IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

UNITED STATES OF AMERICA Plaintiff,	§ § §	
v.	§ §	NO: 4:25-CV-01315
4,230,250.809 USDT Defendant.	§ §	

AFFIDAVIT IN SUPPORT OF COMPLAINT FOR FORFEITURE

I, Christopher Hunt, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), and have been since August 2019. I am currently assigned to the Cyber Crimes group in Dallas, Texas. As a Special Agent, my responsibilities include enforcing federal laws as set forth in the United States Code, including those referenced in this application. I have conducted and led numerous investigations of criminal enterprises and individual criminal activity for acts in violation of state and federal statutes and have utilized various investigative techniques. I have also received formal and informal training from the DHS and other organizations on investigation techniques, computer technology, and cybercrime tactics. I have participated in the execution of warrants involving the search and seizure of computers and electronically stored information.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, analysts, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause

for the requested forfeiture. It does not set forth all my knowledge, or the knowledge of others, about this matter.

PROPERTY FOR FORFEITURE

3. This Affidavit is made in support of a civil forfeiture complaint concerning the following personal property:

4,230,250.809 USDT seized from Tether deposit addresses

- TCm8KpVmsdmxN2XdCbjfd3LojVZvKNNXzq;
- TGZRXdDqeVHUq7CJsRwCDoiBKMiEJY7EGW;
- TL5mAVHa6u7ywZUv4XWFiskNJkq7Y4XsWL;
- TKYNeiWCuU9jEGCjNhE98wPcDcq1LnFsHy;
- TTisQyMK4pdwb8gtd8V62gLavLV7uLKGAV; and
- TLpL1z7ARXRPfKBjFacRPUYgeGgEbnXCa1

on or about November 6, 2024, pursuant to a seizure warrant approved by a United States Magistrate Judge for the Eastern District of Texas in Case No. 6:24-MJ-250 (the "Defendant Property").

LEGAL AUTHORITY FOR FORFEITURE

4. Based on my training and experience and the facts as set forth in this affidavit, the funds to be forfeited represent proceeds of a fraudulent cryptocurrency investment scheme. I believe these funds are proceeds derived from violations of 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud), and 18 U.S.C. § 1343 (Wire Fraud) and were involved in violations of 18 U.S.C. § 1956(h) (Conspiracy to Commit Money Laundering), 18 U.S.C. § 1956 (Money Laundering).

5. 18 U.S.C. § 1343 (Wire Fraud) prohibits, in pertinent part, whoever, having devised to 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, from transmitting or causing to be transmitted by means of wire, radio or television communication in interstate or foreign commerce, any writings, signs, signals, pictures or sounds for the purpose of executing such scheme or artifice. 18 U.S.C. § 1349 prohibits conspiring to commit wire fraud in violation of 18 U.S.C. § 1343.

6. 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering) prohibits, in pertinent part, 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 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. 18 U.S.C. § 1956(h) prohibits conspiring to commit money laundering.

7. I believe the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C). Under 18 U.S.C. § 981(a)(1)(A), "[a]ny property, real or personal, involved in a transaction or attempted transaction" in violation of 18 U.S.C. §§ 1956 or 1957 or "any property traceable to such property" is subject to forfeiture to the United States. Under 18 U.S.C. § 981(a)(1)(C), "[a]ny property, real or personal, which represents or is traceable to the gross receipts obtained, directly or indirectly, from a violation of" "any offense

constituting 'specified unlawful activity,' or a conspiracy to commit such offense" is subject to forfeiture to the United States.[1]

DEFINITIONS AND TECHNICAL BACKGROUND CONCERNING THE CRIMINAL CONDUCT

8. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

9. A domain name is a simple, easy-to-remember way for humans to identify computers on the internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular IP address. For example, "usdoj.gov" and "cnn.com" are domain names.

10. The term "spoofed" refers to domain spoofing and involves a cyberattack in which fraudsters and/or hackers seek to persuade consumers that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a false site controlled by a cybercriminal.

11. The term "shell company" describes businesses that exists primarily as a means to conduct financial maneuvers and which typically have no employees, provide no actual business or service, and offer some anonymity to the beneficial owners. Criminal entities use shell companies to establish business bank accounts so that large sums of monies can be transacted with less potential suspicion from financial institutions. Bank accounts belonging to shell companies are frequently closed by financial

[1] Wire fraud in violation of 18 U.S.C. § 1343 and conspiracy to commit wire fraud under 18 U.S.C. § 1349 both constitute a "specified unlawful activity" pursuant to 18 U.S.C. §§ 1956(c)(7)(A) and 1961(1).

institutions because of fraud reports made by victims. As a result, shell companies are often used to open accounts at different financial institutions.

