ISMAIL J. RAMSEY (CABN 189820)
United States Attorney

THOMAS A. COLTHURST (CABN 99493)
Chief, Criminal Division

CHRIS KALTSAS (NYBN 5460902)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-6915
FAX: (415) 436-7234
chris.kaltsas2@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. APPROXIMATELY 1,360,000.748 TETHER AND $3,859,703.65 IN U.S. CURRENCY, Defendants.	**CASE NO.** **VERIFIED COMPLAINT FOR CIVIL FORFEITURE *IN REM***

The United States of America, by its attorneys, Ismail J. Ramsey, United States Attorney, and Chris Kaltsas, Assistant United States Attorney for the Northern District of California, brings this complaint and alleges as follows:

NATURE OF THE ACTION

1. This is a judicial forfeiture action *in rem*, authorized by Title 18, United States Code, Sections 981 and 983.

2. This Court has jurisdiction under Title 18, United States Code, Section 981; and Title 28, United States Code, Sections 1345 and 1355, as the defendant property constitutes or is derived from proceeds obtained, directly or indirectly, from violations of Title 18, United States Code, Sections 1343

and 1956, as well as property involved in violations of Title 18, United States Code, Section 1956.

3. This action is timely filed in accordance with Title 18, United States Code, Section 983.

4. Venue is proper because the defendant property represents the proceeds of a crime that may be prosecuted in the Northern District of California. 28 U.S.C. §§ 1355, 1395.

5. Intra-district venue is proper in the San Francisco division within the Northern District of California.

PARTIES

6. Plaintiff is the United States of America

7. The Defendant Property includes approximately 1,360,000.748 Tether ("USDT") and $3,859,703.65 formerly held in a Kraken cryptocurrency account identified by a USDT deposit address ending in af9e ("the Subject Account").[1]

BACKGROUND ON CRYPTOCURRENCY EXCHANGES AND VIRTUAL CURRENCIES

8. Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies such as the U.S. dollar, but are generated and controlled through computer software. Bitcoin is currently the most well-known virtual currency in use.

9. 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 alphanumeric characters. Users can operate multiple addresses at any given time, with the possibility of a unique address being used for every transaction.

10. Each virtual currency address is controlled through the use of a corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address' private key can authorize a transfer of virtual currency from that address to another address.

11. A virtual currency wallet is a software application that interfaces with a virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency

[1] The full wallet address has been anonymized to protect potential claimants' privacy and identities.

wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

12. Many virtual currencies publicly record all of their transactions on what is known as a "blockchain." The blockchain is essentially a distributed public ledger, run by a decentralized network, 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 ever received that virtual currency. It also 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.

13. Although the identity of an address holder is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular address. This analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity.

14. Tether, widely known as "USDT," is a blockchain-based cryptocurrency whose tokens in circulation are backed by an equivalent amount of U.S. dollars, making it what is known as a "stablecoin." A stablecoin is a virtual currency whose value is tied to that of another "stable" currency, commodity, or financial instrument. USDT is issued by Tether Ltd., a company headquartered in Hong Kong. Tether is connected to Bitfinex, a cryptocurrency exchange located in the British Virgin Islands.

15. DAI is also a blockchain-based stablecoin. DAI is issued by MakerDAO, a foundation headquartered in Denmark. DAI relies on "smart contracts" to maintain a value equal to the U.S. dollar.

16. Smart contracts allow developers to create markets, store registries of debts, and move funds in accordance with the instructions provided in the contract's code, without any middleman or counterparty controlling a desired or politically motivated outcome, all while using the Ethereum blockchain to maintain transparency. Multiple cryptocurrencies, including DAI, can utilize the Ethereum blockchain to take advantage of this technology. Smart contract technology is one of Ethereum's distinguishing characteristics and an important tool for companies or individuals executing trades on the Ethereum blockchain. When engaged, smart contracts automatically execute according to the terms of the contract written into lines of code. A transaction contemplated by a smart contract occurs on the

Ethereum blockchain and is both trackable and irreversible.

17. U.S.D. Coin ("USDC") is a blockchain-based stablecoin tied to the U.S. dollar. USDC is issued by Centre, a company headquartered in the U.S. USDC is connected to Coinbase and Circle, cryptocurrency exchanges registered in the U.S.

18. USDT, DAI, and USDC are hosted on the Ethereum blockchain, among others. Ether ("ETH") is a cryptocurrency that is open source, public, is the native cryptocurrency of the Ethereum blockchain, and is distributed on a platform that uses smart contract technology. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track the movement of ETH.

