IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA, PLAINTIFF, *v.* APPROXIMATELY 120,084.5390 TETHER SEIZED FROM BINANCE ACCOUNT ENDING 4607, DEFENDANT.	Civil Action No.

VERIFIED COMPLAINT FOR FORFEITURE

NOW COMES Plaintiff United States of America, by Ryan K. Buchanan, United States Attorney, and Norman L. Barnett, Assistant United States Attorney, for the Northern District of Georgia, and shows the Court the following in support of its Verified Complaint for Forfeiture:

NATURE OF THE ACTION

1. The defendant property consists of 120,084.5390 Tether (USDT) virtual currency that the United States Secret Service ("USSS") seized, pursuant to a Federal seizure warrant on or about August 17, 2023, from the Binance account ending 4607 ("TARGET ACCOUNT")[1] ("Defendant Property").

[1] At the time of this filing, 120,084.5390 USDT is worth the equivalent of approximately $119,968.18 USD.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1345 and 1355.

3. This Court has in rem jurisdiction over the Defendant Property pursuant to 28 U.S.C. § 1355(b)(1)(A) because acts or omissions giving rise to the forfeiture occurred in this district.

4. Venue is proper in this district pursuant to 28 U.S.C. § 1355(b)(1)(A) because the acts or omissions giving rise to the forfeiture occurred in this district.

5. The Defendant Property is presently being held in a custodial virtual wallet maintained by the United States Secret Service.

BASIS FOR FORFEITURE

Relevant Statutes

6. The Defendant Property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) on the grounds that it constitutes or was derived from proceeds traceable to violations of 18 U.S.C. §§ 1349 (conspiracy to commit wire fraud) and 1343 (wire fraud).

7. The Defendant Property is also subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) on the grounds that it constitutes property, real or personal,

involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 and 1957 (money laundering), or is property traceable to such property.

Factual Background

Overview of Pig Butchering Scheme

8. In or around June 2023, the USSS began investigating a suspected "pig butchering" scheme after it received a complaint from an individual with the initials MS.

9. MS resided in the Northern District of Georgia during the time period relevant to this Complaint.

10. "Pig butchering" is a type of romance scam wherein the perpetuators pretend to engage in a romantic relationship with a victim – that is exclusively virtual – for the sole purpose of defrauding the victim out of money.

11. The victims in pig butchering schemes are referred to as "pigs" by the co-conspirators because the co-conspirators use elaborate romantic storylines to "fatten up" victims into believing they are in a romantic relationship.

12. The co-conspirators then introduce to the victim a purported investment cryptocurrency opportunity.

13. Specifically, the co-conspirators claim that they have been investing in cryptocurrency and experiencing drastic profitable returns. The co-conspirators

defraud the victims into believing that they also can experience the profitable returns by investing in the same cryptocurrencies. As part of the scheme, the co-conspirators will direct the victims to fake websites or applications that are designed to look like cryptocurrency investment platforms. In reality, the websites or applications have limited functionality and do not provide the user any access to the cryptocurrency platform or cryptocurrency wallet.

14. The co-conspirators also may show victims images of fake cryptocurrency transactions to further create the impression that the co-conspirators are contributing their own funds to the purported cryptocurrency investment opportunity.

15. The co-conspirators then refer to "butchering" or "slaughtering" the victims once the victim transfers the assets to the fake cryptocurrency investment platform, which actually are transferred to wallets that the co-conspirators control.

Technical Definitions

16. "Virtual currencies" or cryptocurrencies are digital assets designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. Cryptocurrencies are circulated over the Internet as a form of value. Cryptocurrencies operate independently of a central bank. Cryptocurrencies are

similar to paper currency in that the exchange of cryptocurrencies between individuals is not recorded by financial institutions. Cryptocurrencies are not issued by any government, bank or company, but rather are generated and controlled through computer software operating via a decentralized peer-to-peer network.

17. 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. It can be updated multiple times per hour and records every virtual currency address that ever received that virtual currency. The blockchain 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.

