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

UNITED STATES OF AMERICA Plaintiff,	§ § §	
v.	§ §	NO: 6:24-CV-00138
$79,685.00 IN UNITED STATES CURRENCY Defendant.	§ § §	

AFFIDAVIT IN SUPPORT OF COMPLAINT FOR FORFEITURE

I, Daniel Leung, after being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the United States Secret Service (USSS) and have been so employed since March 2022. 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 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 $79,685.00 in Bank of America account 325183691341 (**TARGET ACCOUNT**), Check No. 7840021219 seized on or about January 18, 2024 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 United States-based victims, including victims located in Tyler, Texas, which is 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 "pig butchering" (derived from the Chinese phrase, which is used to describe this 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 any 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.

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 a conspiracy to commit such 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 pig butchering scheme involving a fraudulent cryptocurrency investment 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. Victims of this pig butchering scheme report that upon their attempts to contact the "customer service" of the various cryptocurrency investment platforms, they are informed that in order to withdraw their funds they need to pay a tax of up to 35% on the amount to be withdrawn. It is at this point that most victims become aware that they have been victimized. Case -5814 has resulted in Seizure Warrants (6:23MJ235), (6:23MJ245), (6:23MJ259), and (6:23MJ270) being issued by the Court. During the investigation of this scheme, a victim, GC, provided information that he was directed to submit funds to Halycon, Inc. at its CTBC Bank account ending in 9255. Funds from account ending in 9255 were submitted to the **TARGET ACCOUNT**. Thereafter, law enforcement opened an investigation into Noble Trade USA Enterprises and determined the following.

TARGET ACCOUNT INFORMATION AND TRANSACTIONS

16. First, investigators found information that Noble Trade USA Enterprises (NTE) is based in California. Specifically, a query through the California Secretary of State website revealed that NTE was registered on April 17, 2023, with Chi-Mao Chiang

as the listed agent. The incorporation documents available on the website listed a business address of 9650 Telstar Ave, Unit A 262, El Monte, California 91731.

17. Second, investigators could not find any evidence of legitimate business activity by NTE. Specifically, a public domain Internet search for the name of NTE did not reveal any website or information that would generally be available for a legitimate business. Further, your Affiant determined that the 9650 Telstar Ave Unit A address listed with the California Secretary of State is the address for Onboard Coworking. Onboard Coworking is a company that provides shared workspace and mail/package service to its members.

18. Investigators obtained the bank records for the **TARGET ACCOUNT**. The **TARGET ACCOUNT** was opened on June 1, 2023, with a $100 deposit by Chi-Mao Chiang. There was zero account activity for June and July. Activity for the **TARGET ACCOUNT** began in August. Between August 1 and October 18, the **TARGET ACCOUNT** received 7 wire deposits totaling $330,900 as follows:

DATE	AMOUNT	SENDING ACCOUNT NAME	SENDING ACCOUNT NUMBER
8/24/2023	$51,800.00	Yamatian LTD	Ending in 6145
9/7/2023	$30,000.00	Tick Mill, Inc.	Ending in 1390
9/20/2023	$30,500.00	Keystone Tech, Inc.	Ending in 4949
9/21/2023	$20,000.00	Halycon, Inc.	Ending in 9255
10/6/2023	$20,600.00	Beta Expert Enterprises, Inc.	Ending in 5032
10/17/2023	$128,000.00	Integra Trade USA, Inc.	Ending in 0323
10/18/2023	$50,000.00	Asset Board Enterprises US	Ending in 8566

All credits and deposits were whole dollar figures which is unusual for a legitimate business. Additionally, there were no identifiable normal business transactions such as

