victim sent cryptocurrency to Bull Tycoon via Ether, USDT, and Bitcoin. The Texas Victim was introduced to Bull Tycoon by an individual named "Brianna," who sent the Texas Victim a "mis-directed" text message. After a brief period of rapport building, Brianna moved the conversation to WhatsApp and introduced the Texas Victim to Bull Tycoon. Brianna helped the Texas Victim create an account at Bull Tycoon and ultimately transfer approximately $5,000 worth of cryptocurrency to the fraudulent platform. To date, the Texas Victim has been unable to withdraw any funds from Bull Tycoon and has received multiple communications asking to pay bogus fees/taxes to unlock their investment.

48. Included below are screenshots of a conversation between the Texas Victim and Brianna, the Texas Victim's Bull Tycoon account dashboard, the cryptocurrency transaction, and full address.

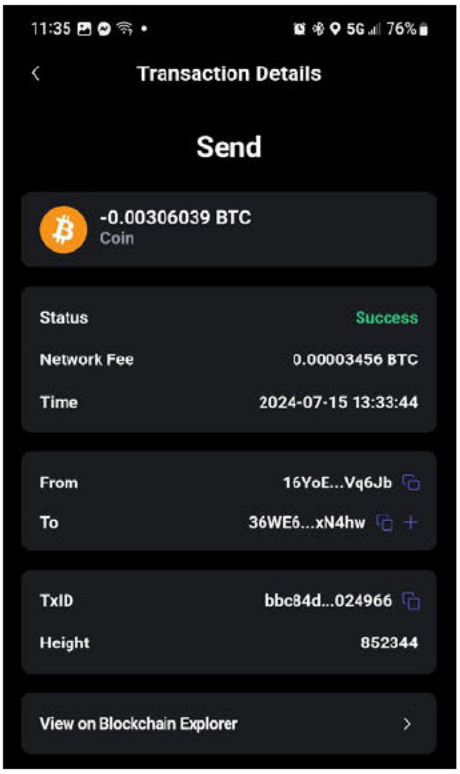
[10] The domain "bull-tycoon.net" contained a subdomain of "m." Based on my training and experience, the "m" subdomain is likely used to deliver a webpage that is compatible with mobile device screen size and resolution.



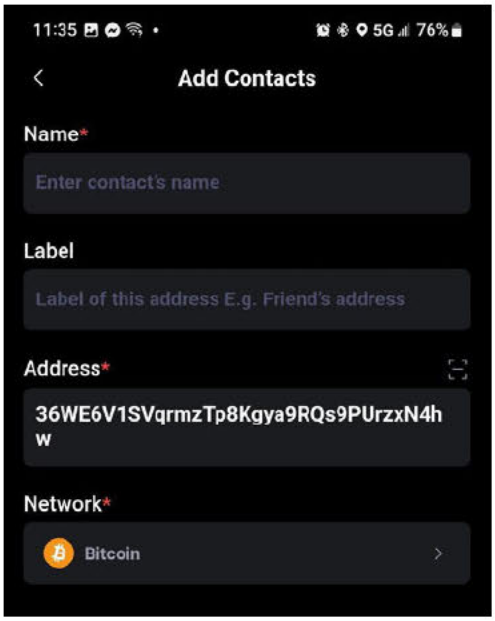
(Screenshot provided by the Texas Victim of the initial contact from Brianna)



(Screenshot provided by the Texas Victim of their Bull Tycoon account dashboard)



(Screenshot sent by the Texas Victim detailing a bitcoin transaction sent to Bull Tycoon deposit address 36WE6…xN4hw)



(Screenshot sent by the Texas Victim showing the full address for 36WE6…xN4hw)

The Florida Victim

49. An individual from West Palm Beach, Florida ("Florida Victim") filed an IC3 report in or around February 2025. The Florida Victim reported a loss of $259,000 to a cryptocurrency confidence scheme carried out by an individual he met on WhatsApp named "Sandy." The Florida Victim had previously been identified by the FBI as a likely victim of the LME Crypto Group due to observed communications between the Florida Victim and LME Crypto Group-attributed infrastructure. In the Florida Victim's complaint, they stated they had utilized Strike to send cryptocurrency to the scam operation which Sandy had introduced.

Analysis of Bitcoin Addresses Relevant to the Texas & Florida Victims

50. On or about July 15, 2024, the Texas Victim sent 0.00306039 BTC to 36WE6V1SVqrmzTp8Kgya9RQs9PUrzxN4hw ("36WE6"). 36WE6 received a total of 1.31018281 BTC between on or about June 28, 2024, and on or about August 19, 2024. On October 20, 2024, 36WE6 sent the entirety of its BTC holdings (sans fees), 1.31006437 BTC, to 166429kBXqFZLfhMjw5WM6MJ3yFMDHhrgM ("HhrgM"). This time period overlaps with the time the Texas Victim was "investing" on the fraudulent platform.

51. The FBI received records from Strike pertaining to selected funding sources of HhrgM. The Florida Victim sent three BTC transactions from their Strike account to bc1qvulygn35l3c7uspcj9lvacrzhk6gmccgppar3x ("par3x"), which constituted the sole deposits made to par3x to date. Subsequently, all of the BTC received to date by par3x had been sent to HhrgM.

