United States District Court

CENTRAL **DISTRICT OF** **CALIFORNIA**

In the Matter of the Seizure of
(Address or Brief description of property or premises to be seized)

Up to $589,625.00 on deposit in Bank of America account 325181151715, up to $56,600.00 on deposit in Bank of America account 325181151896 and up to $119,600.00 on deposit in Bank of America account 325181152031

APPLICATION AND AFFIDAVIT FOR SEIZURE WARRANT

CASE NUMBER: 2:24-MJ-5130

I, Fred D. Apodaca, being duly sworn depose and say:

I am a Special Agent with the United States Secret Service, and have reason to believe that

in the CENTRAL District of CALIFORNIA
there is now concealed a certain person or property, namely (describe the person or property to be seized)

Up to $589,625.00 on deposit in Bank of America account 325181151715, up to $56,600.00 on deposit in Bank of America account 325181151896 and up to $119,600.00 on deposit in Bank of America account 325181152031

which is (state one or more bases for seizure under United States Code)

subject to seizure and forfeiture under 18 U.S.C. §§ 981(a)(1) (C), (b)(2), 982(b), 984 and 21 U.S.C. §§ 853(e) and 853(f)

concerning a violation of Title 18 United States Code, Section(s) 1343.

The facts to support a finding of Probable Cause for issuance of a Seizure Warrant are as follows:

Continued on the attached sheet and made a part hereof. X **Yes** _ **No**

S.A. Fred D. Apodaca
Attested to by the applicant in accordance with the Requirements of Fed. R. Crim. P. 4.1 by telephone

Sworn before me in accordance with requirements of Fed. R. Crim. P. 4.1 by telephone

Date

Los Angeles, California
City and State

Hon. Pedro V. Castillo, U.S. Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

AUSA Ryan Waters;ga

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEIZURE WARRANT

I, Fred D. Apodaca, being duly sworn, hereby depose and state as follows:

I.

INTRODUCTION

1. I am a Special Agent with the United States Secret Service ("USSS") assigned to the Los Angeles Field Office Asset Forfeiture Squad. I have been employed by the USSS since December 2008. In this capacity, I am responsible for investigating violations of federal criminal law, particularly those laws found in Title 18 of the United States Code and relating to financial institution fraud, credit card fraud, identity theft, and stolen U.S. Treasury Checks. I have received formal training at the Federal Law Enforcement Training Center and the USSS James J. Rowley Training Center. My training includes, but is not limited to, various investigative techniques and tactics regarding financial crimes, including credit card fraud, identity theft, illegal methods used to obtain credit cards, bank loans, and other lines of credit, and methods used to launder and conceal the proceeds. Prior to my employment with the U.S. Secret Service, I was employed for four years as a Financial Analyst with the Federal Bureau of Investigation.

2. Unless stated otherwise, I have personal knowledge of the matters set out in this affidavit. To the extent that any information in this affidavit is not within my personal knowledge, it was made known to me through reliable law enforcement sources, and I believe it to be true.

3. The facts set forth in this affidavit are based upon my own personal observations, my training and experience, and information obtained during this investigation from other sources, including: (a) statements made or reported, directly or indirectly, by various witnesses with personal knowledge of relevant facts, including other law enforcement officers; (b) records obtained during the course of this investigation; and (c) interviews conducted by other USSS special agents.

4. This affidavit is intended to show that there is sufficient probable cause for the requested seizure warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only. All figures, times, and calculations set forth herein are approximate.

II.

PURPOSE OF AFFIDAVIT

5. This affidavit is offered in support of applications for warrants to seize:

a. Up to $500,480.00 (the "Subject Funds 1") on deposit in East West Bank account 8861000548 ("Subject Account 1"), held in the name of Valencia Global Limited;

b. Up to $589,625.00 (the "Subject Funds 2") on deposit in Bank of America account 325181151715 ("Subject Account 2"), held in the name of Galaxy Trading Limited;

c. Up to $56,600.00 (the "Subject Funds 3") on deposit in Bank of America account 325181151896 ("Subject Account 3"), held in the name of Nebula Trading Limited; and

d. Up to $119,600.00 (the "Subject Funds 4" and, together with Subject Funds 1 and 2, and 3 collectively referred to herein as the "Subject Funds") on deposit in Bank of America account 325181152031 ("Subject Account 4" and, together with Subject Accounts 1 and 2, and 3, collectively referred to herein as the "Subject Accounts"), held in the name of Zenith Trading Limited.