19. Every transfer from one address to another on the Ethereum blockchain, or conversion of one type of virtual currency to another on that blockchain, costs the user a small amount of money, commonly referred to as a "gas fee." Thus, if a user tried to send $100 in virtual currency from address A to address B, address B would end up with slightly *less* than $100 worth of that currency, due to the gas fee being deducted from the transferred amount. Gas fees are somewhat analogous to other traditional transaction fees, such as credit card fees or wire fees.

FACTS

20. As detailed below, this case concerns the theft and laundering of more than $7 million worth of cryptocurrency through a wire fraud scheme affecting multiple victims and uncovered by tracing the movement of the Defendant Property to the Subject Account.

21. On or about August 8, 2022, Victim 1,[2] a 61-year-old resident of San Francisco, connected with a person identifying themselves as Hao William Yang ("YANG") on a real-estate platform known as Homesnap. YANG claimed to be a cryptocurrency expert and offered Victim 1 a chance to invest in cryptocurrency using an investment platform called NYMEX, promising substantial gains. After investing nearly $3,050,000.00 of their own money and another $2,450,000.00 they obtained from six family members, Victim 1 discovered that NYMEX was a scam as it misrepresented investor returns while pilfering investors' funds.

22. Blockchain analyses and other records indicate that the funds invested in NYMEX were

[2] Victim names have been anonymized to protect their identities.

laundered through over a dozen cryptocurrency addresses with intervening conversions between cryptocurrencies, before reaching the Subject Account. As indicated below, there is no apparent purpose for the transfer of this cryptocurrency through a large number of addresses and its conversion into several different currencies apart from concealing the nature, source, location, ownership, or control of the funds, rendering the Defendant Property subject to forfeiture.

A. Wire Fraud Scheme

23. On or about August 8, 2022, Victim 1 connected with YANG on the Homesnap platform. Homesnap is a real-estate listing platform with a consumer-facing application for buyers. YANG claimed to be looking for real estate in the San Francisco Bay Area.

24. Two days after the initial contact, on or about August 10, 2022, YANG sent Victim 1 a message on LINE, an encrypted messaging service headquartered in Japan. Victim 1 and YANG discussed personal matters on LINE such as their backgrounds, relationship statuses, businesses, and finances. Within a week their relationship became personal, with YANG sending many messages about his "love" for Victim 1.

25. A scammer sending a victim messages about their purported love for them quickly after making contact is a common manipulation tactic in scams known as "love bombing."

26. During their initial LINE conversation, YANG often discussed cryptocurrency futures trading, unprovoked and unrelated to the topic of conversation. YANG claimed that in addition to being a successful automobile parts manufacturer, he had made millions of dollars through cryptocurrency trading. YANG represented himself as a cryptocurrency expert to Victim 1.

27. On or about August 15, 2022, YANG introduced Victim 1 to a company called NYMEX. YANG claimed that NYMEX was a beginner-friendly cryptocurrency exchange based in Chicago. YANG directed Victim 1 to download the NYMEX application through a link that he provided through LINE. Victim 1 pressed the link, and it downloaded the NYMEX application onto their smartphone.

28. Although NYMEX appeared to be a legitimate cryptocurrency platform and application, with graphics and layouts consistent with most extant smartphone currency trading applications, it was, in reality, a fraudulent application. The displayed investment amounts and gains were entirely fictitious, and the perpetrators of the fraud had the ability to adjust the displays as they pleased over the course of

the scam to reflect gains on investments when, in reality, no gains were accruing and the funds were not in the exchange account as represented.

29. On or about August 18, 2022, YANG instructed Victim 1 to purchase USDC from well-known cryptocurrency exchanges BitStamp and Coinbase for the purpose of investing into the NYMEX exchange.

30. On August 27, 2022, Victim 1 made their initial investment into the NYMEX application, with a transfer of 199,990.00 USDC from their Coinbase account to a USDC address ending in 2f20 (the "NYMEX address").

31. Following the initial investment, Victim 1 was able to view their fabricated "earnings" on the NYMEX application, which reported gains of twenty to thirty percent against Victim 1's initial investment in less than a week. Those purported gains were enough to convince Victim 1 to invest an additional $1,099,990.00 in USDC into the NYMEX platform on September 2, 2022.

32. At the request of YANG, Victim 1 asked family members to invest with them. Six family members collectively gave Victim 1 $2,450,000.00 to invest under YANG's guidance, as follows:

a. Victim 1 invested approximately $3,050,000;

b. Relative 1 invested approximately $200,000;

c. Relative 2 invested approximately $200,000;

d. Relative 3 invested approximately $200,000;

e. Relative 4 invested approximately $200,000;

f. Relative 5 invested approximately $600,000; and

g. Relative 6 invested approximately $1,900,000.