BACKGROUND ON VIRTUAL CURRENCY

12. **Virtual Currency**: Virtual currencies are digital tokens of value circulated over the Internet. Virtual currencies are typically not issued by any government or bank like traditional fiat currencies, such as the U.S. dollar, but rather are generated and controlled through computer software. Different virtual currencies operate on different blockchains, and there are many different, widely used virtual currencies currently in circulation. Bitcoin (or BTC) and Ether (ETH) are currently the most well-known virtual currencies in use. BTC exists on the Bitcoin blockchain, and ETH exists on the Ethereum network. Typically, a virtual currency that is "native" to a particular blockchain cannot be used on a different blockchain. Thus, absent technological solutions, those native assets are siloed within a specific blockchain. For instance, ETH (the native token on the Ethereum network) cannot be used on other networks unless it is "wrapped" by smart contract code. This wrapping process results in what is called Wrapped ETH or WETH.

13. **Stablecoins:** Stablecoins are a type of virtual currency whose value 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. Stablecoins achieve their price stability via collateralizations (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

14. **Tether (USDT):** Tether Limited ("Tether") is a company that manages the smart contracts and the treasury (*i.e.,* the funds held in reserve) for USDT, a stablecoin

pegged to the U.S. dollar. Unlike other cryptocurrencies such as Bitcoin whose price tends to fluctuate more unpredictably, Tether tries to hold its value around a specific asset. As a stablecoin, it is pegged or "tethered" to the U.S. dollar as the coin's name suggests in order to minimize price volatility. Payments or transfers of value made with Tether are recorded on blockchains and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire Tether through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), cryptocurrency ATMs, or directly from other people. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Tether transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it is not completely anonymous, Tether allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

15. **Virtual Currency Address**: Virtual currency addresses are the particular virtual locations to 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.

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

17. **Virtual Currency Wallet**: Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26–63 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

18. There are various types of virtual currency wallets, including software wallets, hardware wallets, and paper wallets. The virtual currency wallets at issue for the purposes of this affidavit are software wallets (*i.e.,* 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.

19. 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.

20. Although cryptocurrencies have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an frequently used means of payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transactions.

21. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or

removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (*e.g.*, Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[2] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

22. **Blockchain**: Many virtual currencies publicly record all their transactions on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by the decentralized network of computers, containing an immutable and historical record of every transaction utilizing that blockchain's technology. 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.

[2] A QR code is a matrix barcode that is a machine-readable optical label.

23. **Blockchain Explorer**: These explorers are online tools that operate as a blockchain search engine allowing users the ability to search for and review transactional data for any addresses on a particular blockchain. A blockchain explorer is software that uses API[3] and blockchain nodes to draw data from a blockchain and uses a database to arrange and present the data to a user in a searchable format.

24. **Smart Contracts**: Smart contracts are computer programs stored on a blockchain that run when predetermined conditions are met. Typically, they are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement. The Ethereum network is designed, and functions based on smart contracts.

25. **Virtual Currency Bridge:** A blockchain bridge, otherwise known as a cross-chain bridge, connects two blockchains and allows users to send virtual currency from one chain to the other.

26. **Virtual Currency Exchanges (VCEs)**: VCEs are trading and/or storage platforms for virtual currencies, such as BTC and ETH. There are generally two types of VCEs: centralized exchanges and decentralized exchanges, which are also known as "DEXs." Many VCEs also store their customers' virtual currency in virtual currency wallets. As previously stated, these wallets can hold multiple virtual currency addresses associated with a user on a VCE's network. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers (*i.e.*,

[3] API is an initialism for "application programming interface," which is a set of definitions and protocols for building and integrating application software.

KYC checks) and to have anti-money laundering programs in place (to the extent they operate and service customers in the United States).

27. **Instant VCEs**: Instant exchanges allow their customers to swap (*i.e.*, exchange) one virtual currency for another. Instant exchanges typically do not act as a custodian of their customers' assets in the way that larger VCEs do. In other words, a customer would not store his or her virtual currency on an Instant VCE's platform; instead, he or she would conduct trades and then either move funds to a third-party VCE that acts as a custodian (*i.e.*, a hosted wallet) or move funds to his or her unhosted wallet.

