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

UNITED STATES OF AMERICA PLAINTIFF, *v.* 56,382.9700 TETHER SEIZED FROM BINANCE ACCOUNT ENDING 1678; AND 0.03001485 ETHER SEIZED FROM BINANCE ACCOUNT ENDING 1678 DEFENDANTS.	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 the following virtual currency that the United States Secret Service ("USSS") seized, pursuant to a Federal search warrant on or about June 20, 2023:

a. 56,382.9700 Tether (USDT) seized on or about June 20, 2023, from

the Binance account ending 1678 ("TARGET ACCOUNT"),[1] and

b. 0.03001485 Ether (ETH) seized on or about June 20, 2023 from TARGET ACCOUNT.[2]

(collectively, "Defendant Property").

2. The Defendant Property is presently located in a custodial virtual wallet maintained by the United States Secret Service.

JURISDICTION AND VENUE

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

4. 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.

5. 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.

6. The Defendant Property is presently being held in a government account maintained by the United States Secret Service.

---

[1] At the time of this filing, 56,382.9700 USDT is worth the equivalent of approximately $56,401.86 USD.

[2] At the time of this filing, 0.03001485 ETH is worth the equivalent of approximately $50.45 USD.

BASIS FOR FORFEITURE

Relevant Statutes

7. 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).

8. 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

Pig Butchering Overview

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

10. MC resided in the Northern District of Georgia during the time period relevant to this Complaint.

11. "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.

12. 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.

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

14. 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.

15. 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.

16. The co-conspirators then refer to "butchering" or "slaughtering" the victims once the victim transfers the assets, which the co-conspirators then steal.

Technical Definitions

17. "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.

18. 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.

19. 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.

20. 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.

21. "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."

22. USD Coin, widely known as "USDC," is another blockchain-based cryptocurrency whose tokens in circulation are backed by an equivalent amount. It is also a stablecoin.

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

24. "Ether" ("ETH") is a cryptocurrency that is open source, public, has a 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.

25. "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, all while using the Ethereum blockchain protocol to maintain transparency. When engaged, smart contracts automatically execute according to the terms of the contract written into lines of code.

26. 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.

27. "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 MC

28. In or around December 2022, MC met an individual identifying himself as "John Jay" ("JAY") via Instagram, a social networking platform.

29. JAY did not share any mutual contacts with MC and MC believed that JAY reached out to MC randomly.

30. JAY and MC began chatting via Instagram and eventually moved their conversations to WhatsApp, an encrypted text messaging application.

31. JAY told MC that he graduated from Harvard University, had been a successful businessman in China, and had recently moved to Los Angeles, California.

32. The pictures posted on JAY's Instagram account gave the appearance that JAY was wealthy and lived a lavish lifestyle.

33. Conversations between JAY and MC initially involved personal topics, such as family and travel, but JAY began telling MC that he and his uncle recently made successful investments in cryptocurrency through an investment

platform called Bereajoy.

34. Based on the training and experience of law enforcement personnel involved in this investigation, it is common for perpetrators of pig butchering schemes to gain an individual's trust over days, weeks, or months by using manipulative tactics and language before inviting victims to participate in fake cryptocurrency investments.

35. USSS has determined that Bereajoy.com and Bereajoy's application were fronts for a fake cryptocurrency investment platform established for the purpose of defrauding individuals.

36. JAY instructed MC to download the Bereajoy mobile application from a link on the Bereajoy website.

37. MC downloaded the Bereajoy mobile application, as instructed.

38. After MC downloaded Bereajoy, JAY instructed MC to open an account on Crypto.com.

39. Crypto.com is a legitimate cryptocurrency exchange where users can purchase, send, receive, and trade virtual currencies.

40. MC again followed JAY's instructions and opened a Crypto.com account.

41. JAY also told MC to wire fiat funds from MC's bank account to MC's

Crypto.com account to purchase USDT or ETH virtual currencies because doing so would make it easier to invest on the Bereajoy platform.

42. JAY instructed MC to contact Bereajoy customer service through the application to receive an address to send funds to from MC's Crypto.com account.

43. JAY also encouraged MC to begin investing in smaller amounts, such as $1,100.00 USD, $1,900.00 USD, and $2,800.00 USD, which MC did.

44. MC saw what MC believed to be profits on Bereajoy and increased the amounts of subsequent investments.

45. Between January 25, 2023 and March 14, 2023, MC sent the equivalent of approximately $240,592.00 USD from MC's Crypto.com account to Bereajoy.

46. On or about March 15, 2023, after making a request to withdraw funds from Bereajoy, MC received an email purportedly from Bereajoy customer service indicating that MC's withdrawal request was rejected.

47. Someone purporting to work in customer service for Bereajoy told MC that MC owed a 25% "profit tax" to the "International Tax Bureau," which equaled 133,256.8766 USDT, the equivalent of approximately $133,256.88 USD, and that MC's account would be frozen in 72 hours if the tax payment was not received.

48. USSS has been unable find any legitimate entity called the

"International Tax Bureau."

49. MC discussed the purported tax with JAY, and he instructed MC to pay the tax.

50. Between March 21, 2023 and March 29, 2023, MC sent 114,065.05 USDT, the equivalent of approximately $114,065.05 USD, from MC's Crypto.com account to Bereajoy to pay the purported tax.

51. On or about March 30, 2023, MC received an email purportedly from Bereajoy indicating that MC's withdrawal request was rejected by the "blockchain node" due to "multiple funds in your account with unknown sources."

52. MC was then instructed by Bereajoy to pay 54,250 USDT, the equivalent of approximately $54,250.00 USD, by April 5, 2023, to prove that MC was using the account legally.

