UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA **v.** **APPROXIMATELY 11,814,265 USDT** **Defendant, *in rem.***	§ § § § § § § § §	**COMPLAINT FOR FORFEITURE *IN REM*** ***CIVIL ACTION NO.*** **25-cv-3912**

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 11,814,265 USDT, hereinafter referred to as "Defendant Property", and alleges as follows:

STATEMENT OF THE CASE

1. Criminals believed to be located abroad, their associates, and conspirators together stole funds from at least 15 victims. The funds were then laundered through a series of virtual currency addresses, and often virtual currency exchanges, to evade detection and hide the origin of the funds. The Federal Bureau of Investigation (FBI), investigated, traced, and seized the Defendant Property, which constitutes proceeds traceable to those thefts and property involved in, and traceable to, this 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 illegal activities, and most importantly, to recover assets that may be used to compensate victims.[1]

JURISDICTION AND VENUE

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

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) and (b).

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), and 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.

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 of concealment of 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.

PROPERTY INFORMATION

15. The Defendant Property is 11,814,265 USDT, which is the equivalent to $11,814,265 in U.S. dollars (USD). The Defendant Property is associated with virtual currency addresses:

0xfd10797c02bbCF25E879D8e1d955ef5876FA095b (Subject Address 1);

0x4A4693FCB71204D6C84A6a7e5f795F57b1D44b7b (Subject Address 2);

0x8369E85FdC3C739D7d13AA41022181B4058B8Ae8 (Subject Address 3);

0x45D542E7ea62afe999d5335C8282d740008694da (Subject Address 4);

0xF5C757885BC82384daC6f9d4f170e82a35bA3b8C (Subject Address 5);

0x2d762190Ca7486066EABfEe0C9b2ce841f31A372 (Subject Address 6);

0x8013E1B5Ccc9b508092941EC8ec6f6aA903D3E60 (Subject Address 7);

0x2EF166b673b0933b664393e9e7C5d315179B34De (Subject Address 8);

0xC9AF3Dc1A24D89dCC32B0B6936Ab7CfC58804236 (Subject Address 9); and

0x0Ef6a7200Fb762A1C1f4ae85e58F6dca99465905 (Subject Address 10);

(collectively the "Subject Addresses"), which altogether held 11,814,265 USDT. The currency previously associated with the Subject Virtual Currency Addresses is hereinafter referred to as the "Defendant Property."

16. The Defendant Property is currently in custody and control of the United States Marshals Service.

STATEMENT OF FACTS

Background on Cryptocurrency

17. **Virtual Currency:** Virtual currencies are digital representations of value that, like traditional coin and paper currency, function as a medium of exchange (i.e., they can be digitally traded or transferred, and can be used for payment or investment purposes). Virtual currencies are a type of digital asset separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets. The exchange value of a particular virtual currency generally is based on agreement or trust among its community of users. Some virtual currencies have equivalent values in real currency or can act as a substitute for real currency, while others are specific to particular virtual domains (e.g., online gaming communities) and generally cannot be exchanged for real currency. Cryptocurrencies, like Bitcoin and Ether, are types of virtual currencies, which rely on cryptography for security. Cryptocurrencies typically lack a central administrator to issue the currency and maintain payment ledgers. Instead, cryptocurrencies use algorithms, a distributed ledger known as a blockchain, and a network of peer-to-peer users to maintain an accurate system of payments and receipts.

18. **Blockchain:** A blockchain is a digital ledger run by a decentralized network of computers referred to as "nodes." Each node runs software that maintains an immutable and historical record of every transaction utilizing that blockchain's technology. Many digital assets, including virtual currencies, publicly record all their transactions on a blockchain, including all of the known balances for each virtual currency address on the blockchain. Blockchains consist of blocks of cryptographically signed transactions, and blocks are added to the previous block after validation and after undergoing a consensus decision to expose and resist tampering or manipulation of the data. There are many different blockchains used by many different virtual currencies. For

example, Bitcoin in its native state exists of the Bitcoin blockchain, while Ether (or "ETH") exists in its native state on the Ethereum network.

19. **Blockchain Analysis:** 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.

20. **Virtual Currency Address:** A virtual currency address is an alphanumeric string that designates the virtual location on a blockchain where virtual currency can be sent and received. A virtual currency address is associated with a virtual currency wallet.

21. **Virtual Currency Exchange:** A virtual currency exchange ("VCE"), also called a virtual currency exchange, is a platform used to buy and sell virtual currencies. VCEs allow users to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa. Many VCEs also store their customers' virtual currency addresses in hosted wallets. VCEs can be centralized (i.e., an entity or organization that facilitates virtual currency trading between parties on a large scale and often resembles traditional asset exchanges like the exchange of stocks) or decentralized (i.e., a peer-to-peer marketplace where transactions occur directly between parties).

22. **Virtual Currency Wallet:** A virtual currency wallet (*e.g.,* a hardware wallet, software wallet, or paper wallet) stores a user's public and private keys, allowing a user to send and

receive virtual currency stored on the blockchain. Multiple virtual currency addresses can be controlled by one wallet.

23. **Unhosted Wallet:** An unhosted wallet, also known as a self-hosted, 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. Unhosted wallets allow users to generate and manage their own unhosted wallet addresses.

24. **Hosted Wallet:** A hosted wallet, also known as a custodial wallet, is a virtual currency wallet through which a third party, *e.g.*, a virtual currency exchange, holds a user's private keys. The third party maintains the hosted wallet on its platform akin to how a bank maintains a bank account for a customer, allowing the customer to authorize virtual currency transactions involving the hosted wallet only by logging into/engaging with the third party's platform.

25. **Decentralized Exchange**: A decentralized exchange (or "DEX") is a peer-to-peer marketplace where users can trade virtual currencies directly with other traders without centralized intermediaries. Users generally retain control over their virtual currency rather than entrusting a central authority to host funds in a centralized or "hosted" wallet. DEXs are operated by self-executing agreements written in code, known as "smart contracts," which automate the trading process. DEXs will algorithmically track the prices of various virtual currencies and often leverage locked reserves of virtual currencies (or other digital assets). These locked reserves are known as "liquidity pools," and they are often used to facilitate trades. DEXs are built on blockchains that support smart contracts, including Ethereum, and often levy fees for their services.

26. **Transaction Fee:** A transaction fee is a fee paid by the party sending virtual currency on a blockchain to reward miners and/or validators for verifying and validating transactions.

Transaction fees vary by blockchain and can fluctuate based on factors such as blockchain network traffic and transaction sizes. Senders of virtual currency can increase the transaction fees that they pay to have their transactions confirmed faster by miners and/or validators. Transaction fees are generally paid in a blockchain's native token (*e.g.*, Bitcoin on the Bitcoin blockchain). On the Ethereum network, these transaction fees are called "gas fees." Gas fees are transaction costs paid in Ether ("ETH"), or its fraction, gwei. These fees serve as a form of remuneration for validators who maintain and secure the network. Gas fees fluctuate based on supply, demand, and network capacity, and may increase during periods of network congestion.

27. **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. For example, Tether (also known as USDT) is a stablecoin 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.

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

29. **Ether:** Ether ("ETH") is a virtual currency that is the native token used by the Ethereum blockchain, which is a blockchain with smart contract functionality.

30. **Dai:** Dai ("DAI") is a "stablecoin" virtual currency with its value tied to the US dollar. DAI is issued by the decentralized autonomous organization MakerDAO.

Background on Cryptocurrency Investment Fraud

31. 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 alone, more than 41,000 complaints of CIF were

received by the FBI's Internet Crime Complaint Center (IC3), resulting in $5.8 billion in reported losses.[2] CIF schemes are often orchestrated by Asia-based criminal syndicates, predominately operating in southeast Asia.

32. In CIF schemes, criminals contact potential victims through seemingly misdirected text messages, dating applications, or other online platforms/forums with the goal of building rapport and relationships with the victims.

33. Once that trust is established, the criminal recommends virtual currency 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 subject usually instructs and/or assists the victim with opening an account on a centralized virtual currency exchange, such as Coinbase or Crypto.com, and then walks the victim through transferring money from a bank account to that virtual currency exchange account. Next, the victim will usually receive instructions on how to transfer their virtual currency assets to the fake investment platform. On its surface, the platform typically shows lucrative returns, encouraging further investment. However, in reality, all deposited funds are routed to a virtual currency address controlled by the criminals.

34. In CIF schemes, the subjects will continue to encourage investments until victims have depleted their savings. Oftentimes, the subject will attempt to continue the scheme by coaching victims on taking out loans against their homes or borrowing money from friends and family.

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

Inevitably, these victims generally 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, subjects 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 subjects 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 subjects will continue to concoct new excuses and fees for victims to pay.

Wire Fraud Scheme

M.P. – INITIAL VICTIM

35. The FBI engages in proactive measures to identify active victims of CIF. This effort enables the FBI to contact these victims, oftentimes before the victim is aware of the scam, and thus prevent additional funds from being lost. In or around January 2024, FBI San Diego learned of a CIF victim, M.P., who had already reportedly lost over $730,000.[3]

36. In or around November 2023, following her divorce, M.P. joined the dating website eHarmony and met a man who went by the name of Jack ZHANG ("ZHANG"). Zhang claimed to be from China and spoke both Mandarin and English. M.P. and ZHANG initially communicated through eHarmony and then migrated to WhatsApp at ZHANG's request. ZHANG was very kind and communicated with M.P. every morning.

37. After talking for some time, ZHANG encouraged M.P. to invest in virtual currency. Although M.P. was hesitant and initially resisted, ZHANG persistently pushed M.P. to invest. Around the beginning November 2023, at the direction of ZHANG, M.P. signed up at a non-custodial

[3] M.P. and other victims will be referred to throughout using female pronouns, but those do not necessarily indicate the gender of the individuals.

wallet service, and created accounts at virtual currency exchanges Crypto.com and Kraken. M.P. transferred money from her bank account to both Crypto.com and Kraken to purchase virtual currency. She then transferred that virtual currency to her non-custodial wallet (specifically an address beginning with 0x114594). ZHANG then directed M.P. to access the investment platform GateVPS.com and transfer funds from her wallet to GateVPS.com, which was an alleged trading platform.[4] M.P. believed this trading platform was real since it had a contract and terms and conditions. Using screenshots M.P. provided of her bank and virtual currency exchanges, ZHANG was able to coach her through the entire process.

38. M.P. started by investing small amounts of money and was initially able to make small withdrawals. M.P.'s investments in GateVPS.com appeared to grow substantially and ZHANG encouraged M.P. to invest larger and larger amounts to take advantage of profitable trading opportunities and make higher profits. In total, M.P. invested over $730,000, withdrawing much of the funds from her 401(k). M.P.'s GateVPS.com account balance, including her alleged profits, appeared to grow to approximately $1.28 million.