18. Cryptocurrencies are sent to and received from "addresses." An address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password or PIN needed to access the address. Only the holder of an address's private key can authorize any transfers of cryptocurrencies from that address to other addresses.

19. To transfer a cryptocurrency to another address, the payor transmits a transaction announcement, cryptographically signed with the payor's private key, across the network. The address of the receiving party and the sender's private key are the only pieces of information needed to complete the transaction. These two keys by themselves rarely reflect any identifying information. As a result, little-to-no personally identifiable information about the payor or payee is transmitted in a transaction itself. Once the payor's transaction announcement is verified, the transaction is added to the blockchain. The blockchain logs every address that has ever received a cryptocurrency and maintains records of every transaction for each address.

20. Cryptocurrency exchanges are businesses that allow customers to trade cryptocurrencies for other assets, such as conventional fiat money or other virtual currencies.

21. Binance is a cryptocurrency exchange and custodian that allows customers to buy, sell and store virtual assets. Binance Global, the Binance entity relevant to this complaint is incorporated in the Cayman Islands.

22. Crypto.com, FTX, and imToken are legitimate cryptocurrency exchanges in which users can purchase, send, receive, and trade virtual currencies.

23. "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."

24. "Ethereum" is an open source, public blockchain-based distributed computing platform and operating system that hosts USDT and ETH virtual currencies.

25. "Ether" ("ETH") is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a platform. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track the movement of ETH.

26. A "transaction hash" is a unique string of letters and numbers generated when a cryptocurrency transaction is initiated. Records of transaction hashes are permanent and publicly available on the Ethereum blockchain.

27. A "wallet" is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

28. "Fiat" funds are any funds declared by a government to be legal tender. An example of fiat funds is the United States Dollar.

The Pig Butchering Scheme Targeting Victim MS

29. On or around June 2022, MS connected with an individual identifying themselves as "Shiman Liu" ("LIU") via text message.

30. LIU did not share any mutual contacts with MS and MS believed that LIU reached out to MS randomly.

31. MS and LIU began chatting frequently through text messages and then moved most of their conversations to Line, an encrypted text messaging application.

32. Initially, conversations between MS and LIU involved hobbies and family.

33. LIU told MS that she had divorced prior to coming to the United States.

34. LIU also sent MS pictures of who MS believed to be LIU through the Line messaging application.

35. Eventually, LIU told MS that she worked for Cylance, a company that manages website security and maintenance for Whitcoin, a digital asset trading platform.

36. LIU also told MS that, because of her position at Cylance, she could see the movement of cryptocurrency through backdoor channels.

37. Additionally, LIU told MS that she saw the movement of several virtual currencies at Whitcoin by an unnamed "big money" market maker and that the group was able to invest such large amounts of money that the investments always made money.

38. LIU also told MS that she used her ability to follow the movement of the market maker to begin investing and trading her own funds, and had seen immediate profit.

39. Ultimately, LIU suggested that MS begin investing and trading with Whitcoin.

40. LIU told MS that, when LIU saw movement within Whitcoin, she would tell MS about the movement and instruct MS on what to do within Whitcoin to help MS make money.

41. USSS has determined that Whitcoin does not operate as a trading platform and, instead, appears to be a fake investment platform established for the purpose of defrauding individuals.

42. Whitcoin's domain ownership history is associated with Whitcex.net.

43. Whitcex.net is registered as an employee-owned web hosting provider.

44. Additionally, an internet keyword search for Whitcoin returns

multiple results that recommend caution when dealing with Whitcoin because of reports of Whitcoin withholding client funds.

45. The Whitcoin website is no longer active.

46. Per LIU's suggestion, MS opened a FTX account to invest in cryptocurrency on the Whitcoin platform.

47. MS also opened a Crypto.com account that allowed MS to make transfers to imToken and transfers from imToken to Whitcoin.

48. LIU instructed MS on what trades to make on the Whitcoin platform.

49. Following LIU's instructions, MS began investing in Ethereum (ETH) and Tether (USDT) on the Whitcoin trading platform.

50. MS viewed what MS believed were profits in the Whitcoin platform.

51. Based on MS's perceived profits and LIU's encouragement, MS continued sending virtual currency to Whitcoin to make what MS believed to be investments on the platform.