28. **Virtual Currency Mixers:** Virtual currency mixers (also known as tumblers or mixing services) are software services that allow users, for a fee, to send virtual currency to designated recipients in a manner designed to conceal and obfuscate the source of the virtual currency. Based on my training and experience, I know that virtual currency mixers are a common laundering tool used by criminal cyber actors and their money laundering co-conspirators.

29. **Blockchain Analysis:** As previously stated, while the identity of a virtual currency address owner is generally anonymous, law enforcement can identify the owner of a particular virtual currency address by analyzing the blockchain (*e.g.*, the Bitcoin blockchain). The analysis can also reveal additional addresses controlled by the same individual or entity. "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).

30. Law enforcement can trace transactions on blockchains to determine which virtual currency addresses are sending and receiving particular virtual currency. This analysis can be invaluable to criminal investigations for many reasons, including that it may enable law enforcement to uncover transactions involving illicit funds and to identify the person(s) behind those transactions. To conduct blockchain analysis, law enforcement officers use reputable, free open-source blockchain explorers, as well as commercial tools and services. These commercial tools are offered by different blockchain-analysis companies. Through numerous unrelated investigations, law enforcement has found the information associated with these tools to be reliable.

31. In addition to using publicly available blockchain explorers, law enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions. Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

32. **Decentralized Finance (DeFi)**: Decentralized Finance, or DeFi, is an umbrella term for financial services on public blockchains, primarily the Ethereum network. The Ethereum network's native virtual currency is ETH. Ethereum was the first blockchain that offered various decentralized services within its network. To make these

services possible, the Ethereum network allows other tokens besides ETH to run within the network. These tokens are known as ERC-20 tokens.

33. DeFi is a term used to describe a financial system that operates without the need for traditional, centralized intermediaries. Instead, DeFi platforms offer an alternative financial system that is open for anyone to use, and that allows centralized intermediaries to be replaced by decentralized applications (or dApps). With DeFi, one can do most of the things that banks support—earn interest, borrow, lend, buy insurance, trade derivatives, trade assets, etc.—but it is faster than using traditional banks and does not require paperwork or a third party. DeFi is global, peer-to-peer (*i.e.*, directly between two people rather than routed through a centralized system), pseudonymous, and open to the public.

FACTS SUPPORTING FORFEITURE

34. The United States is investigating a fraud and money laundering scheme. The investigation concerns possible violations of, inter alia, 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud), 18 U.S.C. § 1956 (Money Laundering), and 18 U.S.C. § 1956(h) (Conspiracy to Commit Money Laundering). This investigation has revealed that the Defendant Property consists of proceeds from various wire fraud schemes within the United States, including within the Tyler Division of the Eastern District of Texas.

35. In October 2024, HSI Dallas began an investigation of a criminal money laundering syndicate operating remote employment platforms. In particular, the unknown scammers promoted spoofed domains and websites purporting to look like

legitimate remote employment platforms to U.S.-based victims, including victims located in Frisco, Texas, which is within the Eastern District of Texas. Scammers then fooled victims into depositing cryptocurrency through these fraudulent remote employment platforms, which instead allowed the scammers to steal the victims' money.

36. This type of scam is often identified as "pig butchering" (derived from the Chinese phrase used to describe this scheme) and involves scammers spending significant time getting to know, targeting, and grooming their victims to gain their confidence. After developing a relationship and gaining trust, scammers instruct their victims to visit the spoofed domains to get them to make significant capital deposits in what victims believe are legitimate remote employment platforms. The victims are then typically asked to deposit their funds through a provided cryptocurrency (*e.g.*, BTC, USDT, ETH, or USDC) deposit address and are further told they can expect to make a sizeable return on their investments through the fraudulent remote employment platform. As initial smaller investments are made, the spoofed websites falsely display a significant increase in the victim's account balance, which entices the victim to continue making payments, which typically end with a final large deposit or transaction. When the victim attempts to make a withdrawal, the scammers attempt to coerce the victims to make additional investments. These tactics can include requesting additional deposits due to cover the "withdraw fees" or other reasons such as freezing the account due to "taxes owed" or "suspicious behavior." Regardless of how the scammers attempt to solicit additional deposits from the victims, the victims are unable to retrieve any portion of their deposits.

37. On or about October 17, 2024, HSI Dallas identified a report filed by A.M. in Frisco, Texas that stated he believed he may have been a victim of an illegal remote employment cryptocurrency scheme.

