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

UNITED STATES OF AMERICA Plaintiff, v. $367,026.14 IN UNITED STATES CURRENCY Defendant.	§ § § § § § § §	NO: 6:25-cv-00114

AFFIDAVIT IN SUPPORT OF COMPLAINT FOR FORFEITURE

I, Brad Schley, after being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service (USSS) and have been so employed since September 2001. My current position is the Resident Agent in Charge (RAIC) of the USSS Tyler Resident Office. During my tenure with the Secret Service, I have been assigned to investigate violations of federal laws, including violations of Title 18 of the United States Code, specifically those related to the passing of counterfeit United States currency, money laundering, and wire fraud. I received criminal investigative training at the Federal Law Enforcement Training Center in Glynco, Georgia, and at the James J. Rowley Secret Service Training Center in Beltsville, Maryland, pertaining to criminal investigations of counterfeit currency, bank fraud, money laundering, wire fraud, access device fraud, and identity theft. During my employment with the USSS, I have conducted investigations resulting in the arrest of

suspects and seizures of criminally derived property. I am an investigative and law enforcement officer of the United States, in that I am empowered by law to conduct investigations and to make arrests for felony offenses, under authority of 18 U.S.C. § 3056.

2. The statements contained in this affidavit are based in part upon my experience, my knowledge of the facts and circumstances surrounding this investigation, and on information provided to me by other law enforcement personnel and other witnesses.

PROPERTY FOR FORFEITURE

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

a. $237,426.83 in JP Morgan Chase (JPMC) Bank account XXXXX1823 (Target Account 1); and

b. $129,599.31 in JPMC Bank account XXXXX9738 (Target Account 2);

that totals $367,026.14 into Check No. 4557161023 and was seized on or about December 5, 2023, in Tyler, Texas pursuant to a seizure warrant.

LEGAL AUTHORITY FOR FORFEITURE

4. The funds to be forfeited represent proceeds of a fraudulent cryptocurrency investment scheme that often utilizes spoofed domains. The term "spoofed" refers to domain spoofing and involves a cyberattack in which fraudsters and/or hackers seek to

persuade consumers that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a false site controlled by a cybercriminal. In particular, the unknown scammers promoted spoofed domains and websites purporting to look like legitimate cryptocurrency trading platforms to U.S. based victims, to include victims located in the Eastern District of Texas. Scammers then fooled victims into "investing" in cryptocurrency through these fraudulent investment platforms, which instead allowed the scammers to steal the victims' money.

5. This type of scam is often identified as a cryptocurrency investment fraud scheme and involves scammers spending significant time getting to know, targeting and grooming their victims to gain their confidence. After developing a relationship and gaining trust, scammers instruct their victims to visit the spoofed domains to get them to make significant capital investments in what victims believe are legitimate cryptocurrency trading platforms. The victims are then typically asked to invest their funds through a provided BTC, USDT, ETH or USDC deposit address, and are further told they can expect to make a sizeable return on their investments. As initial smaller investments are made, the spoofed websites falsely display a significant increase in the victim's account balance, which entices the victim to continue making investments, which typically end with a final large deposit or transaction. When the victim attempts to make a withdrawal, the scammers attempt to coerce the victims to make additional investments. These tactics can include requesting additional investments due to

"significant profits" gained on the account or other reasons such as freezing the account due to "taxes owed" or "suspicious behavior." Regardless of how the scammers attempt to solicit additional investments from the victims, the victims are unable to retrieve a large portion of their investment.

6. I believe the above-listed property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) because the property was involved in or traceable to property involved in money laundering in violation of 18 U.S.C §§ 1956 or 1957, or constitutes proceeds from a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)).

7. Any property, real or personal, which was involved in a transaction in violation of 18 U.S.C. §§ 1956 or 1957 or any property traceable to such property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

8. 18 U.S.C. § 1956 (a)(1) makes it a crime to knowingly conduct or attempt to conduct a "financial transaction" with proceeds from "specified unlawful activity" (SUA) with specific intent to: promote the SUA, conceal or disguise the source, origin, nature, ownership, or control of the proceeds; or evade reporting requirements.