52. On or about November 8, 2022, after making a request to withdraw funds from Whitcoin, MS withdrew the equivalent of approximately $55,000.00 USD.

53. Based on the training and experience of law enforcement personnel involved in this investigation, it is common for perpetuators of pig butchering

schemes to allow victims to withdraw perceived profits from fake trading platforms to gain the victim's trust and give the platform the appearance of legitimacy.

54. In or around January 2023, MS made a new request to withdraw funds from Whitcoin.

55. This time, however, MS was told, via a message on the Whitcoin platform, that MS must pay a 20% tax on all of MS's earnings before MS would be able to make a withdrawal.

56. Based on the earnings presented on the Whitcoin platform, the purported tax equaled approximately $740,000.00 USD.

57. LIU assured MS that Whitcoin also had required that LIU pay a 20% tax when she withdrew funds. LIU claimed that her tax only had been $400,000.00 USD because she had earned less than MS.

58. LIU also told MS that, once LIU paid her tax, she would help MS pay MS's tax.

59. LIU subsequently told MS that LIU had been able to withdraw her funds after paying the 20% tax and provided MS a purported screenshot of her withdrawal record sent via a message on the Line application.

60. LIU assured MS that LIU would give MS approximately $600,000.00

USD, a combination of her money and money from one of her friends from Cylance, to pay the tax.

61. LIU sent MS a screencap purporting to be from the Whitcoin platform indicating that LIU transferred $600,000.00 to MS, which caused MS to believe that LIU transferred the funds directly to MS in the Whitcoin exchange.

62. Thereafter, Whitcoin, via a message on the Whitcoin platform, informed MS that MS must pay approximately $150,000.00 USD to access the $600,000.00 USD transferred to MS by LIU.

63. MS borrowed money from friends and obtained loans to pay the purported tax.

64. After MS paid the purported tax, Whitcoin emailed MS that because MS had been three days late, MS now had to pay an additional $90,000.00 USD to increase MS's "credit."

65. Based on this requirement from Whitcoin, MS borrowed $90,000.00 USD and paid Whitcoin.

66. Whitcoin, through a message on the Whitcoin platform, informed MS that MS's account was suspicious and MS was required to pay a $250,000.00 USD refundable deposit to verify MS's account and withdraw more funds from Whitcoin.

67. MS informed LIU that MS did not have the money to pay Whitcoin the amount requested.

68. LIU, again, sent MS a screencap purporting to be from the Whitcoin platform indicating that LIU transferred $250,000.00 USD to MS's Whitcoin account, which made MS believe that LIU transferred funds to MS's Whitcoin account so MS could pay the amount requested by Whitcoin.

69. Because of the supposed fees being charged by Whitcoin, LIU suggested that MS transfer the funds in her account to "Emirexpro.com," which was supposed to be another cryptocurrency investment platform.

70. The USSS has determined that Emirexpro.com is another fake investment platform established for the purpose of defrauding individuals.

71. On or about March 31, 2023, based on transactions perceived on the Emirexpro platform, MS believed that MS transferred the total of what MS believed to be MS's Whitcoin funds, the equivalent of approximately $5,500,000.00 USD, to Emirexpro.com.

72. MS was then told by Emirexpro, through a message on the chat feature of Emirexpro's platform, that MS would need to pay $50,000.00 USD to upgrade MS's account to VIP status, which would allow MS to withdraw funds.

73. At this point, MS contacted law enforcement officials and reported

that MS had been defrauded.

74. Altogether, from approximately September 23, 2022 through February 14, 2023, MS sent the equivalent of approximately $1,600,000.00 USD in virtual currency to Whitcoin.

Fraud Proceeds Obtained from MS were Transferred to TARGET ACCOUNT

75. USSS's review of the blockchain verifies the transactions made by MS and further reflects that MS's funds were transferred to the TARGET ACCOUNT and other addresses that received other known fraud proceeds.

76. Each transaction reviewed by USSS during the investigation involving the pig butchering scheme discussed herein corresponds with its own unique transaction hash.