38. On or about August 16, 2024, A.M. received a text message from an unidentified female via the mobile communication application WhatsApp. The unidentified female inquired if A.M. was interested in a remote employment opportunity. Following a brief conversation with the unidentified female, A.M. stated that all communications regarding potential employment and/or with the "company" was transferred to an individual going by the name "Lin" (WhatsApp #'s646-239-7516 & 212-920-1206). A.M. stated "Lin" coached him on completing the employment tasks and gaining a higher status within the company. A.M. stated "Lin" instructed him to create an account on the website https://differentialworkbrench.cc. A.M. stated his "differentialworkbrench" account monitored his commissions earned for completing the required employment tasks. Additionally, A.M. stated the "differentialworkbrench" account monitored the employee's negative balance or commonly referred to as a deficit.

39. A.M. stated in order to achieve a higher status within the company, he was required to complete more "tasks" and ultimately provided the funds for the required "training." A.M. stated as a result of this training/ higher status cycle he made four (4) separate Coinbase transactions comprised of USDC and Ethereum to the company. A.M. provided the following four transactions that the company and/or "Lin" requested him to send the funds for the remote employment cryptocurrency scheme:

Transaction #1
Transaction Hash: 0xd9caaa84dbdf9c6af91bf02a73df30721483de963d1ba8c14504a537532246b4
From: 0x7830c87C02e56AFf27FA8Ab1241711331FA86F43
To: 0xC3f74889153e29Cf09b65A396f878dB7e7d36B54
Amount: 9,716.738151 USDC
Time: 9/7/2024 04:41:11 PM UTC
Transaction #2
Transaction Hash: 0x0e12beec88ef4d856139833e952fa497451f0debfa5ea5f7662489c3a8835121
From: 0x7830c87C02e56AFf27FA8Ab1241711331FA86F43
To: 0x616359E7616a37055C0c6B102066B1E6A3Ef9F95
Amount: 17,989.10247 USDC
Time: 9/9/2024 04:05:11 PM UTC
Transaction #3
Transaction Hash: 0xef65e8995f56a90bb07b61045778162da4eb3b59adeba8e93bf2a825f1b59896
From: 0xA9D1e08C7793af67e9d92fe308d5697FB81d3E43
To: 0x43510370769683e17D3D20c287F2f92425CA84CB
Amount: 19.07187369 ETH
Time: 9/11/2024 09:02:11 PM UTC
Transaction #4
Transaction Hash: 0x85ebb6943c394f28078eaa2ea2b9155ba16e7d493164d492283be1971f163b60
From: 0x7830c87C02e56AFf27FA8Ab1241711331FA86F43
To: 0x6c34b1450c3Df60f0c2EeD1E92EB555c22ffF8a8
Amount: 34.5438009 ETH
Time: 9/12/2024 08:38:11 PM UTC

40. A.M. stated upon the completion of the final task, he attempted to withdraw his funds that had accumulated in his "differentialworkbrench" account. A.M. stated the company advised him of additional costs associated with his training. A.M. stated the company would not release his funds in his "differentialworkbrench" account unless the deficit was paid in full.

41. All of A.M.'s cryptocurrency transactions were traced to the Subject Tether (USDT) addresses, as detailed below. The traces were conducted using the Last-In, First-

Out accounting principle – meaning the most recently deposited items are recorded as the next withdrawal.

Tracing of Victim Funds to the Subject USDT Addresses

42. On October 17, 2024, special agents with HSI conducted Blockchain analysis on the four transactions that originated from A.M.'s Coinbase account that were ultimately sent to the fraudsters. A.M.'s four transactions of Ethereum and USDC on the Ethereum blockchain ultimately ended up in Ethereum address 0x672A0bAE90828677a0F93e012FdE1914375DbCaB. To obfuscate the source of the funds that were obtained via fraud, the fraudsters used a bridge function to convert one cryptocurrency to another cryptocurrency in the form of a swap.

43. Record checks and blockchain analysis show that A.M.'s funds ultimately ended up on the Tron blockchain in the form of the token Tether (USDT) on Tron cryptocurrency address TCm8KpVmsdmxN2XdCbjfd3LojVZvKNNXzq. The Tron address associated with the initial amount of Tether received from the swap was approximately 238,214 USDT. Utilizing Blockchain analysis, HSI special agents traced the funds traveling through several wallets and ultimately commingling with other funds suspected to be related to fraudulent activity, which aided in further obfuscation of the fund's origin.