9. The purpose of "money laundering" as defined by 18 U.S.C. § 1956 is to disguise illicit nature of funds by introducing it into legitimate commerce and finance thereby making them "clean." This financial process is most commonly conducted using three steps referred to as "placement," "layering," and "integration." Typically, the

"placement" phase of this financial process takes place when proceeds from illicit sources are placed in a financial institution or business entity. "Layering" takes place when these funds are then used in seemingly legitimate commerce transactions which makes the tracing of these monies more difficult and removed from the criminal activity from which they are a source. Finally, the "integration" phase is when these funds are then used to promote the unlawful activity or for the personal benefit of the money launderers and others.

10. I also have probable cause to believe that this property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) because the property constitutes or is derived from proceeds traceable to violations of 18 U.S.C. § 1343 or a conspiracy to commit such offense (18 U.S.C. § 1349). Wire fraud is an SUA.

11. Any property, real or personal, which constitutes proceeds or is derived from proceeds traceable to a violation of 18 U.S.C. § 1343 or 1349 is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

12. Under 18 U.S.C. § 984, for any forfeiture action in rem in which the subject property consists of cash, monetary instruments in bearer form, or funds deposited in an account in a financial institution:

a. The government need not identify the specific funds involved in the offense that serves as the basis for the forfeiture;

b. It is not a defense that those funds have been removed and replaced

by other funds; and

c. Identical funds found in the same account as those involved in the offense serving as the basis for the forfeiture are subject to forfeiture.

13. In essence, 18 U.S.C. § 984 allows the government to seize for forfeiture identical property found in the same place where the "guilty" property had been kept.

FACTS SUPPORTING FORFEITURE

14. The United States is investigating a cryptocurrency investment fraud scheme that utilizes spoofed domains. The investigation concerns possible violations of, inter alia, 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud) and 18 U.S.C. §§ 1956 and 1957 (Laundering of Monetary Instruments).

15. The case involves the laundering of proceeds obtained from victims of the fraudulent scheme. Part of the money laundering scheme was to funnel proceeds from victims through the various business accounts to accounts located abroad. One business, identified as Elights Trading Inc., held a bank account that served as a funnel account and received fraud proceeds from bank accounts held in the names of the victims. The Elights Trading Inc. bank account was provided to victims located within the Eastern District of Texas as a means in which they would pay their "taxes and/or fees" concerning their "earnings" as part of this scheme.

16. Investigators interviewed multiple victims who sent funds to the Citibank held in the name of Elights Trading. In summary, these victims reported to have been tricked into believing they were investing in cryptocurrency, when in fact they were provided with links or information leading them to use spoofed domains or applications of legitimate cryptocurrency exchanges. One of these victims was identified as T.G.

Victim T.G.

17. Investigators interviewed victim T.G. regarding the $230,000 transaction remitted to the ELIGHTS TRADING Account. T.G. met a friend on Facebook in or about May 2023, but has never met this individual face to face. T.G.'s new female friend portrayed herself as being very wealthy and T.G. inquired how he could invest money to earn a large and safe return. T.G.'s friend provided a link to Telegram where he was led to believe he was working with employees of OKEX, a cryptocurrency exchange. T.G. received instructions via Telegram regarding investments, including the information for the ELIGHTS TRADING account. T.G. stated he believed he was purchasing options in cryptocurrency and not specific cryptocurrency coins such as Bitcoin. T.G. has invested approximately $850,000 in total by sending to other bank accounts he received from the OKEX Telegram communications. T.G. stated he has only requested small withdrawals from his investment and has received only a few thousand dollars and has not made any large withdrawal requests.

18. T.G. informed USSS investigators that during this scheme, he was provided the JPMC Bank account in the name of SUNSHINES TRADING, account number ending in 2181. A review of JPMC Bank records pertaining to this account reflect T.G. sent $80,000 to this account on September 20, 2023.

Victim A.V.V.