77. The Ethereum blockchain reflects that, on or about September 25, 2022, MS sent 10.82 ETH[2] from his imToken wallet to a wallet address beginning with 0x6f047d2f.

78. Days later, on or about September 28, 2022, MS sent 116.4 ETH[3] from his imToken wallet to the same wallet beginning with 0x6f047d2f.

---

[2] As of the date of this filing, 10.82 ETH is worth the equivalent of approximately $21,719.74 USD.

[3] As of the date of this filing, 116.4 ETH is worth the equivalent of approximately $233,657.87 USD.

79. MS, on or about October 19, 2022, also sent 144 ETH[4] from his imToken wallet to a wallet address beginning with 0x9fbd9b6c.

80. A review of the Ethereum blockchain shows that, for each of the instances described in Paragraphs 77 through 79 where MS believed MS sent ETH to Whitcoin, the ETH was converted into USDT after being sent to Tokenlon, a decentralized cryptocurrency exchange.

81. Based on the training and experience of law enforcement personnel involved in this investigation, converting one virtual currency to another amid rapid transfers is done in an attempt to confuse or evade law enforcement and conceal proceeds of criminal activity.

82. The ETH sent by MS was then rapidly transferred through multiple hops, that is, different wallet addresses, before reaching the TARGET ACCOUNT.

83. Some of the above-described hops formed a circular flow of funds.

84. For example, USSS determined that the ETH that MS believed MS sent to Whitcoin on or about September 25, 2022 and September 28, 2022, after being converted to USDT, hopped through a wallet with an address beginning with 0x1e8b3cae and a wallet with an address beginning with 0xfb996c3c prior to

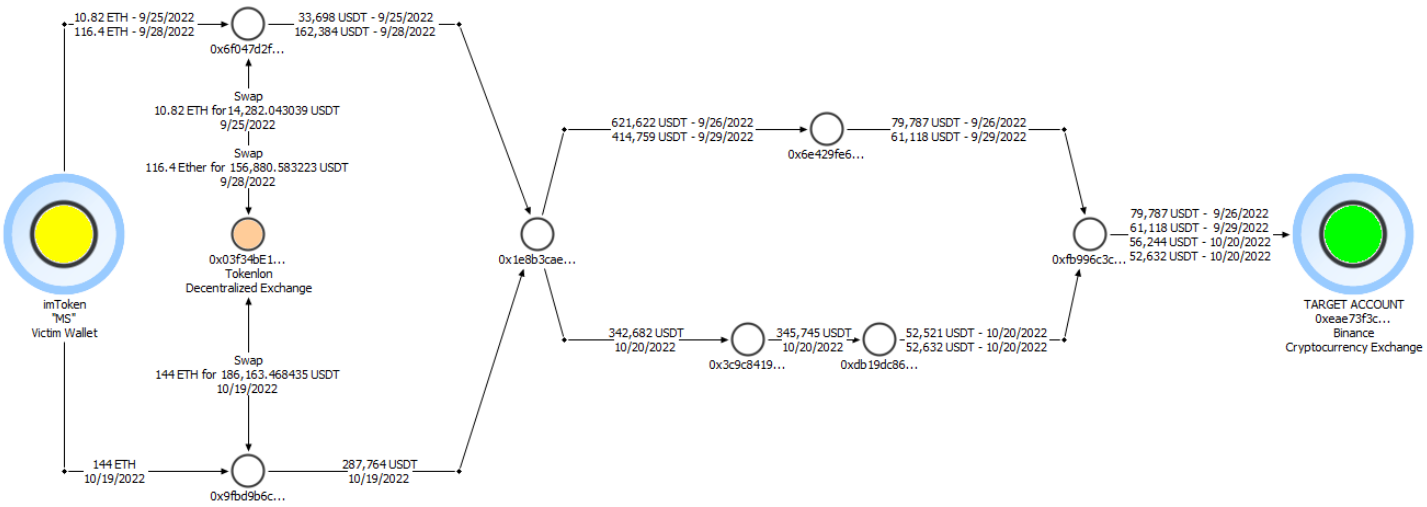
[4] As of the date of this filing, 144 ETH is worth the equivalent of approximately $288,061.28 USD.

entering the TARGET ACCOUNT.