39. In or around January 2024, M.P. received a notification from the FBI warning her she may be a victim of virtual currency investment fraud. Upon receiving the email, M.P. attempted to withdraw her funds but was only permitted to withdraw $5,000 USD.[5] M.P. attempted further withdrawals from GateVPS.com, which were all denied. The website stated M.P. must pay a 10% fee of the full account balance in order to withdraw her money – a fee that GateVPS.com was requiring M.P. to pay with a new source of funds as opposed to withholding 10% from any

[4] As of on or about February 5, 2025, the FBI had received 21 reports referencing GateVPS.com as a fraudulent investment platform. These reports all outline schemes similar to what M.P. experienced. All complaints were submitted to the Internet Crime Complaint Center (ic3.gov).
[5] CIF schemes will often allow users to withdraw relatively small amounts to avoid detection and continue the scheme.

withdrawal. Based on M.P.'s final "would-be" account balance at GateVPS.com, this fee would have required M.P. to pay approximately $128,000 before being eligible for more withdrawals. However, since M.P. recognized it was a scam, she did not pay any fines, taxes, or fees.

40. Given his close role in promoting her investments, M.P. recognized that ZHANG was a part of the GateVPS.com scam. In an effort to scare ZHANG into returning her money, M.P. told him that she was contacted by the FBI. Despite this, ZHANG would not release any of the funds and M.P. terminated contact with him.

41. The figures below reflect conversations between ZHANG and M.P. via WhatsApp. The conversations demonstrate the language used by ZHANG to persuade M.P. to invest in virtual currency and show how ZHANG walked M.P. through the investment process. In addition, the conversations demonstrate how ZHANG coached M.P. to avoid fraud detection by her bank.

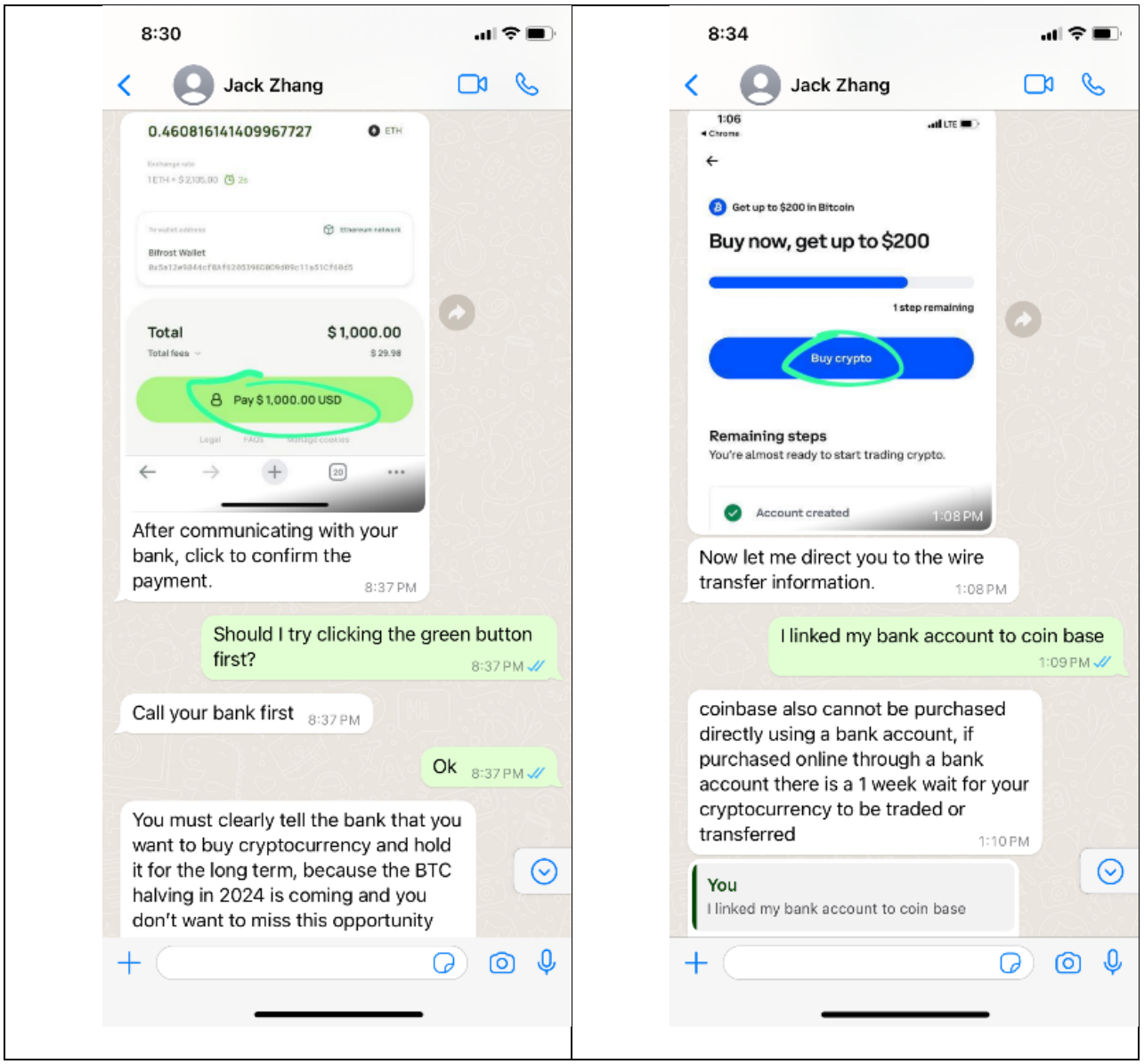

Figure 1 (above): Zhang Coaching M.P. to Invest in Crypto

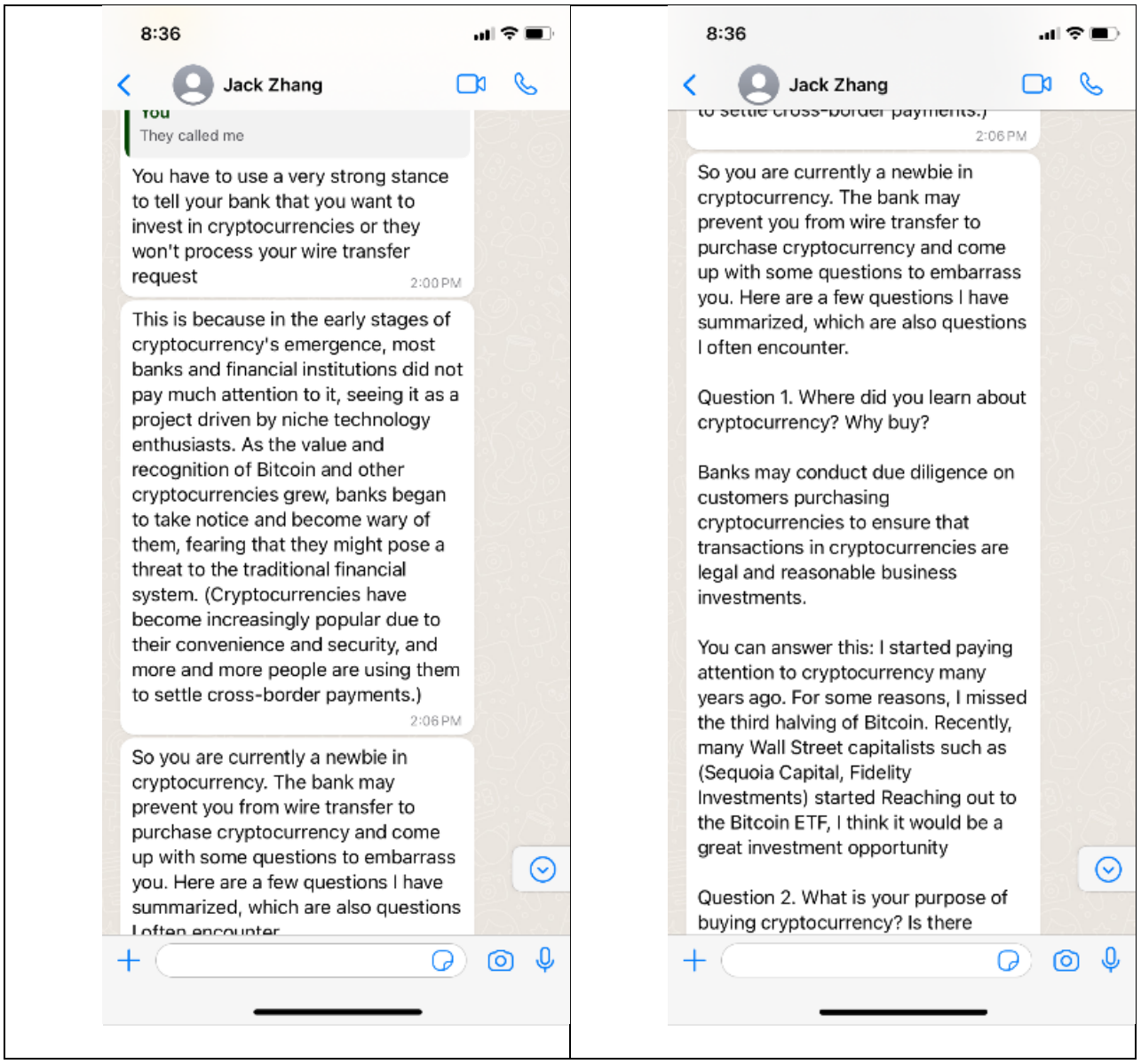

Figure 2 (above): Zhang Instructing M.P. on Bank Communications

FLOW OF M.P.'s FUNDS

42. As described above, M.P.'s funds were sent from her personal bank accounts to virtual currency exchanges, and then from exchanges to her unhosted wallet address. Table One, below, outlines seventeen ETH transactions where M.P.'s unhosted wallet address received virtual currency from her Crypto.com and Kraken exchange accounts and then subsequently sent those

funds to two wallet addresses she believed to be the GateVPS.com trading platform. This table does not include every transaction M.P. made through her unhosted wallet address.