19. USSS investigators interviewed victim A.V.V. regarding the $55,750.00 transaction she sent to the JPMC account in the name of SUNSHINES TRADING, account number ending in 2181. A.V.V. was contacted by an individual via LinkedIn using the name Toby Li, who stated he worked for Apple and was impressed with A.V.V.'s qualifications. A.V.V. explained that Toby Li eventually convinced A.V.V. into investing in cryptocurrency by funding a crypto.com account and sending funds to a wallet A.V.V. was made to believe existed at Blackcoin.com. A.V.V. provided transaction details of the funds she sent as part of this scheme, which included $17,000 on July 28, 2023, to Target Account 1 and $20,000 on October 16, 2023 to Target Account 2. A.V.V. stated she has not been able to retrieve her funds as she was promised. A.V.V. stated she has suffered a great financial loss of approximately $300,000.00 because of this scheme.

20. USSS investigators obtained Internet Crime Complain Center (hereafter known as IC3) reports regarding queries related to STONE WATER TRADING. There were thirteen reports by separate victims whose transactions totaled $622,568.00. A

review of JPMC bank records regarding Target Account 1 verified these deposits as reflected in these IC3 reports. These victims all reported similar instances as other victims who were previously interviewed by USSS investigators throughout this investigation.

TARGET ACCOUNTS' INFORMATION AND TRANSACTIONS

21. Investigators issued a Federal Grand Jury subpoena to JPMC and obtained the bank records for the JPMC Bank accounts in the name of STONE WATER TRADING LLC, account number ending in 1823 (Target Account 1); and the account held in the name of SUNNY PACIFIC LLC, account number ending in 9738 (Target Account 2). These bank records identified the signor on Target Account 1 as JIAO JIAO LIU . The records indicate that on or about January 6, 2023, LIU opened the business bank account identifying STONE WATER TRADING LLC as a limited liability company. The records reflect that LIU provided the business address of 1000 W. 8th Street, Apartment 828, Los Angeles, California 90017.

22. USSS investigators familiar with the apartment building located at 1000 W. 8th Street, Apartment 828, Los Angeles, California 90017 identified this location is in downtown Los Angeles. This area has significant business activity due to its location. However, USSS investigators were unable to discover any business activity related to STONE WATER TRADING LLC at this location.

23. Investigators were unable to locate an Internet business presence for Stone Water Trading LLC or Sunny Pacific LLC.

24. Analysis of the bank records for Target Account 1 indicate the account's activity from July 1 through September 27, 2023, included several deposits via wire transfers and other payments such as Zelle transactions totaling approximately $10,101,898.00. These transactions resembled deposits from mostly individuals that were similar to other accounts identified in this investigation as having received proceeds of the fraudulent cryptocurrency investment scheme.

25. The following wire deposits were made into Target Account 1 and are a small sampling of the total deposits into Target Account 1:

DATE	VICTIM	AMOUNT
7/28/2023	A.V.V.	$17,000.00
8/1/2023	C.S.P.	$8,800.00
8/30/2023	M.T.M.	$12,500.00
9/1/2023	S.D. Jr.	$70,000.00
9/1/2023	A.K.	$20,000.00
9/1/2023	D.S.	$16,500
9/1/2023	W.C.	$15,303.00
9/1/2023	C.M.Y.	$10,000.00
9/1/2023	RNS TR.	$7,800.00
9/1/2023	J.C.	$5,100.00
9/1/2023	E.S.C.	$6,000.00
9/5/2023	J.D.O.	$59,000.00
9/5/2023	J.M.R.	$50,000.00
9/5/2023	A.R.C.	$40,000.00
9/5/2023	S.L.	$32,000.00
9/5/2023	D.A.S.	$25,000.00
9/5/2023	R.D.Q.	$24,000.00
9/5/2023	T.K.	$6,823.58
9/5/2023	W..L.U.G.	$6,000.00