85. Similarly, the ETH that MS believed MS sent to Whitcoin on or about October 19, 2022, after being converted to USDT, also hopped through the same wallet with an address beginning with 0x1e8b3cae and the same wallet with an address beginning with 0xfb996c3c prior to entering the TARGET ACCOUNT.

86. The Ethereum blockchain further revealed that the funds described in Paragraphs 77 through 79 were hopped through multiple wallets, and transferred into TARGET ACCOUNT – all approximately one day after MS initially sent the ETH.

87. The following diagram shows the transactions described in paragraphs 77 through 86, including MS's transfers of the ETH from his imToken wallet on September 25, 2023, September 28, 2023 and October 19, 2023, the ETH being converted into USDT, and the converted funds being deposited into the TARGET ACCOUNT.



88. USSS reviewed records for nine accounts held at cryptocurrency exchanges, including the TARGET ACCOUNT, that received MS's funds and determined that the accounts were consistent with pig butchering schemes because the accounts displayed a history of frequent, large dollar deposit transactions followed by a pattern of rapid movement of funds with large corresponding withdrawals.

The TARGET ACCOUNT is Associated with Fraud Schemes Targeting Other Victims

89. USSS determined that other victims who reported being victimized through fraudulent investment schemes were associated with the wallet addresses connected with the TARGET ACCOUNT.

90. More specifically, USSS analyzed the USDT wallet addresses used in hops between victim MS sending ETH to Whitcoin and MS's funds reaching the TARGET ACCOUNT.

91. The analysis revealed that victims filed complaints with the Federal Bureau of Investigation's Internet Crime Complaint Center ("IC3") or the Federal Trade Commission's ("FTC's") Consumer Sentinel Database regarding the same wallet addresses through which MS's funds flowed before reaching the TARGET ACCOUNT.

92. Altogether, the TARGET ACCOUNT processed virtual currency equaling the equivalent of approximately $45,238,693.78 USD between November 2018 and June 2023.

FIRST CLAIM FOR FORFEITURE
18 U.S.C. § 981(a)(1)(C)

93. The United States re-alleges and incorporates by reference Paragraphs 1 through 92 of this Complaint as if fully set forth herein.

94. Based on the foregoing, the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(C) on the grounds that the funds constitute or were derived from proceeds traceable to violations of 18 U.S.C. §§ 1349 (conspiracy to commit wire fraud) and 1343 (wire fraud).

SECOND CLAIM FOR FORFEITURE
18 U.S.C. § 981(a)(1)(A)

95. The United States re-alleges and incorporates by reference Paragraphs 1 through 92 of this Complaint as if fully set forth herein.

96. The Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) on the grounds that the funds constitute property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 and 1957 (money laundering), or is property traceable to such property.

PRAYER FOR RELIEF

WHEREFORE, the United States prays:

(1) that the Court forfeit the Defendant Property to the United States of America;

(2) that the Court award the United States the costs of this action; and

(3) such other and further relief as the Court deems just and proper.

This 27th day of November 2023.

Respectfully submitted,

RYAN K. BUCHANAN
United States Attorney
75 Ted Turner Drive SW
Atlanta, GA 30303
(404) 581-6000 fax (404) 581-6181

/s/NORMAN L. BARNETT
Assistant United States Attorney
Georgia Bar No. 153292
Norman.barnett@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA, PLAINTIFF, *v.* 120,084.5390 TETHER SEIZED FROM BINANCE ACCOUNT ENDING 4607, DEFENDANT.	Civil Action No.

VERIFICATION OF COMPLAINT FOR FORFEITURE

I, Tyler LaBarr, have read the Complaint for Forfeiture in this action and state that its contents are true and correct to the best of my knowledge and belief based upon my personal knowledge of the case and upon information obtained from other law enforcement personnel.

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

This 27th day of November 2023.

Tyler LaBarr

TYLER LABARR
SPECIAL AGENT
UNITED STATES SECRET SERVICE