Transaction Number	Date	Victim Exchange	Currency	Currency Amount from Exchange to M.P. Unhosted Wallet	Equivalent Amount USD	Currency Amount from M.P. Unhosted Wallet to Receiving Address	Equivalent Amount USD	Receiving Address (From M.P. Unhosted Wallet)
1	11/29/2023	Crypto.com	ETH	7.2530	14,711.19	-7.3400	(14,887.65)	0x78580f2be7c9fb3eed5ef6fd3785e7cafa45ed2d
2	11/30/2023	Crypto.com	ETH	7.1666	14,650.85	-7.1700	(14,713.53)	0x78580f2be7c9fb3eed5ef6fd3785e7cafa45ed2d
3	12/9/2023	Crypto.com	ETH	8.2351	19,424.02	-8.2400	(19,435.57)	0x78580f2be7c9fb3eed5ef6fd3785e7cafa45ed2d
4	12/12/2023	Crypto.com	ETH	4.3429	9,660.31	-4.3400	(9,653.86)	0x78580f2be7c9fb3eed5ef6fd3785e7cafa45ed2d
5	12/16/2023	Crypto.com	ETH	10.8470	24,307.93	-10.8500	(24,314.65)	0x78580f2be7c9fb3eed5ef6fd3785e7cafa45ed2d
6	12/22/2023	Crypto.com	ETH	21.1430	49,236.80	-42.2800	(98,459.63)	0x78580f2be7c9fb3eed5ef6fd3785e7cafa45ed2d
7	12/22/2023	Crypto.com	ETH	21.1430	49,236.80			0x78580f2be7c9fb3eed5ef6fd3785e7cafa45ed2d
8	12/25/2023	Crypto.com	ETH	3.9842	9,051.83	-3.9800	(9,042.28)	0x78580f2be7c9fb3eed5ef6fd3785e7cafa45ed2d
9	1/2/2024	Crypto.com	ETH	41.4500	98,209.60	-41.4500	(97,773.51)	0x4550191b59bb60af6bc4b129654e0ba1984e9554
10	1/8/2024	Crypto.com	ETH	21.4810	47,749.21	-21.4800	(47,746.98)	0x4550191b59bb60af6bc4b129654e0ba1984e9554
11	1/12/2024	Crypto.com	ETH	18.9950	47,936.35	-18.9900	(47,923.73)	0x4550191b59bb60af6bc4b129654e0ba1984e9554
12	1/14/2024	Crypto.com	ETH	1.9950	4,988.16	-2.0000	(5,000.66)	0x78580f2be7c9fb3eed5ef6fd3785e7cafa45ed2d
13	1/15/2024	Crypto.com	ETH	7.1239	17,607.91	-7.1200	(17,598.27)	0x4550191b59bb60af6bc4b129654e0ba1984e9554
14	1/17/2024	Crypto.com	ETH	29.7830	75,408.76	-29.7800	(75,401.17)	0x4550191b59bb60af6bc4b129654e0ba1984e9554
15	1/22/2024	Crypto.com	ETH	39.8000	97,708.50	-39.8000	(97,708.50)	0x4550191b59bb60af6bc4b129654e0ba1984e9554
16	1/22/2024	Kraken	ETH	42.0960	99,932.94	-42.1000	(99,579.57)	0x4550191b59bb60af6bc4b129654e0ba1984e9554
17	1/24/2024	Kraken	ETH	13.1310	29,423.38	-13.1300	(29,421.14)	0x4550191b59bb60af6bc4b129654e0ba1984e9554

Table 1 M.P.'s Transactions to Subject Addresses

43. FBI special agents and forensic accountants traced a portion of M.P.'s funds using reliable blockchain analysis tools. The funds were sent to two addresses (beginning with 0x455019 and 0x78580f) and were transferred through multiple intermediary addresses, comingling with other funds along the way. M.P.'s funds were ultimately transferred to ten addresses, referred to above as the Subject Addresses. On or about February 7, 2024, and on or about February 28, 2024, the Subject Addresses were frozen and held a total value of 11,814,265 USDT (see Table Two below).

Address #	Address	Shorthand Address	Freeze Request Date	USDT Balance
1	0xfd10797c02bbCF25E879D8e1d955ef5876FA095b	0xfd1079	2/7/2024	380,685
2	0x4A4693FCB71204D6C84A6a7e5f795F57b1D44b7b	0x4A4693	2/7/2024	960,012
3	0x8369E85FdC3C739D7d13AA41022181B4058B8Ae8	0x8369E8	2/7/2024	4,261
4	0x45D542E7ea62afe999d5335C8282d740008694da	0x45D542	2/7/2024	1,736,380
5	0xF5C757885BC82384daC6f9d4f170e82a35bA3b8C	0xF5C757	2/7/2024	6,470,108
6	0x2d762190Ca7486066EABfEe0C9b2ce841f31A372	0x2d7621	2/28/2024	87,647
7	0x8013E1B5Ccc9b508092941EC8ec6f6aA903D3E60	0x8012E1	2/28/2024	200,141
8	0x2EF166b673b0933b664393e9e7C5d315179B34De	0x2EF166	2/28/2024	102,352
9	0xC9AF3Dc1A24D89dCC32B0B6936Ab7CfC58804236	0xC9AF3D	2/28/2024	979,867
10	0x0Ef6a7200Fb762A1C1f4ae85e58F6dca99465905	0x0Ef6a72	2/28/2024	892,812
			Total	**11,814,265**

Table 2 (above): Subject Addresses' USDT Balances

44. As seen in Figure 3 (below), the ETH virtual currency that M.P. paid into the scam was laundered through numerous unhosted wallet addresses. All this virtual currency was quickly swapped into the virtual currency Dai ("DAI"). It was comingled with other funds and split up down different laundering paths – essentially scattering M.P.'s funds on the blockchain. Along these paths, M.P.'s virtual currency was swapped once again from DAI into Tether ("USDT"). This USDT, which had originally been the ETH that M.P. had sent to the scam, was ultimately laundered into all ten Subject Addresses.

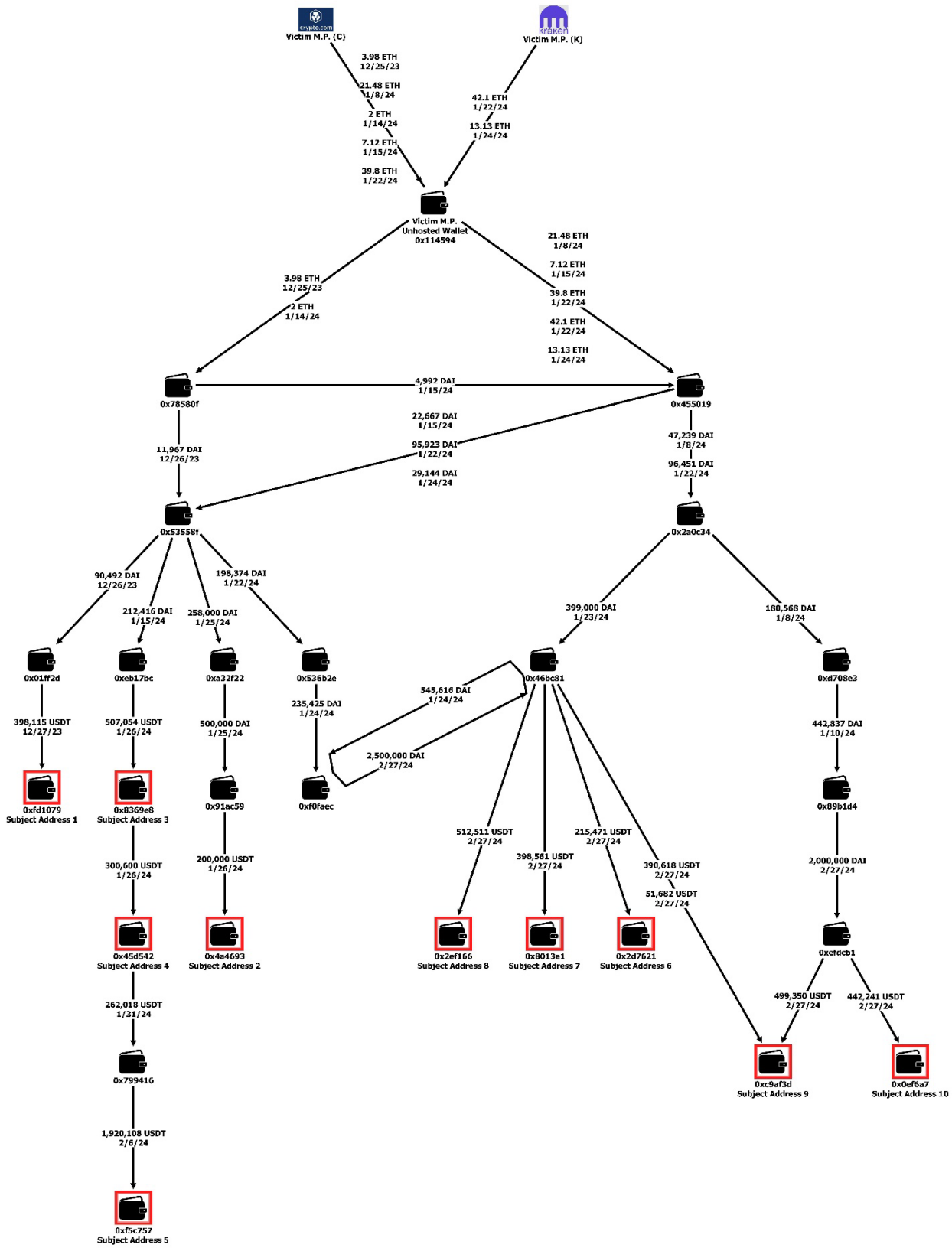

Figure 3 (above): Illustration of M.P.'s Flow of Funds to Subject Addresses

45. The above flow of funds (as seen in Figure 3) is indicative of concealment money laundering through virtual currency. At each stage above, various methods were used to try conceal or disguise the nature, location, source, ownership, or control of scam proceeds, and to thwart law enforcement's ability to trace, and ultimately recover, any illicit proceeds. Those methods include:

- **Leveraging Victim-Controlled Unhosted Virtual Currency Wallets (0x114594, Figure 3).** Criminals often coach victims to create new unhosted virtual currency wallet addresses in which to deposit their funds before sending them to what they believe to be the legitimate investment platform. In M.P.'s case, this was done using a wallet creation software called "Trust Wallet." Trust Wallet itself has its own web browser, called the Web3 portal. This portal enables users to access websites that are only available through similar portals, and not traditional web browsers, due to the sites themselves running on blockchain technology. Since victims are accessing the malicious investment websites within the Web3 portal, they are left with the impression that they are investing their virtual currency through their unhosted wallet address(es). This was the case with M.P., where she accessed GateVPS.com through Trust Wallet and initially believed that Trust Wallet was the culprit withholding her funds. This provides an additional barrier, where law enforcement cannot easily access the malicious websites and where victims cannot easily identify the scam.

- **Use of Unattributable "0 Level" Deposit Addresses (0x455019, 0x78580f, Figure 3).** 0 Level addresses are the initial deposit addresses in which victims deposit funds on the blockchain. These addresses are provided to victims by the criminals. Because of this, criminals usually provide unhosted wallets as 0 Level addresses to evade identification or potential interference by third parties. Such is the case here with 0x455019 and 0x78580f. Additionally, these 0 Level addresses are oftentimes only shared with one victim to make it more difficult for law enforcement and others to track and report common scams.

- **Use of Decentralized Exchanges (0x455019, 0x78580f, 0xeb17bc, 0x91ac59, 0x01ff2d, 0xefdcb1, 0x46bc81, Figure 3).**[6] Decentralized exchanges allow users to swap one virtual currency type for another, often without having to provide any identifying information (i.e., know your customer ("KYC") data), so users can remain anonymous. M.P.'s funds were swapped numerous times from the virtual currency Ether (ETH) to the virtual currency Dai (DAI), and later to the virtual currency Tether (USDT).