33. Sometime in September 2022, Victim 1 received multiple message requests in the same day on Homesnap from men living in Asia to view property in San Francisco. When Victim 1 mentioned this oddity to YANG during one of their conversations on LINE, YANG became angry and accused Victim 1 of "cheating" on him. YANG demanded that Victim 1 delete their LINE messages up to that point to prove Victim 1's dedication to him. Victim 1 did as YANG asked and deleted all previous LINE messages with YANG, including the NYMEX application link.

34. By December 2022, Victim 1's NYMEX account on the fictitious application showed

that their and their family's investments had grown to nearly $10,000,000.

35. On or about December 19, 2022, Victim 1 tried to withdraw the $10 million from their NYMEX account but received a message from NYMEX "customer service" saying that Victim 1 needed to pay $200,000 in taxes in order to withdraw the funds. At YANG's urging, Victim 1 paid the $200,000 in USDC to NYMEX, but was still unable to withdraw the funds. Victim 1 ultimately learned of the fraud when they reported the incident to Coinbase and Bitstamp.

36. Between August 27, 2022 and December 14, 2022, Victim 1, on their own and on behalf of their relatives, conducted 16 investment transactions into the NYMEX exchange totaling approximately 5.5 million USDC from their accounts at Coinbase and Bitstamp. The 16 transfers were all sent to the NYMEX Address, as follows:

Date	Exchange Used	Receiving Address	Amount	Asset
8/27/2022	Coinbase	0x6b8a0968e027e2dead440e48b850ca4d4eb22f20	199,989.26	USDC
8/30/2022	BitStamp	0x6b8a0968e027e2dead440e48b850ca4d4eb22f20	798,850.79	USDC
9/2/2022	Coinbase	0x6b8a0968e027e2dead440e48b850ca4d4eb22f20	1,099,989.32	USDC
9/16/2022	Coinbase	0x6b8a0968e027e2dead440e48b850ca4d4eb22f20	700,771.03	USDC
10/1/2022	Coinbase	0x6b8a0968e027e2dead440e48b850ca4d4eb22f20	499,989.42	USDC
10/12/2022	Coinbase	0x6b8a0968e027e2dead440e48b850ca4d4eb22f20	199,988.16	USDC
10/18/2022	Coinbase	0x6b8a0968e027e2dead440e48b850ca4d4eb22f20	199,987.83	USDC
10/28/2022	Coinbase	0x6b8a0968e027e2dead440e48b850ca4d4eb22f20	199,987.60	USDC
11/7/2022	Coinbase	0x6b8a0968e027e2dead440e48b850ca4d4eb22f20	199,987.44	USDC
11/14/2022	Coinbase	0x6b8a0968e027e2dead440e48b850ca4d4eb22f20	199,987.98	USDC
11/21/2022	Coinbase	0x6b8a0968e027e2dead440e48b850ca4d4eb22f20	200,189.24	USDC
12/2/2022	Coinbase	0x6b8a0968e027e2dead440e48b850ca4d4eb22f20	300,288.58	USDC
12/8/2022	Coinbase	0x6b8a0968e027e2dead440e48b850ca4d4eb22f20	300,288.57	USDC
12/9/2022	Coinbase	0x6b8a0968e027e2dead440e48b850ca4d4eb22f20	100,086.70	USDC
12/14/2022	Coinbase	0x6b8a0968e027e2dead440e48b850ca4d4eb22f20	100,088.01	USDC
12/19/2022	Coinbase	0x6b8a0968e027e2dead440e48b850ca4d4eb22f20	200,188.70	USDC
Total			**5,500,658.63**	

37. The NYMEX scam described here is consistent with an emerging fraud trend known as "Pig Butchering." According to the Global Anti-Scam Organization, pig butchering originated in China in 2019. The scheme often begins with a scammer sending a victim a purportedly misdialed message, but recent cases have included real estate-related connections, such as the one described here. From there, the scammer establishes a more personal relationship with the victim using manipulative tactics similar to those used in online romance scams.

38. The victims in pig butchering schemes are referred to as "pigs" by the scammers, because they are "fattened up" by the manipulative tactics of the scammer. Once the victim is sufficiently trusting, they are invited to participate in a cryptocurrency investment scheme and are provided with fabricated evidence to bolster the credibility of the scammer. The fabricated evidence typically includes a fake investment platform that displays fictitious investment gains. In reality, and in this case, the investment platform has limited functionality and does not provide the user any access to a real cryptocurrency wallet or address.