44. The following Tron addresses were utilized:

- TCm8KpVmsdmxN2XdCbjfd3LojVZvKNNXzq
- TY8jRsk6UfkR5nCK6svZFkAeBNkqRLvsWu
- TGZRXdDqeVHUq7CJsRwCDoiBKMiEJY7EGW

- TL5mAVHa6u7ywZUv4XWFiskNJkq7Y4XsWL
- TV9uiAR1L3WbcZzuXv7yYXqCPRJvPao5og
- TAeRqXh1ZTWp49DF251J889hhXLd5bmd7C
- TF3jJnqFSActfyNfG1PrpWXDwPys9UmGHe
- TKYNeiWCuU9jEGCjNhE98wPcDcq1LnFsHy
- TTisQyMK4pdwb8gtd8V62gLavLV7uLKGAV
- TLpL1z7ARXRPfKBjFacRPUYgeGgEbnXCa1

The following Tron addresses still contain USDT that are related to A.M.'s movement of funds:

- TCm8KpVmsdmxN2XdCbjfd3LojVZvKNNXzq
- TGZRXdDqeVHUq7CJsRwCDoiBKMiEJY7EGW
- TL5mAVHa6u7ywZUv4XWFiskNJkq7Y4XsWL
- TKYNeiWCuU9jEGCjNhE98wPcDcq1LnFsHy
- TTisQyMK4pdwb8gtd8V62gLavLV7uLKGAV
- TLpL1z7ARXRPfKBjFacRPUYgeGgEbnXCa1

The total approximate value of USDT in the aforementioned accounts is 4,230,250.809 USDT.

45. The aforementioned funds will remain seized in place until they are transferred to HSI-controlled addresses.

46. On or about December 4, 2024, HSI Dallas received email correspondence from The Potu & Partners Law Office based in Jakarta, Indonesia. This law firm was acting as legal representation for the purported owner of the two seized wallets

mentioned below. "We are writing on behalf of our client who is the owner of 2 (two) USDT wallets with the following wallet addresses":

- 1st wallet: TTisQyMK4pdwb8gtd8V62gLavLV7uLKGAV

- 2nd wallet: TLpL1z7ARXRPfKBJFaRPUYgeGqEbnXCa1

Combined value of wallets (Approx): $2,900,000.00 USDT

The law firm stated an Indonesian National named Antoni BUDIANTO was the rightful owner of the two aforementioned wallets. The law firm stopped responding to all email correspondence in or about May of 2025. Neither BUDIANTO nor Potu & Partners filed a formal petition or claim with DHS for the aforementioned seized cryptocurrency.

47. In October 2025, HSI Dallas was notified by the Fines Penalties & Forfeiture (FP&F) Division of Customs & Border Protections (CBP), of a formal petition filed for the same two wallets previously claimed by BUDIANTO (TTisQyMK4pdwb8gtd8V62gLavLV7uLKGAV and TLpL1z7ARXRPfKBJFaRPUYgeGqEbnXCa1). An Indonesian National named Kevin SOH provided over 800 pages of documentation in order to demonstrate the source of the aforementioned funds. None of the documentation provided illustrated the source of the funds, but merely duplicated transfers conducted by victims of the remote employment cryptocurrency scheme.

CONCLUSION

I submit that this affidavit supports probable cause to forfeit all funds, assets, and other things of value up to 4,230,250.809 USDT seized from Tether deposit addresses:

- TCm8KpVmsdmxN2XdCbjfd3LojVZvKNNXzq

- TGZRXdDqeVHUq7CJsRwCDoiBKMiEJY7EGW
- TL5mAVHa6u7ywZUv4XWFiskNJkq7Y4XsWL
- TKYNeiWCuU9jEGCjNhE98wPcDcq1LnFsHy
- TTisQyMK4pdwb8gtd8V62gLavLV7uLKGAV
- TLpL1z7ARXRPfKBjFacRPUYgeGgEbnXCa1

on or about November 6, 2024.

48. Based on my experience and the information herein, I have probable cause to believe that the seized 4,230,250.809 USDT constitutes proceeds from a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)), are traceable to a money laundering transaction in violation of 18 U.S.C. §§ 1956 and 1957 and are therefore subject to forfeiture pursuant to pursuant to 18 U.S.C. § 981(a)(1)(A).

49. I also have probable cause to believe that the seized 4,230,250.809 USDT constitutes proceeds traceable to a violation of 18 U.S.C. § 1343 and/or 18 U.S.C. § 1349, and are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

As provided in 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Respectfully submitted,

Christopher Hunt

Christopher Hunt
Special Agent
Homeland Security Investigations