- **Swapping for Stablecoins, Especially USDT (numerous, Figure 3).** CIF scammers involved in laundering victims' funds regularly exchange or "swap" the non-stablecoin cryptocurrencies that victims send them for stablecoins, especially USDT**.** Money launderers are particularly drawn to USDT because of its low transaction fees and stability compared to other more volatile cryptocurrencies. Additionally, USDT is compatible on several different blockchains, which makes it easier to move funds across blockchains to further obfuscate the nature, source, control, and/or ownership of criminal proceeds.

- **High Velocity Flow of Funds to a Consolidation Wallet**. **(numerous, Figure 1).** Once deposited into the 0 Level Address, it is common for the funds to flow quickly from address to address before reaching a consolidation wallet, where the funds will rest for a longer period, allowing criminals time to comingle those funds with other illicit gains before moving the funds again towards a cash-out point where they can convert the pool of funds to fiat currency. M.P.'s funds reflect this method on numerous occasions by being transferred into, and out of, an address within hours or even minutes.

[6] The virtual currency swaps for M.P.'s funds occurred within the referenced addresses and their interaction with various decentralized exchanges.

- **Use of a Consolidation Wallet to Comingle Funds. (0x53558f, 0x2a0c34, Figure 3).** Defined as the "layering" stage of money laundering, funds derived from multiple victims are routed to the same address, where they are comingled, consolidated, and transferred together downstream. Criminals use consolidation wallets to try to obfuscate the source of funds and complicate tracing efforts by investigators. M.P.'s funds were comingled at almost every step, and ultimately passed through multiple consolidation wallets before entering the Subject Addresses in large transactions that contained funds from her and multiple other victims.

46. There is no reason, economic or otherwise, for legitimate businesses or individuals to conduct virtual currency transfers in the above fashion. Whether transferring Bitcoin (BTC) or, in this case, USDT, ETH, and DAI, each individual virtual currency transfer costs money. For USDT transferred on Ethereum, that cost comes through the payment of transactions fees, or "gas" fees, required by the Ethereum blockchain. It is reasonable to assume that businesses and individuals would strive to minimize those fees by conducting transfers with as few transactions, or "hops," as possible.

47. Based on this evidence, and additional evidence outlined below, unknown subjects orchestrated a criminal CIF scheme against M.P. and laundered her funds, and funds from other victims, into the Subject Addresses.

IDENTIFICATION OF ADDITIONAL VICTIMS

48. FBI special agents and forensic accountants performed blockchain analysis to trace transactions backwards from the Subject Addresses to eventually identify other 0 Level wallets that may have received victim deposits directly. It was determined that the identified 0 Level wallets received deposits from the virtual currency centralized exchanges Coinbase, Kraken, and Crypto.com. Investigators sent legal process to the exchanges to identify likely victim account

holders. The FBI's blockchain analysis was not conducted on all activity of the Subject Addresses, as it focused primarily on the funds still associated with the addresses following the freeze.

49. Through legal process to Coinbase, Kraken, and Crypto.com, review of IC3 reports, and subsequent interviews with identified account holders, investigators confirmed that the Subject Addresses contained additional victim proceeds. Specifically, victims with initials T.S., M.G., J.H., A.P., R.C.A., P.C., L.M., S.M., N.H., R.M., B.T.N., I.C.C, J.Y, and L.C.L. contributed proceeds to 0 Level addresses, which were ultimately transferred to the Subject Addresses.

50. As seen in Figure 4 (below), victims J.H., M.G., A.P., P.C., and R.C.A., sent either ETH or the stablecoin USDC to their respective scams. For all of these victims, this currency was swapped into DAI and later swapped into USDT before being sent to Subject Addresses 1, 2, or 10. For each of these victims, their virtual currency was laundered through a series of unhosted wallet addresses while being comingled with the funds of other victims. This transaction behavior, involving a series of rapid, same day "hops" across unhosted wallet addresses, before being consolidated into consolidation wallets, and habitually exchanging one stablecoin, DAI, for another, USDT, right before transferring it into Subject Addresses 1, 2, or 10, serves no legitimate financial purpose. Similar to the transaction activity displayed in Figure 3, this pattern-like transfer activity was conducted to obfuscate the nature, location, source, ownership, or control of these victims' stolen funds.

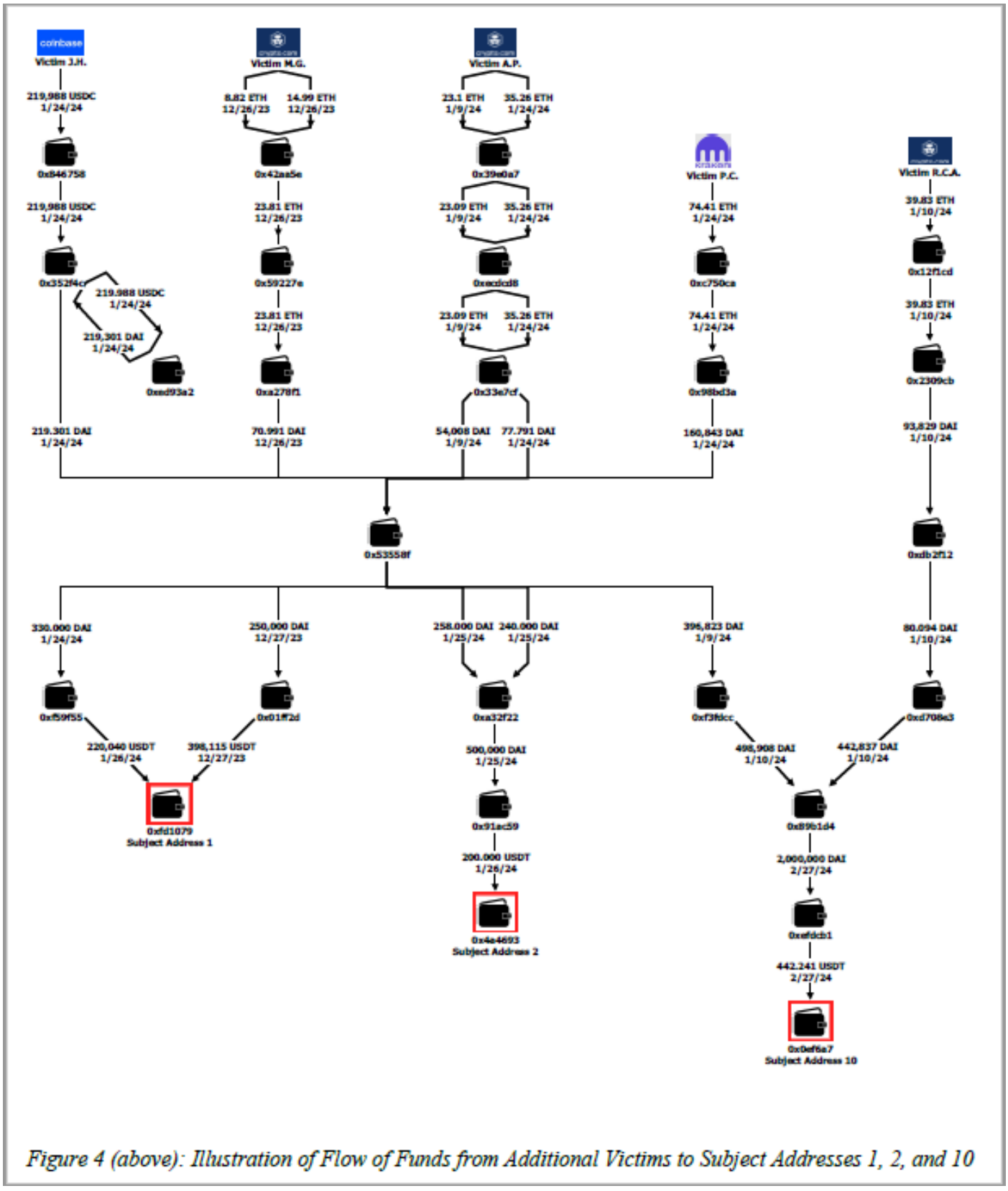

Figure 4 (above): Illustration of Flow of Funds from Additional Victims to Subject Addresses 1, 2, and 10

51. As seen below in Figure 5, victims S.M., L.C.L., I.C.C., T.S., J.Y., L.M., B.T.N., N.H., and R.M., sent either ETH or USDT cryptocurrencies to their respective scams. Other than S.M., N.H., and R.M., whose transfers were in USDT, the funds of the other victims were quickly swapped into DAI. The funds of all victims were later swapped into USDT, or remained as USDT, before being sent into Subject Addresses 3, 4, or 5. For each of these victims, their virtual currency was laundered through a series of unhosted wallet addresses while being comingled with the funds of other victims. The funds were eventually consolidated in Subject Address 4, before some of the funds were transferred to Subject Address 5**.** This transaction behavior also serves no legitimate financial purpose. Like the transaction activity displayed in Figures 3 and 4, this pattern-like transfer activity was conducted to obfuscate the nature, location, source, ownership, or control of these victims' stolen funds.