39. The scammers may also provide fake transaction photos to victims that create the illusion that they are contributing their own funds to the victim's initial investment. However, the investment gains displayed on the platform are fabricated. In reality, the investment platform does not exist. The scammers will then refer to "butchering" or "slaughtering" the victims once their assets are stolen by the criminals, ultimately causing the victims financial and emotional ruin.

40. Criminal organizations engaging in pig butchering scams often operate in multiple tiers of responsibility. The person who communicates with the victim is usually in a lower tier of responsibility within the organization, while the person who receives funds at the end of the scheme are those who profit the most and are typically higher in the organizational hierarchy.

B. Laundering the Fraud Proceeds to the Subject Account

41. For each of Victim 1's transactions, the funds were traced on the publicly available blockchain through a series of transfers between cryptocurrency addresses, known as hops, to their arrival at the Subject Account.

42. Victim 1's funds were swapped for various cryptocurrencies, specifically, DAI, USDC, and USDT. Notably, all three of these cryptocurrencies are stablecoins, and each of their respective values are tied to the U.S. Dollar at a ratio of approximately 1:1. Accordingly, there is no apparent financial or legitimate business benefit to conducting the swaps performed in this instance. Indeed, each of the swaps and transfers resulted in a net *loss* due to fees paid for the swaps and subsequent transfers. Rather, the swaps were conducted with the intention of obfuscating the nature, location, source, ownership, and/or control of the funds.

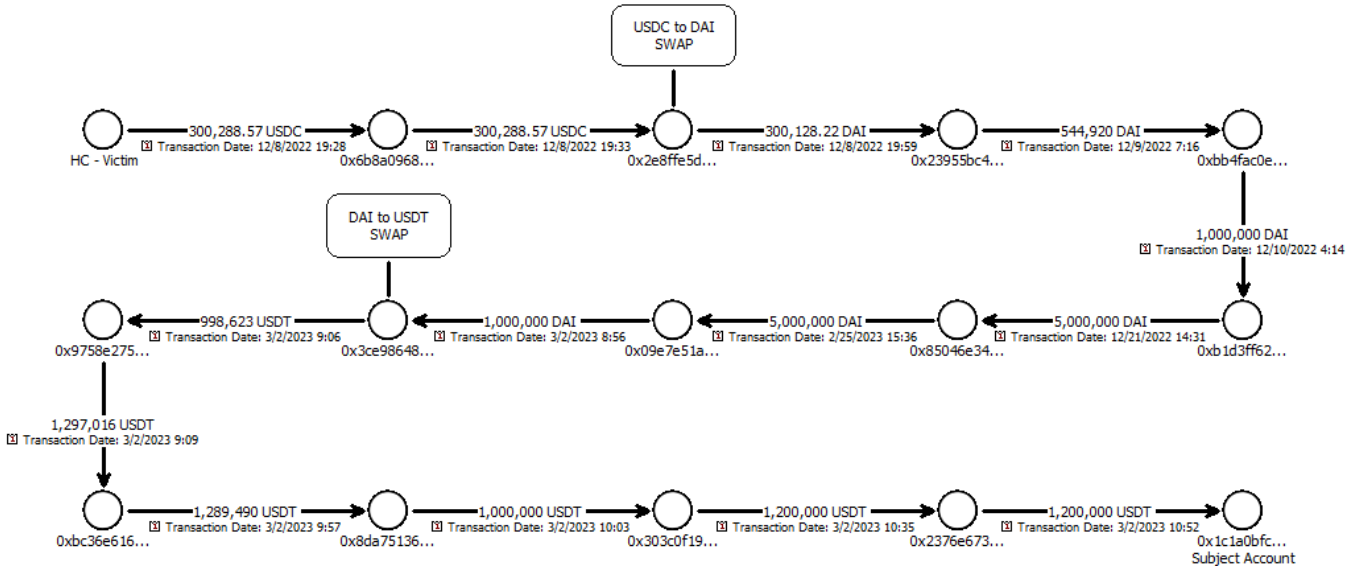
43. During the funds tracing and analysis, law enforcement analyzed the DAI, USDC, and

USDT wallet addresses utilized in the various hops between Victim 1's initial transactions to the NYMEX Address and the funds' ultimate arrival in the Subject Account. That analysis revealed a pattern where the same addresses appeared in other complaints where individuals reported falling victim to pig butchering scams. In these instances, law enforcement located victim complaints on either the Federal Bureau of Investigation's ("FBI's") Internet Crime Complaint Center, known as IC3 (http://www.ic3.gov), or the Federal Trade Commission's ("FTC's") Consumer Sentinel Database (http:/reportfraud.ftc.gov).