payroll, utilities, or other operational expenses in the **TARGET ACCOUNT**. According to Bank of America, the remaining account balance is $79,685.00. A $3,000.00 wire transfer was sent from the **TARGET ACCOUNT** to JPMC bank account ending in 0323 in the name of Integra Trade USA, Inc. on September 13, 2023. As detailed later in this affidavit, investigators have identified and interviewed one fraud victim associated with the 0323 account. Furthermore, a $3,000.00 wire transfer was sent from the **TARGET ACCOUNT** account to JPMC bank account ending in 2832 in the name of Juniper Trade Group on August 30, 2023, and a $3,000.00 wire transfer was sent from the **TARGET ACCOUNT** to JPMC bank account ending in 0260 in the name of Hyperion Trade USA Inc on September 15, 2023. Documents available on the California Secretary of State website indicate a business address of 9650 Telstar Ave, Unit A 269, El Monte, California for Juniper Trade Group and a business address of 9650 Telstar Ave, Unit A 266, El Monte, California for Hyperion Trade USA Inc. The address on Telstar Ave is the same physical address as the address for Noble Trade USA Enterprises.

INTERVIEWS OF FUNDING OF THE TARGET ACCOUNT

Follow-up investigation of Halycon, Inc., which funded the TARGET ACCOUNT

19. First, investigators found information that Halycon, Inc. is based in California. Specifically, a query through the California Secretary of State website revealed that Halycon was registered on April 13, 2023, with Chang-Chi Wu as the listed agent. The documents available on the website listed a business address of 9650 Telstar

Ave, Unit A 263, El Monte, California 91731. This is the same physical address as Noble Trade USA Enterprises.

20. One account for Halycon, Inc. has been identified. The account was held at CTBC Bank. Per representatives of CTBC Bank this account was closed due to suspicious activity and no funds remain.

Interviews of Fraud Victims

21. To date, agents with the USSS have been able to identify and telephonically interview two victims tied to the Halycon, Inc. CTBC Bank account ending in 9255. These victims deposited $364,000.00 into the Halycon, Inc. account. Both those interviewed stated they were victims of fraud.

22. For example, investigators contacted an individual victim identified herein as GC of Honolulu, HI. GC confirmed he was involved with investments in cryptocurrency. GC confirmed a financial transaction to Elights Trading (the target of Seizure Warrant 6:23MJ235) and identified its purpose as to pay taxes on his earnings from his investment in cryptocurrency. GC stated that despite paying his "taxes" he remains unable to withdraw any funds from his "cryptocurrency account." GC provided information regarding communications he had with unknown subjects who purported to operate a customer service platform for Zaif CS, a cryptocurrency exchange. These communications reflect non-standard business practices, specifically, a two-hour time limit for a bank account to be available in order to receive funds. GC stated he has suffered a loss of approximately $240,000 as a result of this scheme. GC provided

documentation for two wire transfers; one of the wires was submitted on September 6, 2023, to CTBC bank account ending in 9255 held in the name of Halycon, Inc. for $100,000.

23. Additionally, investigators contacted an individual victim identified herein as "AE" of Cincinnati, Ohio, regarding financial transactions made to Halycon, Inc.'s account held at CTBC Bank. AE confirmed he was involved with investments in cryptocurrency. AE stated that he was initially contacted by a stranger through WhatsApp around February 2023. Through conversations over a period of approximately four months, this individual, along with another individual who claimed to be the first individual's uncle, convinced AE to begin investing in cryptocurrency through a purported Australian cryptocurrency platform named "TMGM". AE stated that he has been unable to withdraw any funds that he invested, and that he has suffered a loss of approximately $4,000,000 as a result of this scheme. AE provided documentation for 12 wire transfers he submitted for the purpose of investments related to this scheme, including one $264,000.00 wire submitted on September 12, 2023, to CTBC bank account ending in 9255 held in the name of Halycon, Inc.

Follow-up investigation of Keystone Tech, Inc., which funded the TARGET ACCOUNT

24. First, investigators found information that Keystone Tech, Inc. is based in New York. Specifically, a query through the New York Secretary of State website revealed that Keystone Tech, Inc. was registered on April 20, 2023. No agent was listed

on the New York Secretary of State website for Keystone Tech, Inc. The documents available on the website listed a business address of 139 Centre St., Ste. 304, New York, New York 10013.

25. Multiple accounts for Keystone Tech, Inc. have been identified. An account held at Cathay[1] Bank was closed by its fraud department due to suspicious activity. This activity included more than $1 million in incoming wire transfers within thirty-five days. Bank of America also confirmed suspicious activity had occurred in an account owned by Keystone Tech. The activity involved the rapid transfer of funds into and out of the account via wire transfers. The Bank of America fraud department indicated the account was closed.