53. On April 4, 2023, MC withdrew 54,593.95 USDT, the equivalent of approximately $54,593.95 USD, from MC's Crypto.com account and sent the funds to Bereajoy.

54. On April 5, 2023, MC received an email from Bereajoy indicating the withdrawal application was approved but that MC owed a service fee of 15% of the total assets in the account because the account balance exceeded 500,000.00 USDT.

55. MC was instructed to pay the 137,730.0344 USDT service fee, the equivalent of approximately $137,730.03 USD, to Bereajoy by April 10, 2023.

56. MC was told that, if the service fee was not paid, MC's account would be frozen, and a late fee would be assessed.

57. MC spoke with an individual purporting to work at Bereajoy to ask if funds in MC's account could be used to pay the service fee.

58. In response, the purported representative from Bereajoy told MC that the service fee could not be deducted from the USDT balance, and that MC had to use MC's own bank account to pay the service fee before funds could be restored to "normal use."

59. On April 10, 2023, MC made one withdrawal totaling 50,635.10 USDT, the equivalent of approximately $50,635.10 USD, from MC's Crypto.com account and sent the funds to Bereajoy.

60. That same day, MC received an email from Bereajoy instructing MC to pay the remaining balance of the service fee.

61. MC then told JAY that MC would have a difficult time paying the service fee.

62. In response, JAY encouraged MC to use all possible means to gather the funds to pay the fee.

63. Based on these instructions, MC took out a personal loan to pay the service fee.

64. JAY told MC that he would assist with the service fee and sent MC a screenshot showing that he made a payment of over 30,000.00 USDT to Bereajoy on MC's behalf.

65. On April 14, 2023, MC withdrew 59,250.70 USDT, the equivalent of approximately $59,250.70 USD, from MC's Crypto.com account and sent the funds to Bereajoy.

66. Thereafter, MC received an email from Bereajoy saying MC's account had been returned to normal status and MC could withdraw money.

67. On or about April 15, 2023, MC received an email purportedly from Bereajoy indicating that MC's withdrawal request was rejected "by the blockchain node."

68. This time, MC was instructed to pay 91,860.2847 USDT, the equivalent of approximately $91,860.28 USD, as a "risk verification fund" to verify the security on MC's account. Again, Bereajoy told MC that the account would be frozen if the fee was not paid.

69. On April 23, 2023, MC received an email from Bereajoy indicating that MC had not timely paid the risk verification fund, that MC's account was

temporarily frozen, and that, if payment was not made, the account would be permanently frozen.

70. Altogether, MC lost the equivalent of approximately $516,000.00 USD to the pig butchering scheme involving JAY and Bereajoy.

Fraud Proceeds Obtained from MC were Transferred to TARGET ACCOUNT

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

72. Specifically, the Ethereum blockchain reflects that on or about February 17, 2023, an address that USSS confirmed belonged to MC transferred approximately 14,990 USDC, the equivalent of approximately $14,990.00 USD, to a wallet address beginning with 0x8e3521af.

73. The Ethereum blockchain further reflects that on or about February 18, 2023, 14,990 USDC was transferred from 0x8e3521af to a wallet address beginning with 0xc8f9d239.

74. Based on USSS's review of the blockchain, between February 18, 2023 and April 21, 2023, MC's funds were transferred through approximately 11 hops before reaching the TARGET ACCOUNT.

75. A "hop" is a transfer between wallet addresses.

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

77. Based on the training and experience of law enforcement personnel investigating this case, there is no apparent lawful purpose for moving funds in a circular pattern because each transfer involves transaction fees and moving virtual currency in such a manner is likely an attempt to further evade law enforcement, which is consistent with money laundering practices.

Fraud Proceeds from Other Victims were Transferred to TARGET ACCOUNT

78. During its investigation, USSS determined that roughly 46 victims, many of which reported being victimized through fraudulent investments, were associated with addresses connected with the TARGET ACCOUNT.

79. USSS analyzed the hops used to transfer MC's funds and located reports of additional fraud involving addresses through which MC's funds hopped.

80. For example, USSS determined that a USDT address starting with 0xf38665c6, an address through which MC's funds hopped, interacted with an address where an individual reported being a victim of a scam to the Federal Bureau of Investigation's Internet Crime Complaint Center ("IC3").

81. Similarly, USSS determined that MC's funds also hopped through an Ethereum address starting with 0x8e3521af, which is the same address that 13

other victims reported sending cryptocurrency to in IC3.

82. Altogether, 46 victims, through IC3, reported being the victim of fraud related to addresses associated with the TARGET ACCOUNT.

83. Collectively, the aforementioned victims reported losses equaling the equivalent of approximately $8,257,408.08 USD.

84. Based on the training and experience of the law enforcement personnel involved in this investigation, the presence of numerous victims of similar fraud depositing funds into the same addresses indicates that the addresses involved also are used in the fraudulent scheme.

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

85. The United States re-alleges and incorporates by reference Paragraphs 1 through 84 of this Complaint as if fully set forth herein.

86. 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)

87. The United States re-alleges and incorporates by reference

Paragraphs 1 through 86 of this Complaint as if fully set forth herein.

88. 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 23rd day of October 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.* 56,382.9700 TETHER SEIZED FROM BINANCE ACCOUNT ENDING 1678; AND 0.03001485 ETHER SEIZED FROM BINANCE ACCOUNT ENDING 1678 DEFENDANTS.	Civil Action No.

VERIFICATION OF COMPLAINT FOR FORFEITURE

I, Kelly Wilson, 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 23rd day of October 2023.

KELLY WILSON
SPECIAL AGENT
UNITED STATES SECRET SERVICE