44. The cryptocurrency tracing revealed two separate transaction paths, both of which ultimately ended with deposits into the Subject Account. The transactions are detailed separately, below.

C. Subject Account – Transaction Path 1

45. The illustration below demonstrates the movement of funds from Victim 1's account to the Subject Account on one of the two transaction paths, using a transfer to the NYMEX address on December 8, 2022 as an example.



46. As illustrated above, on December 8, 2022, Victim 1 transferred approximately 300,288.57 USDC on the Ethereum blockchain to the NYMEX Address as part of the NYMEX investing scheme. Continuing on December 8, 2022, the NYMEX Address transferred 300,288.57 USDC to a USDC address beginning with 0x2e8ffe5d.

47. Subsequently, on the same day, a cryptocurrency swap was initiated that converted

300,288.57 USDC for 300,128.22 DAI. The reduction in value is primarily due to fees associated with the transaction and swap. The 300,128.22 DAI is fully traceable to Victim 1's initial deposit of USDC into the NYMEX Address. Both USDC and DAI are stablecoins operating on the Ethereum blockchain.

48. Once again on December 8, 2022, the 0x2e8ffe5d address transferred 300,128.22 DAI to a DAI address beginning with 0x23955bc4. On December 9, 2022, the 0x23955bc4 address transferred 544,920 DAI to a DAI address beginning with 0xbb4fac0e. On December 10, 2022, the 0xbb4fac0e address transferred 1,000,000 DAI to a DAI address beginning with 0xb1d3ff62. On December 21, 2022, address 0xb1d3ff62 transferred 5,000,000 DAI to a DAI address beginning with 0x85046e34.

49. Each of the above transfers contained all of the funds traceable to Victim 1's initial deposit of 300,288.57 USDC into the NYMEX address.

50. The aforementioned 5,000,000 DAI stayed dormant in the 0x85046e34 address for over two months. This transactional behavior has been observed frequently in the laundering of funds derived from other pig butchering scams.

51. On February 25, 2023, the 0x85046e34 address became active once more and transferred 5,000,000 DAI to a DAI address beginning with 0x09e7e51a. On March 2, 2023, the 0x09e7e51a address transferred 1,000,000 DAI to a DAI address beginning with 0x3ce98648. This transfer again contained funds traceable to Victim 1's initial deposit into the NYMEX address.

52. Continuing on March 2, 2023, three consecutive cryptocurrency swaps converted 1,000,000 DAI to 998,623.43 USDT. The reduction in value is primarily due to fees associated with the transaction and currency swap from DAI to USDT.

53. On March 2, 2023, address 0x3ce98648 transferred 998,623.43 USDT to a USDT address beginning with 0x9758e275. Continuing on March 2, 2023, address 0x9758e275 transferred 1,297,016 USDT to a USDT address beginning with 0cbc36e616. Address 0xbc36e616 then transferred 1,289,490 USDT to a USDT address beginning with 0x8da75136. These transfers contained funds traceable to Victim 1's initial deposit into the NYMEX Address.

54. Continuing on March 2, 2023, address 0x8da75136 transferred 1,000,000 USDT to a USDT address beginning with 0x303c0f19. On March 2, 2023, address 0x303c0f19 transferred 1,200,000 USDT to a USDT address beginning with 0x2376e673.