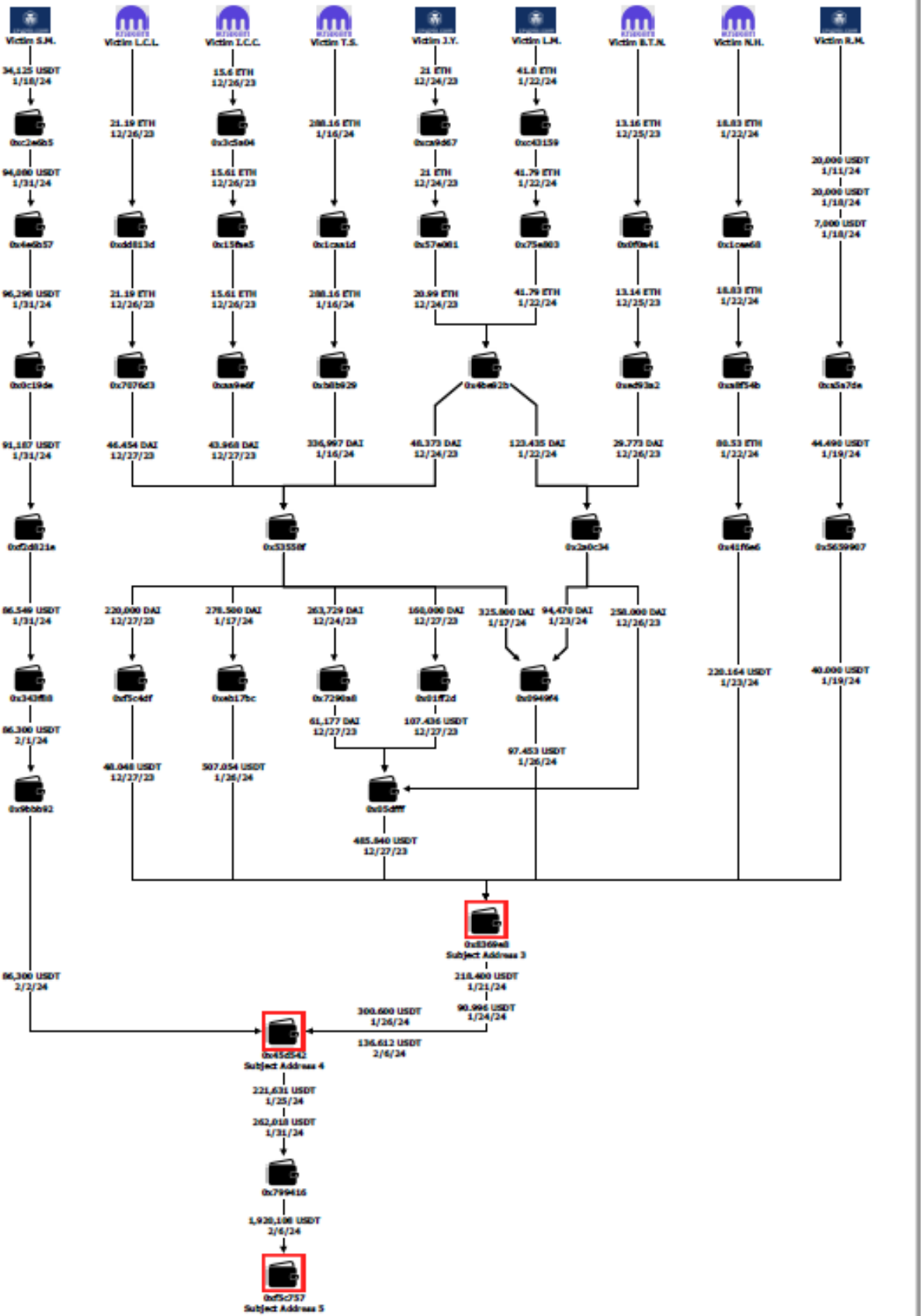

Figure 5 (above): Illustration of Flow of Funds from Additional Victims to Subject Addresses 3,4, and 5

52. As seen below in Figure 6, victims J.H., M.G., and L.M., sent either the virtual currency ETH or USDC from centralized exchange accounts at Coinbase and Crypto.com. In each case, their funds were quickly swapped into the virtual currency DAI before later being swapped into USDT and transferred into Subject Addresses 6, 7, 8, and 9. For each of these victims, their virtual currency was laundered through a series of unhosted wallet addresses while being comingled with the other victims' funds.

53. Also seen in Figure 6 (below), and earlier in Figure 3 of M.P.'s funds, the unhosted wallet address 0x46bc81 (abbreviation) played a pivotal role in the laundering of funds into multiple Subject Addresses. Specifically, Subject Addresses 6, 7, 8, and 9. 0x46bc81 itself has been flagged as associated with the scam "iceleo.com Pig Butchering Grouping" by a reliable blockchain analytical tool. This same tool has flagged 48.08% of the virtual currency that was transferred into 0x46bc8 as having passed through other addresses associated with scams or that were referenced in community complaints.

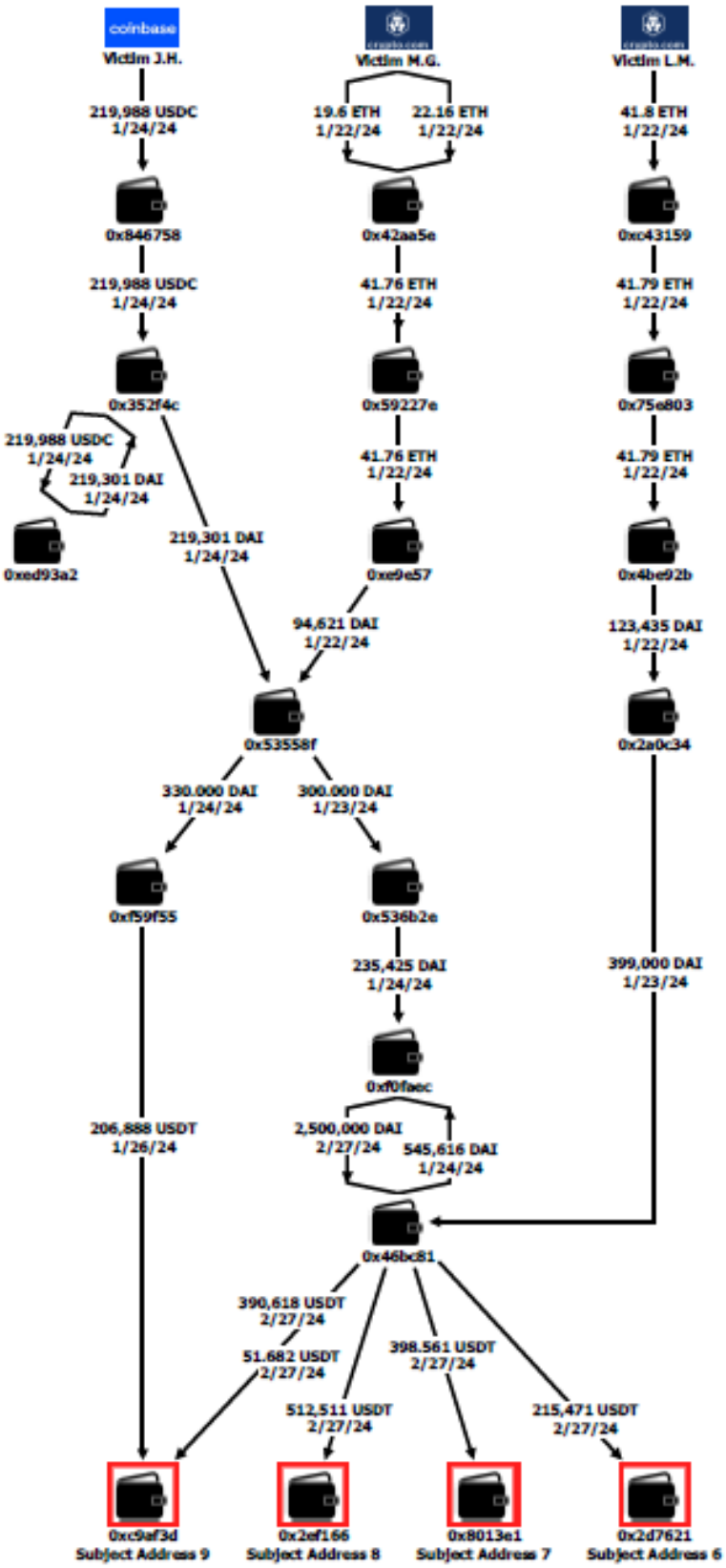

Figure 6 (above): Illustration of Flow of Funds from Additional Victims to Subject Addresses 6, 7, 8, and 9

54. On or about January 23, 2024, 0x46bc8 received 399,000 DAI containing proceeds from M.P. and other victims. The next day, 545,616 DAI was sent out to a second address. Within a couple minutes, this second address received 235,425 DAI, which also contained proceeds from M.P. and other victims that had been previously laundered down a separate path. This second address now contained comingled funds including those from the two transfers on or around January 24, 2024, and funds previously associated with this second address. The funds sat idle in the second address with no additional DAI received or sent for approximately one month, at which point those funds were sent in one transaction on or about February 27, 2024, of 2,500,000 DAI back to 0x46bc81.

55. 0x46bc81 then followed a rapid series of swapping DAI, via decentralized exchanges, for USDT before immediately sending the USDT to Subject Addresses 6, 7, 8, and 9. Within approximately 23 minutes, the user of 0x46bc81 converted 2,000,000 DAI into USDT and sent 1,568,995 USDT into these Subject Addresses through five transactions.

Date	Time	To/From	Amount	Virtual currency
2/27/2024	1:47 PM	From 0xf0fae	+ 2,500,000	DAI
2/27/2024	2:09 PM	To Decentralized Exchange SWAP	- 500,000	DAI
2/27/2024	2:09 PM	From Decentralized Exchange SWAP	+ 499,395	USDT
2/27/2024	2:13 PM	To SUBJECTADDRESS 8	- 512,511	USDT
2/27/2024	2:15 PM	To Decentralized Exchange SWAP	- 500,000	DAI
2/27/2024	2:15 PM	From Decentralized Exchange SWAP	+ 499,380	USDT
2/27/2024	2:18 PM	To SUBJECTADDRESS 7	- 398,561	USDT
2/27/2024	2:20 PM	To Decentralized Exchange SWAP	- 500,000	DAI
2/27/2024	2:20 PM	From Decentralized Exchange SWAP	+ 499,366	USDT
2/27/2024	2:23 PM	To SUBJECTADDRESS 6	- 215,471	USDT
2/27/2024	2:28 PM	To SUBJECTADDRESS 9	-390,618	USDT
2/27/2024	2:30 PM	To Decentralized Exchange SWAP	- 500,000	DAI
2/27/2024	2:30 PM	From Decentralized Exchange SWAP	+ 499,389	USDT
2/27/2024	2:32 PM	To SUBJECTADDRESS 9	- 51,682	USDT

Table 2: Accounting of the rapid blockchain activity within 0x46bc81[7]

56. This rapid pattern of swapping virtual currency and immediately redistributing the new tokens into multiple destinations is highly indicative of money laundering practices conducted to conceal the nature, source, ownership, and control of the funds. If any of the 2,500,000 DAI transferred into 0x46bc81 had originally been obtained legally, it was immediately comingled with the proceeds from multiple victims, facilitating the commission of money laundering. However, based on the consistent money laundering techniques used, the pairing of funds from multiple victims, from multiple paths, flowing into that 2,500,000 DAI transfer, it is likely that the full 2,500,000 DAI was originally obtained through illegal means. Therefore, it is likely that any

[7] All dates, times, and amounts in the table are approximations.

subsequent transaction into Subject Addresses 6, 7, 8, and 9, is made up of funds illegally obtained from multiple victims. The funds currently associated with Subject Addresses 6, 7, and 8, are made up entirely of these subsequent transactions. As mentioned earlier in this section, each of these addresses has a transaction history that is indicative of money laundering. Subject Address 9, while also having a suspicious transaction history, contains funds that were from the 2,500,000 DAI transaction as well as a separate transaction that investigators determined to include funds that originate from both M.P. and other victims.

57. Victims L.M., P.C., A.P., L.C.L., and J.Y. were all initially contacted through LinkedIn. The scammers communicated with the victims, developing trust either by offering business opportunities or by creating romantic connections. The scammers requested the conversations continue through WhatsApp where they persuaded the victims to invest in virtual currency and provided links to fake trading platforms.

58. L.M. invested approximately 1.3 million dollars, draining her IRA account. When L.M. attempted to withdraw her funds, the withdrawal was blocked. L.M. has since passed away from cancer and her husband has reportedly sold many assets to cover the IRA withdrawal penalties.