9/5/2023	M.T.M.	$5,145.00
9/5/2023	R.P.Z.	$5,000.00
9/5/2023	T.H.	$1,165.00
9/6/2023	G.A.R.	$48,612.00
9/6/2023	K.M.	$35,000.00
9/6/2023	S.A.T.	$5,100.00
9/6/2023	L.L.B.	$3,900.00
9/7/2023	R.J.G.	$137,835.00
9/7/2023	L.A.S.	$55,000.00
9/7/2023	R.M.S.	$20,000.00
9/7/2023	C.E.S. Jr.	$14,800.00
9/7/2023	H.S.F.	$14,133.00
9/7/2023	Y.R.L.T.	$10,000.00
9/8/2023	G.A.M.	$52,000.00
9/8/2023	E.Z.	$40,000.00
9/8/2023	S.Y.A.	$10,000.00
9/8/2023	J.R.K. Jr.	$10,000.00
9/8/2023	Y.L.	$3,017.00
9/11/2023	J.K.	$100,000.00
9/11/2023	N.N.H.	$35,000.00
9/11/2023	M.J.V.	$25,000.00
9/11/2023	F.J.R.	$25,000.00
9/11/2023	P.K.N.	$25,000.00
9/11/2023	R.H.	$21,000.00
9/11/2023	K.D.	$19,000.00
9/11/2023	CHUCHI	$15,000.10
9/11/2023	R.T.R.	$10,000.00
9/11/2023	T.K.	$5,000.00
9/11/2023	C.C.	$3,000.00
9/12/2023	J.K.H.	$393,000.00
9/12/2023	M.O.S.	$165,000.00
9/12/2023	M.C.O.	$140,000.00
9/12/2023	C.W.B.	$100,040.00
9/12/2023	G.G.	$40,000.00
9/12/2023	F.E.S. Jr.	$25,000.00
9/12/2023	R.D.	$15,000.00
9/12/2023	F.J.R.	$13,000.00
9/12/2023	S.S.A.	$10,001.00
9/12/2023	M.A.D.	$8,500.00

9/12/2023	S.M.P.	$8,200.00
9/12/2023	K.C.D.	$8,000.00
9/12/2023	D.W.	$5,000.00
9/12/2023	C.C.	$4,000.00
9/12/2023	M.T.M.	$3,200.00
9/13/2023	J.K.	$100,000.00
9/13/2023	G.A.R.	$60,000.00
9/13/2023	M.J.V.	$25,000.00
9/13/2023	P.K.N.	$25,000.00
9/13/2023	M.O.S.	$25,000.00
9/13/2023	S.S.	$15,000.00
9/13/2023	R.J.	$230,000.00
9/20/2023	H.F.Y.	$118,000.00

INTERVIEWS OF ADDITIONAL VICTIMS THAT SENT FUNDS TO TARGET ACCOUNT 1

26. In addition to victim A.V.V., investigators interviewed additional victims who were identified as having sent funds to Target Account 1 as a result of a cryptocurrency investment fraud scheme.

Victim T.K.

27. USSS investigators identified and interviewed victim T.K. regarding the $10,000 transaction he sent to a suspect account that was previously seized in this investigation pursuant to a search and seizure warrant. T.K. stated he received a wrong number call from an unknown female subject on or about August 3, 2023. T.K. stated the unknown female caller befriended him and they communicated often. T.K. stated their conversations turned to investments and how to make money by investing in Gold via "Goldman Sachs." T.K. stated he sent various wire transfers to bank accounts that were identified to him by the unknown female and claimed he was able to make small cash

withdrawals early on in the scheme. T.K. stated he was persuaded to invest additional funds and when he attempted to make larger withdrawals from his "investment account," he was informed he needed to pay fees equal to 10% of his "earnings." T.K. stated he paid the 10% fee and an additional 15% fee to separate entities, and still was unable to withdraw any of his funds.

28. T.K. stated in addition to a previously seized account in this investigation, he also sent payments to Target Account 1 as noted here:

9/05/23	$6,823.58	Stone Water Trading LLC/JPMC
9/11/23	$5,000.00	Stone Water Trading LLC/JPMC

29. T.K. stated he also sent $20,000 to a JPMC account in the name of Metapay Technology LLC. USSS investigators learned that the JPMC account in the name of Metapay Technology LLC was previously closed by JPMC for reports of similar fraud activity.