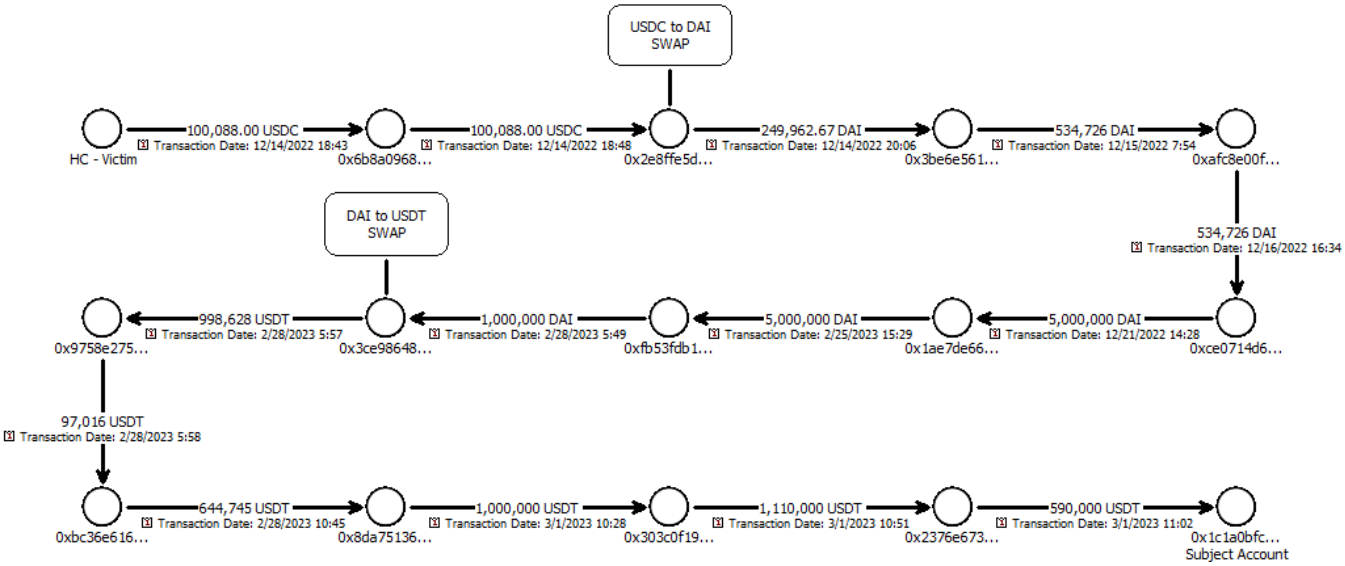
55. Finally, on March 2, 2023, address 0x2376e673 transferred 1,200,000 USDT to a USDT address beginning with 0x1c1a0bfc, which belongs to the Subject Account.

56. Approximately 300,128.22 USDT of the balance in the Subject Account is traceable to Victim 1's original transaction. This number was obtained by tracing the initial investment of 300,288.57 USDC into the NYMEX Address through 14 hops and two swaps that culminated in the transfer to the Subject Account. The amount that ended in the Subject Account is smaller than the amount first transferred to the NYMEX Address, likely due to fees associated with the cryptocurrency swaps that occurred along the transfer path.

57. Criminals engaging in cryptocurrency scams will often conduct an otherwise unnecessary number of transactions in the transfer of funds in an attempt to layer ill-gotten funds and ultimately conceal or disguise the nature, location, source, ownership, or control of the proceeds before they are ultimately transferred into a cryptocurrency exchange. The number of hops in this transfer path indicates that the movement of funds was performed in a manner meant to conceal or disguise the nature, location, source, ownership, or control of the proceeds from the wire fraud described above.

D. <u>Subject Account – Transfer Path 2</u>

58. The illustration below demonstrates the movement of funds from Victim 1's account to the Subject Account on the second of the two transaction paths, using a transfer to the NYMEX address on December 14, 2022 as an example.



59. As illustrated above, on December 14, 2022, Victim 1 transferred approximately 100,088

USDC on the Ethereum blockchain to the NYMEX Address. Continuing on the same day, the NYMEX Address transferred 100,088 USDC to a USDC address beginning with 0x2e8ffe5d.

60. On December 14, 2022, a cryptocurrency swap was conducted that converted 100,088 USDC for 100,040.49 DAI. The reduction in value is primarily due to fees associated with the transaction and swap. The 100,040.49 DAI is fully traceable to Victim 1's initial deposit of USDC into the NYMEX Address.

61. Continuing on December 14, 2022, the 0x2e8ffe5d address transferred 249,962.67 DAI to a DAI address beginning with 0x3be6e561. On December 15, 2022, the 0xbe6e561 address transferred 534,726 DAI to a DAI address beginning with 0xafc8e00f. On December 16, 2022, the 0xafc8e00f address transferred 534,726 DAI to a DAI address beginning with 0xce0714d6. On December 21, 2022, the 0xce0714d6 address transferred 5,000,000 DAI to a DAI address beginning with 0x1ae7de66. Each of these transfers contained funds traceable to Victim 1's initial deposit of 100,088 USDC into the NYMEX Address.

62. Similar to the first transaction path, the funds sat dormant in DAI address 0x1ae7de66 for over two months. This transactional behavior has been frequently observed in the laundering of funds derived from pig butchering scams.

63. On February 25, 2023, DAI address 0x1ae7de66 became active and transferred 5,000,000 DAI to a DAI address beginning with 0xfb53fdb1. On February 28, 2023, address 0xfb53fdb1 transferred 1,000,000 DAI to a DAI address beginning with 0x3ce98648.

64. At this point, the transaction followed Transfer Path 1, beginning with two consecutive cryptocurrency swaps that converted 1,000,000 DAI to 998,628.34 USDT. The reduction in value is primarily due to fees associated with the transaction and swap. Of that 1,000,000 DAI, 100,040.49 DAI, which was converted to USDT, is fully traceable to Victim 1's initial deposit of USDC into the NYMEX Address.