Date	Receiving Address	Counterparty Address	BTC Value	USD Value
9/5/2024 22:16	bc1qvulygn35l3c7uspcj9lvacrzhk6gmccgppar3x	bc1qdrv8tacv0feev4pd5aja7z3hqf3qa5a2vazctl	0.52815537	29654.43794
9/6/2024 4:03	166429kBXqFZLfhMjw5WM6MJ3yFMDHhrgM	166429kBXqFZLfhMjw5WM6MJ3yFMDHhrgM	-0.52815085	-29880.2919
9/12/2024 2:03	bc1qvulygn35l3c7uspcj9lvacrzhk6gmccgppar3x	bc1qy6a3rrw9enmj6ywngdtwm26kun8ss4eavd9kv5	0.85898677	49930.66765
9/12/2024 4:00	166429kBXqFZLfhMjw5WM6MJ3yFMDHhrgM	166429kBXqFZLfhMjw5WM6MJ3yFMDHhrgM	-0.85898112	-50035.39474
9/19/2024 22:20	bc1qvulygn35l3c7uspcj9lvacrzhk6gmccgppar3x	bc1qwgpy4eh9dj3dlczcwvq6j53kdhhmg0n9qkfnhz	0.62975088	39629.47122
9/20/2024 3:28	166429kBXqFZLfhMjw5WM6MJ3yFMDHhrgM	166429kBXqFZLfhMjw5WM6MJ3yFMDHhrgM	-0.62974636	-39751.52588

(Visual aid detailing in/out BTC from the Florida Victim to par3x and into consolidation address Hhrgm)

52. The HhrgM BTC address conducted activity that is indicative of consolidation activity between on or about September 9, 2024, and on or about October 29, 2024. This consolidation activity is indicative of the initial centralization of funds for the purpose of laundering the funds through multiple subsequent transactions. In total, HhrgM received 6.27641579 BTC from multiple addresses, including 36WE6. HhrgM sent the majority of this BTC out in 11 separate transactions, which occurred from on or about September 23, 2024, to on or about October 29, 2024. All 11 of these outbound transactions were sent to a bitcoin address controlled by SwapSpace.

53. All of the BTC sent to Hhrgm from par3x was sent to SwapSpace, converted to USDT_TRX, and sent to TH4qXPSp3S5g3HnDr1pgnEq4XAoJh7McvZ ("7McvZ"). In total, McVZ received approximately 89,107.14 USDT_TRX that is connected to the Florida Victim's stolen BTC.

54. The FBI received information from SwapSpace pertaining to these 11 BTC transactions. The SwapSpace account these transactions were made through was the same account utilized to swap the Illinois Victim's funds from the Bitcoin Network to the Tron Network, registered with email address lingxingyu999@gmail.com. All 11 conversion transactions were from BTC to USDT_TRX, and the resulting USDT was sent to two different addresses: 334,491.98 USDT was sent to 7McvZ and 87,137.04 USDT was sent to KNWAN (the Subject Virtual Currency Addresses).

55. The USDT_TRX received by 7McvZ from the lingxingyu999@gmail.com SwapSpace transactions comprises approximately 68.57% of all USDT_TRX received by 7McvZ to

date, including the 0.00306039 BTC converted by SwapSpace originally from the Texas Victim, as well as the 2.01689302 BTC from the Florida Victim. 7McvZ was blacklisted by Tether on or about November 4, 2024, at the request of the FBI.

COUNT ONE – FORFEITURE OF DEFENDANT PROPERTY
(18 U.S.C. § 981(a)(1)(C))

56. The Defendant Property includes property constituting or derived from proceeds traceable to wire fraud and conspiracy to commit wire fraud, in violation of 18 U.S.C. §§ 1343 and 1349.

57. Accordingly, the Defendant Property is subject to forfeiture to the United States under 18 U.S.C. § 981(a)(1)(C).

COUNT TWO – FORFEITURE OF DEFENDANT PROPERTY
(18 U.S.C. § 981(a)(1)(A))

58. The Defendant Property constitutes property involved (a) domestic and international concealment money laundering transactions committed in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 1956(a)(2)(B)(i), (b) a conspiracy to engage in money laundering, committed in violation of 18 U.S.C. § 1956(h), and (c) violations of 18 U.S.C. § 1957.

59. Accordingly, the Defendant Funds are subject to forfeiture to the United States under 18 U.S.C. § 981(a)(1)(A).

PRAYER FOR RELIEF

WHEREFORE, the United States of America prays that notice issue on the Defendant Property as described above; that due notice be given to all parties to appear and show cause why the forfeiture should not be decreed; that this Honorable Court issue a warrant of arrest *in rem* according to law; that judgment be entered declaring that the Defendant Property be forfeited to the United States of America for disposition according to law; and that the United States of America be granted such other relief as this Court may deem just and proper.

Respectfully submitted,

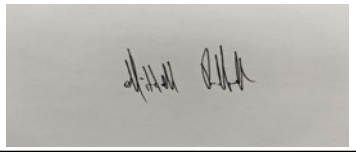
JEANINE FERRIS PIRRO
United States Attorney

/s/ Rick Blaylock, Jr.
Rick Blaylock, Jr.
TX Bar No. 24103294
Assistant United States Attorney
Asset Forfeiture Coordinator
United States Attorney's Office
601 D Street, N.W.
Washington, D.C. 20001
(202) 252-6765
rick.blaylock.jr@usdoj.gov

VERIFICATION

I, Mitchell Rubbelke, a Special Agent with the Federal Bureau of Investigation, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *in rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 2nd day of September 2025.



Mitchell Rubbelke
Special Agent
Federal Bureau of Investigation