Interviews of Fraud Victims

26. To date, agents with the USSS have been able to identify and telephonically interview 7 victims tied to the Keystone Tech, Inc.'s Bank of America account ending in 4949. These victims deposited $315,500 into the Keystone Tech account. All those interviewed stated they were victims of fraud.

27. For example, investigators contacted an individual victim identified herein as "AP" of Clarksville, Tennessee, regarding financial transactions made to Keystone Tech's account held at Bank of America. AP reported receiving a random text late this summer from someone he knows only as Yexin. AP said they communicate through

[1] Cathay Bank is a financial institution headquartered in Charlotte, North Carolina, within the Western District of North Carolina.

WhatsApp via text and have never met or video chatted. AP stated they spoke about crypto investments, particularly short-term trading of two-way contracts. AP stated after some research he did believe it was a way to make good profits. AP stated his initial investment was small, and he was able to make a withdrawal after the investment grew. After everything worked as expected, AP made two additional investments. AP stated he recently tried to make a withdrawal but was informed his account was flagged as high-risk potential for involvement in money laundering, so a pre-payment of taxes was required. AP stated he was informed he needed to pay approximately 30 percent of his investment in taxes. AP suspected he was a victim of fraud after learning he could not retrieve his funds. AP stated the website he used to see his investment was UBIITL.COM. AP provided documents regarding his wire transfers, primarily to banks in China. One of the wires was a $100,000.00 wire transfer submitted on September 14, 2023, to Bank of America account ending in 4949 held in the name of Keystone Tech, Inc. Based on the provided documents AP's total loss is $305,794.00.

28. Additionally, investigators contacted an individual victim identified herein as "MM" of Dahlonega, GA, regarding financial transactions made to Keystone Tech's Bank of America account. MM reported that earlier this year, he was contacted through LinkedIn by a stranger using the name Emily Miller. MM stated that after initial conversations on LinkedIn, he primarily communicated with Miller through Telegram. MM stated that Miller discussed cryptocurrency trading with him and introduced him to a cryptocurrency platform named Star Funds. MM began investing funds into this platform

and realized significant returns on his investments. In October this year, MM attempted to withdraw funds from his Star Funds account, but a Star Funds customer service representative informed him that he would need to pay a 25% tax on his profits to withdraw his funds. The Star Funds representative informed MM that this payment could not be deducted from existing funds in his account. After considering paying this tax, MM ultimately decided that he would not pay Star Funds any additional fees. The Star Funds customer service representative continued to attempt to convince MM to pay the tax and threatened to involve the Australian Securities and Investments Commission (ASIC). MM provided documents regarding his wire transfers and communication with Star Funds, including a $20,000.00 wire transfer submitted on September 15, 2023, to Bank of America account ending in 4949 held in the name of Keystone Tech, Inc.

29. Furthermore, investigators contacted an individual victim identified herein as "DK" of Lehi, Utah, regarding financial transactions made to Keystone Tech's account held at Bank of America. DK reported that in August this year, he received a text from an individual known to him only as Maggie. DK stated that Maggie mentioned that she was a day trader in cryptocurrency, and she described a formula she used to ensure a profitable gain for every investment. The website of the exchange she was using is https://ausfits.com/mobile/index.html. Maggie later convinced DK to observe her investing several thousand dollars and realizing a return of 30% in a 30 second trading node. She also promised DK that if he followed her advice, she could ensure him profitable trades because she would reimburse him for any losses he might incur. DK

decided to begin with a $1,000.00 investment, which led to a successful trade. This happened several more times over the next two months.