65. On February 28, 2023, the 0x3ce98648 address transferred 998,628 USDT to a USDT address beginning with 0x9758e275. Continuing on the same day, the 0x9758e275 address transferred 97,016 USDT to a USDT address beginning with 0xbe36e616. On the same day, the 0xbc36e616 address transferred 644,745 USDT to a USDT address beginning with 0x8da75136.

66. On March 1, 2023, the 0x8da75136 address transferred 1,000,000 USDT to a USDT address beginning with 0x303c0f19. Continuing on the same day, the 0x303c0f19 address transferred 1,110,000 USDT to a USDT address beginning with 0x2376e673.

67. Finally, on March 1, 2023, the 0x2376e673 address transferred 590,000 USDT to a USDT address beginning with 0x1c1a0bfc, which belongs to the Subject Account.

68. Approximately 97,016 of the USDT transferred to the Subject Account is traceable to Victim 1's initial deposit of 100,088 USDC into the NYMEX Address. The government traced the initial investment of 100,088 USDC into the NYMEX Address through 14 hops and two swaps that culminated in the transfer to the Subject Account. The amount that ended in the Subject Account is smaller than the amount first transferred to the NYMEX Address primarily due to fees associated with the cryptocurrency swaps that occurred along the transfer path.

69. As with Transfer Path 1, the number of hops and swaps that were used to move the funds from the NYMEX Address to the Subject Account, as well as the timing of the transactions, is a strong indication that the transfers were intended to conceal or disguise the nature, location, source, ownership, or control of the proceeds of the wire fraud detailed above.

E. Additional Fraud

70. Victim 1's funds were traced through 14 hops before arriving at the Subject Account. The government analyzed each of the addresses in the movement of funds and repeatedly located reports of additional fraud.

71. The 0x9758e275 address mentioned above had interacted with cryptocurrency addresses where, six hops earlier, 12 victims reported having deposited cryptocurrency into the addresses as victims of scams, including pig butchering.

72. The 0xbc36e616 address mentioned above, into which the 0x9758e275 address transferred funds traceable to wire fraud activity, also interacted with addresses where, five hops prior, three victims reported depositing cryptocurrency into the addresses as victims of a pig butchering scam.

73. The 0x8da75136 address mentioned above, where the 0xbc36e616 transferred the same funds traceable to wire fraud activity, interacted with a series of addresses where, five hops prior, two victims reported depositing cryptocurrency into the addresses as the victims of various scams, including

pig butchering.

74. Lastly, the 0xbb4fac0e address mentioned above interacted with a series of address where, four hops prior, a victim reported depositing cryptocurrency into the address as part of a pig butchering scam.

75. These victims collectively reported losses of approximately $2,118,23.14.

76. Another victim ("Victim 2") reported another pig butchering scam who was similarly induced to "invest" in a fraudulent cryptocurrency exchange.

77. Victim 2 was contacted on LinkedIn by a person identifying themselves as Dot Qian ("QIAN"), who said she was investing cryptocurrency and making large profits on those investments.

78. QIAN offered to assist Victim 2 in conducting similar investments and told them to send Ethereum to a deposit address ending in 2C39fF66.

79. Over the course of 20 days, from December 1, 2022, to December 20, 2022, Victim 2 sent a total of 157.01 Ethereum[3] across six transactions and 40,002.33 USDC to the 2C39fF66 address.

80. Law enforcement traced the path Victim 2's Ethereum took and found that it was converted to DAI, combined with other funds, and then converted to USDT before being deposited into the Subject Account.

81. Law enforcement traced the path Victim 2's USDC took and found that it was converted to DAI, combined with other funds, and then converted to USDT before arriving in the subject account.

82. Based on the tracing, the subject account received the full value of Victim 2's stolen funds, to wit, 157.01 Ethereum and 40,002.33 USDC.

83. Pursuant to a seizure warrant obtained on March 7, 2023, the government sought to seize the assets held in the Subject Account for forfeiture as proceeds of money laundering.

84. The government subsequently learned that between the time the warrant was served and the time it took to freeze the funds, the funds in the account were converted to Australian Dollars ("AUD"). Specifically, the account contained 5,767,900 AUD, along with 200,000.748 of the original

[3] Open-source searches on Etherscan.io, which tracks the historical and current value of cryptocurrencies, show that the value of the deposited Ethereum, taken at the time of each transaction, was approximately $207,546.55. Its value as July 21, 2023 is $297,659.56.