59. P.C. works in the technology industry and believed the trading platform looked like a legitimate website. P.C. invested approximately $250,000, which she was planning on using for her son's education.

60. A.P. developed an emotional relationship with the scammer and invested approximately $300,000. The "trading platform" A.P. used was a spoof of a legitimate company in Turkey. When A.P. attempted to withdraw the funds, she was charged fake taxes, fines, and fees. When A.P. contacted the legitimate company and the Turkish government, she was informed that the website was fraudulent.

61. Similarly to M.P., L.C.L. developed a romantic relationship with a man she knew as Kevin Zhang ("Zhang"). Zhang convinced L.C.L. they would be investing to support their future together. L.C.L. drained her 401(k) and invested approximately $1.1 million. When L.C.L. attempted to withdraw her funds, she was charged 30% in fake taxes and fees. Zhang asked her to take out loans to cover the fees and allegedly assisted her in covering some of the costs of the fees. Zhang then convinced L.C.L. to allow him to use her account to move additional funds from other individuals. Eventually Zhang disappeared and L.C.L. was left with no retirement and the taxes consequences for the early withdrawal of her 401(k).

62. J.Y. conversed with the scammer for some time, building trust with her. The scammer alleged working for financial institutions in Los Angeles. After approximately a month, the scammer introduced virtual currency investing and said they could walk J.Y. through the steps. J.Y. acquired virtual currency and saw her investment grow on the trading platform. When J.Y. attempted to withdraw her funds, her account was frozen, and she was charged $50,000 to unfreeze it. After paying, she was charged $100,000 in "taxes." After completing this payment, she was charged another $50,000, which J.Y. did not pay and instead contacted the FBI. J.Y. took out loans and pulled from her investments with a total reported loss of $250,000.

63. Victims T.S., J.H., and S.M were all contacted through misdirected text messages. The three victims responded, and the scammers created trust with the victims and then convinced them to invest in virtual currency. After investing, victims saw their profits grow and they invested larger and larger sums.

64. T.S. was reportedly offered short and long-term trades which allegedly yielded high profits. T.S. recommended the investment to her family and friends who also participated. T.S. reportedly invested approximately $400,000 and conducted transactions for her sister through her

cryptocurrency accounts. T.S.'s sister invested over one million dollars. When T.S. attempted to withdraw her funds, she was charged a 10% "fee," which she did not pay. T.S. was unable to recover any of her money and was reportedly charged fines for withdrawing funds from her 401(k) early.

65. Scammers reportedly offered J.H. short- and long-term trades which were supposed to yield 15% to 90% profits. J.H. was convinced to invest in virtual currency because her job at the time was not very stable and her parents were in bad health. J.H. later lost her job and invested her severance pay in the trading platform. J.H. also reportedly sold stocks to invest additional funds. When J.H. attempted to withdraw her funds, she was charged a $300,000 "fee," which she reportedly paid by withdrawing money from her IRA account. Eventually the scammer disappeared and J.H. reportedly lost approximately $1.4 million.

66. S.M. was directed by the scammer to communicate through the messaging app Telegram. The scammer walked her through investing. When S.M. attempted to withdraw her funds, she was charged a "fine" to unlock the funds, a "tax," "VIP membership," and "premium processing." After paying all the requested fees, she was told her account was flagged for money laundering and shut down. S.M. reportedly lost approximately $200,000, described as her life savings.

67. R.C.A. worked in financial services, and M.G. worked in the real estate industry. Both were contacted by individuals who were allegedly interested in their services. During the conversations, the individuals introduced virtual currency investing and encouraged R.C.A. and M.G. to invest.

68. R.C.A.'s email and contact information are public on her website. An individual reached out to R.C.A. seeking information about annuities. The individual suggested R.C.A. invest in virtual currency and provided her links that mimicked a legitimate website. After investing

approximately $115,000, R.C.A. was unable to withdraw her funds and thus contacted the legitimate website and was informed the website was a spoof.

69. M.G. worked as a real estate agent and was contacted by an individual allegedly named Henrick Michael (Michael), who expressed interest in purchasing a home. As they communicated regarding property, Michael introduced virtual currency and encouraged M.G. to invest. Throughout their communications they developed a romantic relationship and M.G. grew to trust Michael. M.G. invested hundreds of thousands of dollars. When she attempted to withdraw the funds, she was charged a 10% "security deposit" in the amount of $173,356. After paying, she was charged a "VIP member cost" for accelerated processing which she could not pay. When she confronted Michael about the scam, she disappeared and M.G. reportedly lost over $400,000.

70. B.T.N. created a friendship online with a man. This man encouraged B.T.N. to invest in virtual currency but B.T.N. was nervous to do so. In order to convince her, the man walked her through creating an account on a trading platform and then transferred $50,000 to B.T.N.'s account. B.T.N. reportedly invested $150,000 and after doing so, the man disappeared.

71. Several IC3 reports filed by victims of virtual currency investment fraud indicate similar scams and frauds as those reported above, including victims R.M., N.H., and I.C.C.

72. R.M. reportedly invested on two fraudulent platforms. Initially she was able to make small withdraws, however, when she attempted to make more significant withdraws, she was charged fake taxes and fees. One of the platforms claimed her account was under FinCEN (Financial Crimes Enforcement Network) and FATF (Financial Action Task Force) review. Eventually, the platforms became non-functional and then disappeared. R.M. reportedly lost approximately $557,225.

73. N.H. was communicating with a woman through WhatsApp. After several months, the woman suggested N.H. invest in virtual currency. The woman provided step by step instructions and sent N.H. a website to a trading platform. N.H. was initially able to make a small withdrawal. After reportedly investing $65,000, her account was frozen and she was charged $16,000 in fake taxes, which she did not pay since she realized it was a scam.

74. I.C.C. transferred funds from her Kraken account to a fraudulent website provided by the scammers. When she attempted to withdraw her funds, she was charged fees, which she did not pay. I.C.C. lost $250,000.

75. The two tables displayed below, Tables 3 and 4, list identified victims' total reported loss amounts and the amount of their funds traced to the Subject Addresses.

Victim	Total Loss Amount
M.P.	730,000
T.S.	400,000
M.G.	400,000
J.H.	1,400,000
A.P.	300,000
R.C.A.	115,000
P.C.	250,000
L.M.	1,300,000
S.M.	200,000
N.H.	65,000
R.M.	557,225
B.T.N.	150,000
I.C.C.	250,000
J.Y.	250,000
L.C.L.	1,100,000

Table 3 (see above) Summary of Total Reported Victim Loss Amounts

Subject Address	Associated Victims	Amount of Victim Funds Traced To Subject Address
1	M.P., J.H., M.G.	219,790
2	M.P., P.C., A.P.	199,997
3	M.P., T.S., L.M., S.M., N.H., R.M., B.T.N., I.C.C., J.Y., L.C.L.	651,934
4	M.P., T.S., L.M., S.M., N.H., R.M., B.T.N., I.C.C., J.Y., L.C.L.	712,028
5	M.P., T.S., N.H., R.M., B.T.N., I.C.C., J.Y., L.C.L.	483,649
6	M.P., M.G., L.M.	60,235
7	M.P., M.G., L.M.	60,235
8	M.P., M.G., L.M.	60,235
9	M.P., M.G., J.H., L.M.	202,739
10	M.P., A.P., R.C.A.	157,722

Table 4 (see above) Summary of Victim Funds Traced to Subject Addresses[8]

ADDITIONAL ANALYSIS OF SUBJECT ADDRESSES

76. As outlined below, FBI special agents and forensic accountants utilized reliable blockchain analytical tools to review the address activity, patterns, and associations with other known scams. In all Subject Addresses, there was a history of activity that matches common money laundering techniques deployed in CIF frauds.

77. Additionally, the companies that provide blockchain analytical tools previously found to be reliable by law enforcement have in-house investigative teams that conduct their own research on suspicious blockchain activity and flag relevant information for the benefit of law enforcement. These blockchain analytical companies utilize open-source information, their own community

[8] The traced victim funds include funds that were frozen in the Subject Addresses' balances, as well as funds that the Subject Addresses sent before the freezes occurred.

complaint reporting platforms, and submissions generated in-tool by other law enforcement, to build an intelligence base to support their efforts. In the case of all Subject Addresses, there was a substantial amount of deposited virtual currency that came directly from, or indirectly through, other addresses that the tool flagged as having suspicious transaction activity or being part of a scam.

Subject Address 1:

78. Subject Address 1 received large deposits of USDT, which is one of the most common cryptocurrencies that law enforcement observes being used when investigating CIF schemes. Using a reliable blockchain analytical tool, investigators determined that a majority of the funds received by this address indirectly came from a decentralized exchange via intermediary transfers from other unhosted wallet addresses. As noted previously, use of decentralized exchanges is another common technique to launder CIF proceeds, often to swap one virtual currency for another, often without needing to provide any identifying information about the actual user.

79. Analysis of the funds sent from Subject Address 1 indicates that a majority of these funds were sent through unhosted wallet addresses to decentralized exchanges or centralized exchanges, such as Binance or OKX.

80. Additionally, investigators reviewed information from a reliable blockchain analytical tool that indicated that Subject Address 1 was associated with a scam listed as "iceleo.com Pig Butchering Grouping." This blockchain analytical tool also flagged two addresses as scams that a significant amount of victim funds had passed through before being deposited into Subject Address 1. These scams were identified as "coinstoreup.com" and "gatevlink.com." The FBI has received

IC3 complaints regarding iceleo.com and gatevlink.com indicating that both are CIF scam websites.[9]

Subject Address 2:

81. Subject Address 2 received large deposits of ETH and USDT, both of which are commonly used in CIF schemes. Investigators determined that a majority of the funds received by this address indirectly came from centralized exchanges, such as Binance, via intermediary transfers from other unhosted wallet addresses. By using "pass through accounts" at centralized exchanges, launderers are able to exit the public blockchain, often conduct transactions that are not publicly viewable on blockchains, and then send funds back onto public blockchains to continue their laundering efforts. Sending funds to a centralized exchange as part of laundering transactions forces investigators to serve legal process on exchanges to counter this obfuscation technique, and then analyze the returns before continuing to follow the flow of funds.

82. Analysis of the funds sent from Subject Address 2 indicates that a majority of these funds were sent to a decentralized exchange to once again swap one type of virtual currency for another.

83. A reliable blockchain analytical tool flagged four addresses that investigators traced victim funds through before the funds ultimately reached Subject Address 2. The tool flagged these addresses associated with scams, such as "iceleo.com Pig Butchering Grouping," "coinstoreup.com," and an unnamed high yield investment scheme.

[9] Scams such as iceleo.com, coinstoreup.com, gatevlink.com, and others, are mentioned multiple times as associated with the Subject Addresses. Multiple addresses have been flagged as being part of these scams. In some cases, multiple Subject Address received funds that passed through one address flagged as part of one of these scam. The Subject Addresses sometimes received funds that were transferred through multiple different addresses that were flagged as part of the same scam.