30. USSS investigators reviewed IC3 reports submitted by individuals who sent funds to Target Account 1 as part of the fraudulent cryptocurrency investment scheme. The individuals reported to IC3 similar circumstances as other victims that sent funds to Target Account 1. The IC3 reports were dated from on or about August 1, 2023, to September 27, 2023, and report that seven (7) separate individuals sent funds to Target Account 1 totaling approximately $522,745.00.

31. Some of the victims who reported the fraud by filing IC3 reports not only sent to Target Account 1, but they also reported to have sent funds to other accounts previously seized during this investigation.

INVESTIGATION IDENTIFIES TARGET ACCOUNT 2 AS RECEIVING VICTIMS' FUNDS

32. USSS investigators discovered TARGET ACCOUNT 2 was held in the name of Sunny Pacific LLC. USSS investigators reviewed the bank records for Target Account 2 and discovered that this account was also utilized to receive funds from victims of this cryptocurrency investment fraud scheme.

33. Bank records reveal that Target Account 2 was opened on or about September 19, 2023, and the signor on the account was Qian Sun. The address utilized for this account is 24206 Sylvan Glen Road, Unit G, Diamond Bar, California 91765.

34. Investigators located business records for Sunny Pacific LLC were filed with the State of California Secretary of State on or about September 20, 2023. The records indicate Sunny Pacific LLC utilizes address 24206 Sylvan Glen Road, Unit G, Diamond Bar, California 91765. The reported manager or member of Sunny Pacific LLC is identified as Qian Sun.

35. Analysis of the bank records for Target Account 2 indicate the account received deposits totaling approximately $1,508,210.14. These transactions resembled deposits from mostly individuals that were similar to other accounts identified in this

investigation as having received proceeds of the fraudulent cryptocurrency investment scheme.

36. The following wire deposits were made into Target Account 2 and are a small sampling of the total deposits into Target Account 2:

DATE	VICTIM	AMOUNT
9/28/2023	M.G.F.	$20,000.00
10/2/2023	S.S.J.	$125,000.00
10/3/2023	P.K.N.	$35,572.97
10/3/2023	J.J.B.	$10,000.00
10/3/2023	J.J.B.	$5,000.00
10/6/2023	U.S.C.	$73,000.00
10/6/2023	A.V.V.	$20,000.00
10/13/2023	E.A.S.	$60,000.00
10/13/2023	D.W.R. Jr.	$22,896.29
10/16/2023	R.N.	$145,000.00
10/16/2023	R.J.T.	$45,000.00
10/24/2023	M.A.D.	$50,600.00
10/24/2023	R.N.	$22,000.00
10/26/2023	I.L.	$1,200.00
10/26/2023	I.L.	$1,000.00

INTERVIEWS OF VICTIMS WHO SENT FUNDS TO TARGET ACCOUNT 2

37. In addition to victim A.V.V., USSS investigators interviewed the following victims who sent funds to Target Account 2 as part of their involvement in a fraudulent cryptocurrency investment scheme.

Victim J.J.B.

38. USSS investigators identified and interviewed victim J.J.B. regarding the $15,000.00 he sent to Target Account 2. J.J.B. stated he was utilizing a dating website, seeking.com, and met an individual using the moniker “seductive actress.” J.J.B. stated

the conversation was quickly moved to WhatsApp where he communicated with "Alice Smith" at number 646.389.3813. J.J.B. claimed Smith introduced him to a platform referred to as Meta Trader 5, that was represented by Smith to be a platform that invested in currency trading. According to J.J.B., Smith claimed her uncle in Switzerland was very successful with buying and selling currency and relied on timing of the transactions to earn significant returns.