30. At one time, DK realized a $10,000 investment loss, but Maggie did as she had promised, and deposited $10,000 into his Ausfits exchange account. DK's continued investments totaled over $104,000. When DK decided to cash out the account, he was told by the Exchange that he needed to pay 10% in a tax on profits before he could withdraw any of the funds. The exchange informed him that he could not use any of the funds in his exchange account to pay this tax, and that it had to come from a wire transfer as new funds. DK paid this tax, but the exchange representative allegedly misapplied the funds and directed them to the investment account, and not the tax account. The exchange claimed they could not transfer these funds and that he needed to pay the tax amount again. Maggie informed DK she would pay the second tax payment for him if he paid her back. DK applied for an extension, which cost $2,000 in extension fees. At this point, Maggie claimed that she was unable to pay the tax payment. DK provided documentation for a $60,000.00 wire transfer submitted on September 15, 2023, to Bank of America account ending in 4949 held in the name of Keystone Tech, Inc.

Follow-up investigation of Integra Trade USA, Inc., which funded the TARGET ACCOUNT

31. First, investigators found information that Integra Trade USA, Inc. (Integra Trade) is based in California. Specifically, a query through the California Secretary of State website revealed that Integra Trade was registered on April 13, 2023, with Chia-

Chen Liu as the listed agent. The incorporation documents available on the website listed a business address of 9650 Telstar Ave, Unit A 265, El Monte, California 91731. This is the same physical address as Noble Trade USA Enterprises.

32. One account for Integra Trade USA, Inc. has been identified. The account is held at JPMorgan Chase Bank.

Interviews of Fraud Victims

33. To date, investigators have been able to identify and telephonically interview one victim tied to the Integra Trade JPMorgan Chase Bank account ending in 0323. This victim deposited $190,000 into the Integra Trade account. The interviewee stated he was a victim of fraud.

34. Investigators contacted an individual victim identified herein as "RG" of Cincinnati, Ohio, regarding financial transactions made to Keystone Tech's account held at Cathay Bank. RG said he was approached through social media and began a friendship with a man he believes is named Jack Davis. He believes Jack Davis is in Charlotte, North Carolina. RG stated they communicate through WhatsApp and Davis guided him into crypto currency investments. RG believed his funds were submitted to a Crypto.com account then transferred into a crypto mining company, Exmar Tech. RG indicated the investment has grown substantially. RG stated when he first began investing, he started with a small sum and afterwards conducted a withdrawal for about $1,000. Establishing the legitimacy of the investment he then made substantial deposits. RG provided documentation for eight wires totaling $601,060.00. One of the wire transfers was a

$190,000.00 wire submitted on October 11, 2023, to JPMorgan Chase account ending in 0323 held in the name of Integra Trade USA.

SEIZURE OF FUNDS IN THE TARGET ACCOUNT

35. Based on my training and experience, the movement of funds reflected in the transaction history of the **TARGET ACCOUNT** points to money laundering activity that is common in these fraud schemes.

36. On or about October 24, 2023, investigators provided a freeze letter request to Bank of America for assets and monies in the **TARGET ACCOUNT** to be frozen. Bank of America employees informed investigators that the **TARGET ACCOUNT's** balance is approximately $79,685.00.

37. On or about January 18, 2024, USSS investigators obtained and served a federal seizure warrant for any and all funds up to $79,685.00 held in the **TARGET ACCOUNT.**

38. On or about January 30, 2024, USSS investigators received a Bank of America cashier's check bearing number 7840021219 that was drawn on the **TARGET ACCOUNT** in the amount of $79,685.00.

CONCLUSION

39. I submit that this affidavit supports probable cause for a warrant to forfeit all funds, monies, and other things of value up to $79,685.00 seized from Bank of America account 325183691341 in the name of NOBLE TRADE USA ENTERPRISES.

40. Based on my experience and the information herein, I have probable cause to believe that the seized $79,685.00 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 18 U.S.C. § 981(a)(1)(A).

41. The seized property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) because it is personal property involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 and 1957, or any property traceable to such property, and pursuant to 18 U.S.C. § 981(a)(1)(C) because it is personal property which constitutes or is derived from proceeds traceable to a violation of any offense constituting a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7)), namely, a violation of 18 U.S.C. § 1343, or a conspiracy to commit such offense (18 U.S.C. § 1349).

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

DANIEL P LEUNG Digitally signed by DANIEL P LEUNG
Date: 2024.04.12 19:02:38 -05'00'

Daniel Leung, Special Agent
U.S. Secret Service