Subject Address 3:

84. Subject Address 3 received deposits of USDT. Investigators determined that a majority of the funds received by this address indirectly came from a decentralized exchange via intermediary transfers from other unhosted wallet addresses or came from the virtual currency exchange, OKX. Analysis of the funds sent from Subject Address 3 indicates that a majority of these funds were sent to other unhosted wallet addresses, or were sent to centralized exchanges, such as Binance or OKX. Subject Address 4 received the majority of the funds sent by Subject Address 3.

85. Investigators traced funds through three addresses that a reliable blockchain analytical tool flagged as scams, such as "coinstoreup.com," "gatevlink.com," and an unnamed high yield investment scheme, before being sent to Subject Address 3.

Subject Address 4:

86. Subject Address 4 received large deposits of USDT. Investigators determined that most of the funds received by this address indirectly came from a decentralized exchange or centralized exchanges, such as Crypto.com, Kraken.com, and Coinbase.com. Subject Address 4 sent funds to two other unhosted wallet addresses, and the majority of the funds sent from these two addresses were ultimately sent to Subject Address 5 or to Binance.

87. A reliable blockchain analytical tool flagged three addresses associated with the scams "coinstoreup.com," "gatevlink.com," "asx-avenue.com," [10] and an unnamed high yield investment scheme. Investigators traced victim funds through these addresses, which were ultimately sent to Subject Address 4.

[10] The FBI has received one IC3 report regarding asx-avenue.com.

Subject Address 5:

88. Subject Address 5 received large deposits of USDT. Most of the funds received by Subject Address 5 were first deposited from centralized exchanges including OKX, Bybit, Binance, and Coinbase, into three unhosted wallet addresses. Then, these addresses sent Subject Address 5 all its funds. The USDT received by Subject Address 5.

89. A reliable blockchain analytical tool flagged six addresses as being associated with scams[11] that investigators traced victim funds through before being sent to Subject Address 5.

Subject Address 6:

90. Subject Address 6 received large deposits of USDT. Investigators determined that a majority of the funds received by Subject Address 6 came directly or indirectly from a decentralized exchange. Most of the funds sent from Subject Address 6 were sent directly to a decentralized exchange or to other unhosted wallet addresses, and then eventually sent to either decentralized or centralized exchanges, such as Binance or OKX.

91. A reliable blockchain analytical tool flagged six addresses as being associated with scams[12] that investigators traced victim funds through, and then ultimately into Subject Address 6**.**

Subject Address 7:

92. Subject Address 7 received deposits of USDT. Investigators determined that the funds received by Subject Address 7 came from one unhosted wallet address, which received funds tracing back to a decentralized exchange. Approximately half of the funds received by Subject Address 7 were not spent prior to the Subject Address 7 being frozen. Also, funds sent by Subject Address 7

[11] These scams include "coinstoreup.com," "gatevlink.com," "asx-avenue.com," an unnamed high yield investment scheme, and one address tied to a Chainabuse community complaint.
[12] These scams include as "iceleo.com Pig Butchering Grouping," "coinstoreup.com," and an unnamed high yield investment scheme.

were later transfered to an address that blockchain analytical tools flagged as belonging to Huione Pay, which is part of the Huione Group. FinCEN has issued a final rule to prohibit covered U.S. financial institutions from opening or maintaining a correspondent account for, or on behalf of Huione Group, which FinCEN found to be of primary money laundering concern pursuant to section 311 of the USA PATRIOT Act, noting its involvement in laundering CIF proceeds, among other illicit proceeds.[13]

93. A reliable blockchain analytical tool flagged six addresses as being associated with scams that investigators traced victim funds through and ultimately into Subject Address 7.[14]

Subject Address 8:

94. Subject Address 8 received deposits of USDT from one unhosted wallet whose funds were traced back to a decentralized exchange. Subject Address 8 sent most of its funds to another unhosted wallet address, which eventually were sent to Binance.

95. A reliable blockchain analytical tool flagged six addresses as being associated with scams that investigators traced victim funds through and ultimately into Subject Address 8.[15]

Subject Address 9:

96. Subject Address 9 received large deposits of USDT. Investigators determined that the funds received by Subject Address 9 indirectly came from a decentralized exchange via intermediary

[13] Imposition of Special Measure Regarding Huione Group, as a Foreign Financial Institution of Primary Money Laundering Concern, 90 Fed. Reg. 48295, 48302 (Oct. 16, 2025) ("Huione Group also has significant exposure to, and has facilitated transactions associated with suspected fraud activity, including [convertible virtual currency] investment scams, also referred to as 'pig-butchering.').

[14] These scams include "iceleo.com Pig Butchering Grouping," "coinstoreup.com," and an unnamed high yield investment scheme.

[15] These scams include "iceleo.com Pig Butchering Grouping," "coinstoreup.com," and an unnamed high yield investment scheme.

transfers from other unhosted wallet addresses. Most of the funds sent by Subject Address 9 were ultimately traced into Binance.

97. A reliable blockchain analytical tool flagged ten addresses as being associated with scams that investigators traced victim funds through and ultimately into Subject Address 9.[16]

Subject Address 10:

98. Subject Address 10 received large deposits of USDT. Investigators determined that the majority of the funds received by Subject Address 10 indirectly came from a decentralized exchange via intermediary transfers from other unhosted wallet addresses. Most of the funds sent by Subject Address 10 were transferred either directly or indirectly through intermediary unhosted wallet addresses to centralized exchanges. Funds from Subject Address 10 were sent directly and indirectly (indirectly via transfers through intermediary unhosted wallet addresses), to Huione Pay.

99. A reliable blockchain analytical tool flagged seven addresses associated with scams that investigators traced victim funds through and ultimately into Subject Address 10.[17]

DEFENDANT PROPERTY IS FORFEITABLE BECAUSE IT FACILITATED AND WAS INVOLVED IN CONCEALMENT MONEY LAUNDERING

100. The Defendant Property was used to commit and facilitate—and were therefore involved in—concealment money laundering. Based on its investigation, the FBI traced approximately $2,808,564 worth of victim proceeds from at least 15 victims into the Subject Addresses. USDT worth approximately $1,666,241.55 was directly traced from identified CIF victims into the balances of the Subject Addresses at the time the balances were seized.

[16] *Id.*
[17] These scams include "iceleo.com Pig Butchering Grouping," and an unnamed high yield investment scheme.

101. As described above, the transaction activity between the victims' deposits to scammer-controlled addresses to the Subject Addresses exemplify patterns that investigators know to be common money laundering techniques, especially in CIF schemes like those afflicting the aforementioned victims. These techniques include the following, which were employed by scammers to conceal or disguise the nature, location, source, ownership, or control of the proceeds of CIF schemes.

102. Scammers directed victims to open accounts at centralized virtual currency exchanges to convert their fiat currency into virtual currency, in part because it is the most user-friendly way to onboard new users to purchase and send virtual currency. Sometimes, like in M.P.'s case, the scammers will even direct victims to set up their own unhosted wallet address(es) to send their exchange account(s)' funds to before sending it to the scammers, in part so victim proceeds can move away from exchanges, who may freeze or seize the funds per law enforcement requests and warrants.

103. Scammers set up new or minimally used "0 Level" addresses and directed victims to deposit their funds to those addresses. If or when victims report these addresses to law enforcement after they realize they have been scammed, they are typically only reporting one deposit address (or sometimes a small number of addresses) that may be compromised, where the funds have likely already been moved by the scammers before first analyzed by law enforcement. This scenario is present here—law enforcement was not able to request that victim-linked USDT be frozen until the aforementioned victim funds were traced to the Subject Addresses. The use of these 0 Level addresses as unique and/or ephemerally used unhosted wallet addresses is part of scammers' initial staging to conceal the nature, location, source, ownership, and control of victims' proceeds.

104. After receiving possession of victims' funds, scammers will send the funds through numerous unhosted wallet addresses, often at a quick pace, with multiple transactions often occurring

within the same day. These types of transfers are exhibited in Figures 3-6, showing law enforcement's tracing of victims' funds to the Subject Addresses. These repeated transactions through multiple unhosted wallets, which incur transaction fees, serve no apparent legitimate business or financial purpose, but instead facilitate money laundering by helping conceal or disguise the nature, location, source, ownership, or control of CIF proceeds.

105. Before victims' funds entered the Subject Addresses, they were also converted to stablecoins, mainly USDT, if victims' initial deposits were in another form of cryptocurrency. As described earlier, according to investigators, money launderers are particularly drawn to USDT because of its low transactions fees and stability compared to other more volatile cryptocurrencies. Additionally, USDT is compatible on several different blockchains, which makes it easier to move funds across blockchains to further obfuscate the nature, source, control, and/or ownership of criminal proceeds.

106. According to investigators, CIF money launderers regularly use decentralize exchanges for swapping victim proceeds from one type of cryptocurrency to another (*e.g.*, stablecoins) to facilitate additional laundering transactions on the blockchain, and in preparation for converting funds to fiat currency off the blockchain. As discussed earlier, funds entering and/or exiting Subject Addresses 1, 2, 3, 4, 6, 7, 8, 9, and 10 passed through decentralized exchanges, which often collect little to no KYC information to help users remain anonymous.

107. Even before victim funds were sent into the Subject Addresses, they were often commingled with other victims' funds in "consolidation wallets," which, according to investigators, is common tradecraft used by CIF launders. Instead of exclusively passing victim funds through a linear list of addresses, CIF scammers, including those involved in the scams discussed in this complaint, merge victim funds in consolidation wallets to disguise the nature, location, source,

ownership, and control of proceeds, requiring oftentimes resource and expertise-intensive tracing and investigative efforts to trace funds sent from consolidation wallets back to victim deposits. [18]

108. Based on the FBI's tracing and analysis of victim funds, and the analysis of other deposits of currently unknown origins into the Subject Addresses, the users of the Subject Addresses commingled known victim funds with other funds for the purpose of facilitating the concealment of the nature, location, source, ownership, and control of wire fraud proceeds.

109. When the government shows that the suspected money launderer(s) commingled proceeds of specified unlawful activity with funds of unknown origins in an account or wallet via transactions apparently designed to conceal the nature, source, ownership, location, or control of criminal proceeds, then those commingled unattributed funds are forfeitable as having facilitated—and therefore as having been "involved in"—money laundering. *See, e.g.*, *United States v. Bikundi*, 926 F.3d 761, 793-94 (D. C. Cir. 2019) (collecting cases); *see also United States v. Guerrero*, 2021 WL 2550154, *9 (N.D. Ill. June 22, 2021) (money from unknown source that was commingled with fraud proceeds facilitated the concealment laundering of the fraud proceeds and, accordingly, property acquired with the commingled funds was forfeitable as property traceable to property involved in a money laundering offense); *United States v. Romano*, 2021 WL 1711633, *5-6 (E.D.N.Y. Apr. 29, 2021) (by laundering fraud proceeds through their personal bank accounts, to commingle the proceeds with other funds for a concealment laundering purpose, the defendants made the commingled funds forfeitable as facilitating property); *United States v. Coffman*, 859 F.