USDT, all of which was traceable to the original funds subject to the seizure warrant. A second seizure warrant was obtained on March 15, 2023. Prior to being transferred from the Subject Account, the AUD contained therein was converted to U.S. Dollars so that they could be processed by the Federal Reserve in a wire transaction. The resulting U.S. Currency is one of the Defendant Properties in this case as those funds constitute the proceeds of the aforementioned wire fraud scheme, as well as the proceeds of the money laundering that followed.

85. On March 21, 2023, the government learned that approximately five hours after the service of the initial warrant, the Subject Account received an additional USDT deposit of 1,160,000 USDT. This deposit was received into the Subject Account via a USDT address ending in 5LuH. The source of these funds was a transfer from a second cryptocurrency exchange account traced three hops prior.

86. This account was owned by a 37-year-old Chinese national. Moreover, an Ethereum USDT address used by this account to receive USDT, to wit, an address beginning with 0x12b0897f.

87. The government analyzed incoming USDT deposits into the 0x12b0897f address and observed a frequent pattern where this account repeatedly interacted with other USDT addresses involved in a variety of pig butchering scams, per reports of fraud to the FBI.

88. Specifically, the government identified eight separate USDT addresses where 29 individuals reported sending their funds as part of a pig butchering scam. These individuals reported their scams to IC3 and reported losing over $2.6 million to fraud. Notably, several of these victims reported the same pig butchering elements, such as USDT addresses and websites, as the victims in the original probable cause statement giving rise to the March 7, 2023 seizure warrant.

COUNT ONE

Civil Forfeiture (Title 18, United States Code, Section 981(a)(1)(C)) for Wire Fraud (Title 18, United States Code, Section 1343)

89. Civil forfeiture of the proceeds of wire fraud is authorized by Title 18, United States Code, Section 981(a)(1)(C). Specifically, Section 981(a)(1)(C) authorizes forfeiture of "any property, real or personal, which constitutes or is derived from proceeds traceable to . . . any offense constituting 'specified unlawful activity' (as defined in section 1956(c)(7) of this title), or a conspiracy to commit

such offense." Section 1956(c)(7)(A) defines the term "specified unlawful activity" as including "any act or activity constituting an offense listed in section 1961(1) of this title." Title 18, United States Code, Section 1961(1), in turn, includes violations of Title 18, United States Code, Section 1343 in its definition of racketeering activity.

90. Because Victim 1's funds are traceable to the Subject Account, the Defendant Property constitutes, and is derived from, the proceeds of wire fraud, in violation of Title 18, United States Code, Section 1343. It is therefore subject to forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C).

COUNT TWO

Civil Forfeiture (Title 18, United States Code, Section 981(a)(1)(A)) for Money Laundering (Title 18, United States Code, Section 1956(a)(1)(B)(i))

91. Civil forfeiture of property involved in a money laundering transaction, or property traceable to such property, is authorized by Title 18, United States Code, Section 981(a)(1)(A), which allows the United States to forfeit "any property, real or personal, involved in a transaction . . . in violation of section 1956 . . . of this title, or any property traceable to such property."

92. A violation of Title 18, United States Code, Section 1956(a)(1)(B)(i) occurs when a person conducts or attempts to conduct a financial transaction knowing that the transaction involves the proceeds of a specified unlawful activity when the transaction is designed in whole or part "to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of the specified unlawful activity."

93. Wire fraud is a specified unlawful activity pursuant to Title 18, United States Code, Sections 1956(c)(7)(A) and 1961(1). Thus, the Defendant Property not directly traceable to Victim 1 is subject to forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(A) because it was involved in, or is traceable to property involved in, money laundering transactions in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

PRAYER FOR RELIEF

94. The United States requests that due process issue to enforce the forfeiture of the above listed Defendant Property; that notice be given to all interested parties to appear and show cause why

forfeiture should not be decreed; that the Court enter a judgment forfeiting the Defendant Property; and that the United States be awarded such other relief as may be proper and just.

DATED: August 25, 2023

Respectfully submitted,

ISMAIL J. RAMSEY
United States Attorney

/s/
CHRIS KALTSAS
Assistant United States Attorney

VERIFICATION

I, Alfonso Speed, state as follows:

1. I am a Special Agent with the United States Secret Service. I am an agent assigned to this case. As such, I am familiar with the facts and the investigation leading to the filing of this Complaint for Forfeiture.

2. I have read the Complaint and affirm that the allegations contained therein are true.

* * *

I declare under penalty of perjury that the foregoing is true and correct. Executed this 25th day of August, 2023 in San Francisco, California.

Alfonso Speed
Special Agent
United States Secret Service