39. J.J.B. stated Smith enticed him to invest funds into Meta Trading 5 by sending wire transactions to Target Account 2. J.J.B. stated he sent wire transactions of $10,000 and $5,000 to this account on or about October 2, 2023. J.J.B. stated the business address he was provided was 24700 Sylvan Glen Road, Diamond Bar, California. A review of the bank records pertaining to Target Account 2 confirmed these deposits.

Victim M.C.

40. USSS investigators interviewed victim M.C. regarding his involvement in a cryptocurrency investment fraud scheme. M.C. stated he resides within the Eastern District of Texas. M.C. stated he viewed a Tiktok video on July 24, 2023, entitled "BTC investor club 920." M.C. stated he enrolled in the class that claimed to teach investors how to trade in BTC contracts. M.C. stated the investment was initiated with $500 and $1,000 credits to his investment account that grew rapidly in 30 days. M.C. stated he was enticed to invest more funds as a result of the performance of the $1,500 that was initially

invested. M.C. stated he was able to withdraw $100 from his account and received the $100 via his Coinbase account.

41. Based on my training and experience conducting fraud investigations, fraudsters controlling these domains and can manipulate the data in the domain, to include the "account balance" and make it appear as if there was a deposit or gain in the victim's "account."

42. M.C. stated as part of this fraud scheme, he sent funds to entities familiar to this investigation at their respective bank accounts, to include $10,000 to a Citibank account held in the name of Sunny Pacific LLC.

43. USSS investigators have identified several shell companies that receive funds as part of this fraud scheme. It is common practice for the owners of the shell companies to establish bank accounts at several financial institutions as part of their ability to accept funds in multiple bank accounts to avert detection by law enforcement officers and bank investigators.

44. USSS investigators reviewed IC3 and other victim reports submitted by individuals who sent funds to Target Account 2 as part of the fraudulent cryptocurrency investment scheme. The individuals reported to IC3 similar circumstances as other victims that sent funds to Target Account 2. The reports were dated from on or about October 10, 2023, to November 2, 2023, and indicate that 3 separate individuals sent funds to Target Account 2 totaling approximately $22,200. These transactions were

verified by USSS investigators by reviewing the bank records pertaining to Target Account 2.

TARGET ACCOUNT TRANSACTION ACTIVITY FOR ALL TARGET ACCOUNTS

45. Investigators obtained bank records regarding Target Account 1 and discovered that between July 7, 2023, and September 21, 2023, the withdrawal activity included bank fees, other/cash withdrawals and several outgoing wire/Zelle transactions. The other/cash withdrawals totaled approximately $84,474.00. The wire/Zelle transactions totaled approximately $9,777,628.60. These wire transactions were sent to financial institutions in China and other shell companies of record with this investigation as receiving proceeds of this fraud scheme.

46. Investigators obtained bank records regarding Target Account 2 and discovered that between October 2, 2023, and October 31, 2023, there were cash withdrawals totaling $89,800. During this time frame, there were also electronic/wire withdrawals totaling $1,289,310.83. These electronic withdrawals were sent to parties of record with this investigation, to include those located in Hong Kong and other entities located domestically.

CONCLUSION

47. I submit that this affidavit supports probable cause for a warrant to forfeit all funds, monies, and other things of value up to $367,026.14 seized from JPMC Bank accounts:

a. $237,426.83 in JP Morgan Chase (JPMC) Bank account XXXXX1823 (Target Account 1); and

b. $129,599.31 in JPMC Bank account XXXXX9738 (Target Account 2).

48. Based on my experience and the information herein, I have probable cause to believe that the seized $367,026.14 constitutes proceeds from a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)), are traceable to a money laundering transaction and are therefore subject to forfeiture pursuant to pursuant to 18 U.S.C. § 981(a)(1)(A).

49. I also have probable cause to believe that the seized $367,026.14 constitutes proceeds traceable to a violation of 18 U.S.C. § 1343 and/or 18 U.S.C. § 1349, and are therefore is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

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

bschley Digitally signed by bschley Date: 2025.04.02 13:29:01 -05'00'

Brad Schley, Special Agent
U.S. Secret Service