[18] *See e.g.*, 0x53558f (featuring outgoing funds that ultimately were sent to Subject Address 1 and Subject Address 2) and 0x89b1d4 (featuring outgoing funds that ultimately were sent to Subject Address 10) in Figure 4; 0x53558f and 0x2a034 comingling funds from multiple identified CIF victims before their sent funds were further consolidated with victim funds in Subject Addresses 3, 4, and 5 in Figure 5; 0x46bc81 (receiving funds traced back to multiple victims that were then dispersed to Subject Addresses 6, 7, 8, and 9) in Figure 6.

Supp. 2d 871, 876-77 (E.D. Ky. 2012) (holding that forfeiture of legitimate and criminal proceeds commingled in an account is proper as long as the government demonstrates that the defendant pooled the funds to facilitate money laundering by, for example, disguising the nature and source of proceeds; concluding that clean funds in bank account were subject to forfeiture because they had "been co[m]mingled with tainted funds for the purpose of obfuscating the origin or existence of the tainted money").

110. According to investigators, tracing more than one victim's funds to the same addresses from multiple frauds committed within a short time period suggests that the addresses and the funds contained in that address are being used to collect, conceal, and launder those funds. In this case, all the Subject Addresses received funds from at least three or more known CIF victims, as outlined in Table 4 above. Everyone that the FBI was able to speak with who was identified as a potential victim from back tracing funds from the Subject Addresses provided stories that described, CIF schemes. Based on the transaction history for the funds sent to and from the Subject Addresses**,** including funds traced back to CIF victims, there are likely numerous additional victims that the FBI has not yet identified whose funds were deposited into, and remain associated with the Subject Addresses**.**

111. Additionally, SUBJECT ADDRESSES 1, 2, 3, 4, 5, 6, 7, and 10 all either received or sent funds to addresses that a reliable blockchain analytics tool associated with at least one type of scam, or with a company publicly associated with providing money laundering services for scams.

CLAIMANTS OF SUBJECT ADDRESSES

112. The Subject Addresses are all unhosted wallet addresses where the owners cannot be easily identified. After freezing the USDT within these addresses, the company Tether Ltd. often receives messages from individuals claiming ownership of the frozen addresses. Tether Ltd.'s

company practice is to notify the law enforcement entity who initiated the freeze and to refer the claimant to a contact provided by that entity. Following the freeze of the ten Subject Addresses, Tether Ltd. was contacted by claimants for several Subject Addresses and referred those individuals to the FBI.

113. As described below, multiple individuals contacted Tether Ltd., were then directed to the FBI, and emailed the FBI. However, many individuals chose not to follow up with the FBI. Investigators offered claimants the opportunity to self-identify and explain their use of the Subject Addresses in question. However, no claimant responded to those questions.

114. On or about May 21, 2025, an attorney emailed the FBI and attached an April 25, 2025 judgment issued in the Sixteenth Judicial Circuit of Missouri in *Hu "George" Zongqi v. Coincolaprosib.com and Dana "Noami" Li*, Case No. 2416-CV34056. The judgment finds that the defendants in that case control the cryptocurrency held in four cryptocurrency addresses, including Subject Addresses 1, 9, and 10, that the defendants moved the plaintiff's property to these addresses, and orders Tether Holdings Limited to "[r]elease any restrictions placed on said cryptocurrency, and transfer said cryptocurrency into the possession of [plaintiff's counsel's wallet]" or to "[r]replenish said cryptocurrency by destroying [sic] reminting new Tether cryptocurrency in an equivalent amount with the new public and private keys being transferred into the possessions of [plaintiff's counsel's wallet] for dispersal." The plaintiff filed a Petition for Damages on or about November 26, 2024, and alleged that he was the victim of a pig butchering scam, and that the defendants were responsible for the scam. Plaintiff purportedly "served" the defendants, the pig butchering company and "Dana Li" through three WhatsApp phone numbers and an address in Los Angeles. Defendants did not respond to any of the court filings, interrogatories, or motions. The Court eventually entered a default judgement against the defendants.

115. Plaintiff's counsel reached out seeking to work with the FBI in light of the Court's order. On or about May 20, 2025, an amended judgment appears to have been entered in the case, which also orders Tether Holdings Limited, a foreign corporation, to effect the transfer of the funds, or funds of an equivalent value in multiple cryptocurrency addresses, including SUBJECT Addresses 1, 9, and 10, to the plaintiff's attorney.

Subject Address 1:

116. On or about February 25, 2024, Tether Ltd alerted investigators that an individual had contacted them claiming ownership of Subject Address 1. Tether Ltd added that the person contacted them from the email address 773819747@qq.com with the name and alias "Titi."[19] Tether directed this individual to contact the FBI. On or about February 26, 2024, investigators received an email from the same email address under the name "as," who requested how to have their address unfrozen. This email included Chinese-language characters in the signature line. Investigators responded the next day with a list of questions for "as" to self-identify and explain the use of the address. The investigators never received a response.

Subject Address 2:

117. On or about February 21, 2024, Tether alerted investigators that an individual had contacted them claiming ownership of Subject Address 2. Tether Ltd added that the person messaged them from the email address Kakaxrun@gmail.com with the name and alias "Kaka." Tether directed this individual to contact the FBI. On or about February 27, 2024, investigators received an email from BrentLawFirm@outlook.com with the name Brent Darson. This sender claimed to be representing their unnamed client to pursue the release of their virtual currency address. The email did not include any information lending credibility to the sender being an attorney. Investigators

[19] QQ Mail, providing email addresses ending in @qq.com, is a provider in China.

were also unable to find information online about the alleged attorney. Nevertheless, investigators responded with a list of questions for the sender to identify their client and explain the use of the address. The investigators never received a response.

Subject Address 3:

118. The FBI did not receive any messages regarding claimants of Subject Address 3 from Tether Ltd or anyone else.

Subject Address 4:

119. On or about June 13, 2024, Tether alerted investigators that an individual had contacted them claiming ownership of Subject Address 4. Tether Ltd added that the person messaged them from mgm150123@gmail.com with the name and alias "HHK." Tether Ltd directed this individual to contact the FBI. Later that day, investigators received a message from the same email address under the name "gm m" inquiring about the frozen address. Investigators responded with a list of questions for the sender to self-identify and explain the use of the address. The investigators never received a response.

120. On or about October 15, 2024, Tether Ltd alerted investigators that another individual contacted them to claim ownership of Subject Address 4. Tether Ltd added that the person messaged them from fratelemac@gmail.com with the name and alias "Fratele Mac." The claimant introduced themselves as "LiZeran" and provided a Chinese ID card with the name Li Zeran, date of birth January 16, 1992, and an address in China. Tether Ltd directed this individual to contact the FBI. Investigators did not receive a message from this claimant but proactively sent this claimant a list of questions to further self-identify and explain the use of this account. Investigators did not receive a response.

121. On or about November 27, 2024, Tether Ltd alerted investigators that another individual contacted them to claim ownership of Subject Address 4. Tether Ltd added that the person messaged them from 82d740@proton.me with the name and alias "82d740." Tether Ltd directed this individual to contact the FBI. Investigators did not receive a message from this claimant.

122. On or about January 15, 2025, investigators received a message from the email address from an attorney who noted that they were messaging on behalf of their client Mr. Dejiang Zeng regarding Subject Address 4. On or about February 21, 2025, an Department of Justice attorney asked the attorney claiming to represent Mr. Zeng a series a questions about his client and Subject Address 4, but no response was received from Zeng's attorney.

Subject Addresses 5, 6, 7, and 8:

123. The FBI did not receive any messages regarding claimants of Subject Address 5, 6, 7, and 8 from Tether Ltd or anyone else.

Subject Address 9:

124. On or about March 16, 2024, investigators received a message from the email address a9161796@gmail.com under the name written in Chinese characters for "boy holding sword," who was claiming ownership of Subject Address 9. Investigators responded with a list of questions for the claimant to self-identify and explain the use of the address. The investigators never received a response.

125. On or about March 16, 2024, investigators received a message from the email address rhaber779@gmail.com under the name Rolando Haber. Investigators responded with a list of questions for the claimant to self-identify and explain the use of the address. The investigators never received a response to their questions but received two additional messages written in Chinese-characters requesting that the address be unfrozen.

126. On or about August 26, 2024, Tether Ltd alerted investigators that an individual contacted them to claim ownership of Subject Address 9. Tether Ltd added that the person messaged them from desktopv77@gmail.com with the name and alias "yuu." Tether Ltd directed this individual to contact the FBI. Investigators did not receive a message from this claimant.

127. On or about August 26, 2024, investigators received a message from the email address mgm150125@gmail.com under the name "125 mgm." This email address was very similar to another from a claimant in Subject Address 4. Investigators responded with a list of questions for the claimant to self-identify and explain the use of the address. The investigators never received a response.

128. On or about October 14, 2024, Tether Ltd alerted investigators that an individual contacted them to claim ownership of Subject Address 9. Tether Ltd added that the person messaged from ChinnyDalki@gmail.com with the name and alias "yth." Tether directed this individual to contact the FBI. Investigators did not receive a message from this claimant.

129. On or about November 11, 2024, investigators received a message from the email address wombleshasch@gmail.com under the name "Wombles Hasch." The message was written in Chinese-language characters. Investigators responded with a list of questions for the claimant to self-identify and explain the use of the address. The investigators never received a response.

130. On or about November 18, 2024, Tether Ltd alerted investigators that an individual contacted them to claim ownership of Subject Address 9. Tether Ltd added that the person messaged from Naso95@163.com with the name and alias "Naso Liu." Additionally, Tether Ltd noted that this user has an unverified account on their platform under the name Naso Yao Liu with an IP address geolocating to Hong Kong. Tether directed this individual to contact the FBI. Investigators did not receive a message from this claimant.

131. On or about December 25, 2024, Tether alerted investigators that an individual contacted them to claim ownership of Subject Address 9. Tether added that the person messaged from kakb123456789@163.com with the name and alias "kbb." Tether directed this individual to contact the FBI. Investigators did not receive a message from this claimant.

Subject Address 10:

132. The FBI did not receive any messages regarding claimants of Subject Address 10 from Tether Ltd or anyone else.

COUNT ONE – FORFEITURE OF DEFENDANT PROPERTY

(18 U.S.C. § 981(a)(1)(C))

133. 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.

134. 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))

135. The Defendant Property constitutes property involved (a) domestic and international concealment of money laundering transactions committed in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i) and 1956(a)(2)(B)(i), (b) a conspiracy to engage in money laundering, committed in violation of Title 18, United States Code, Section 1956(h).

136. 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, Charles Linnerooth, 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 13 th day of November 2025.

Charles Linnerooth

Charles Linnerooth
Special Agent
Federal Bureau of Investigation