6. Based on the facts set forth below, there is probable cause to believe that the Subject Funds represent proceeds or are involved in violations of 18 U.S.C. § 1343 (Wire Fraud), which constitutes "specified unlawful activity" pursuant to 18

U.S.C. §§ 1956(c)(7)(A) and 1961(1)(B). Specifically, there is probable cause to believe that the Subject Funds are proceeds of confidence frauds[1] and social engineering scams[2], perpetrated against numerous victims. Therefore, the Subject Funds are subject to seizure pursuant to 18 U.S.C. § 981(b)(2) and forfeiture pursuant to 18 U.S.C. § 981 (a)(1)(C).

7. In addition, there is probable cause to believe that the Subject Funds are subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 982(b) and 21 U.S.C. § 853(f) because the funds would, in the event of conviction on the alleged underlying offenses, be subject to forfeiture, and an order under section 21 U.S.C. § 853(e) would not be sufficient to assure the availability of the property for forfeiture.

8. To the extent that the Subject Funds are not the actual monies traceable to or involved in the illegal activities

---

[1] According to Blackstone's Criminal Practice, confidence frauds involve a victim transferring money and/or property as a result of being deceived or misled by the offender.

[2] Social engineering is a method used to manipulate victims into performing certain actions or providing confidential information. When successfully executed, social engineering techniques can cause a victim to send money to someone whom he or she met on a dating website or to provide confidential information such as his or her personal identifiable information and bank account information. Additionally, victims sometimes serve as money mules, individuals recruited to receive and transfer money acquired from criminal activities on behalf of criminals and money launderers.

identified herein, the government alleges that these funds are identical property found in the same account as the property traceable to or involved in the illegal activities, rendering these funds subject to forfeiture pursuant to 18 U.S.C. § 984 (forfeiture of fungible property).

III.

SUMMARY OF PROBABLE CAUSE

9. The USSS has interviewed multiple victims of confidence frauds who transferred funds based on fraudulent pretenses directly into Subject Accounts 2, 3, and 4 and a Bank of America account ending in 0637 (the "X0637 Account"). These accounts were first identified as suspicious in April 2024, after a Bank of America investigator flagged suspicious activity in the accounts, with multiple large deposits within a short time and attempted same day or next day withdrawals. Given the suspicious activity on the account, Bank of America contacted USSS for further investigation. Investigation revealed that funds from the X0637 Account were ultimately transferred to Subject Account 1.

IV.

STATEMENT OF PROBABLE CAUSE

HISTORY OF SUBJECT ACCOUNTS

10. On or about July 30, 2024, Subject Account 1 was opened in the name of Valencia Global Limited, with an

identified address in Brooklyn, NY, and Mai-Ke Lin("Lin"), identified as the only authorized signer. According to New York Secretary of State records, Valencia Global Limited is a New York Corporation registered in July 2024 with a principal address in Brooklyn, NY. Lin, the Subject Account 1 authorized signer, is listed as the Registered Agent.

11. On or about January 18, 2024, Subject Account 2 was opened in the name of Galaxy Trading Limited, with an identified address in Arcadia, CA 91007 ("Arcadia Address 1"), and Mei-Ying Kuo ("Kuo") identified as the authorized signer. According to California Secretary of State records, Galaxy Trading Limited is a California Corporation registered in December 2023 with a principal address in Arcadia, CA ("Arcadia Address 2"). Kuo, the Subject Account 2 authorized signer, is listed as the Registered Agent.

12. On or about January 16, 2024, Subject Account 3 was opened in the name of Nebula Trading Limited, with an identified address at Arcadia Address 1, and Kuo identified as the only authorized signer. According to California Secretary of State records, Nebula Trading Limited is a California Corporation registered in December 2023 with a principal address at Arcadia Address 2. Kuo, the Subject Account 3 authorized signer, is listed as the Registered Agent.

13. On or about January 18, 2024, Subject Account 4 was opened in the name of Zenith Trading limited, with an identified address at Arcadia Address 1, and Kuo identified as the only authorized signer. According to California Secretary of State records, Zenith Trading Limited is a California Corporation registered in December 2023 with a principal address at Arcadia Address 2. Kuo, the Subject Account 4 authorized signer, is listed as the Registered Agent.

14. Subject Accounts 2, 3, and 4 all share Kuo as the authorized signer and use Arcadia Address 1 as the account address.

15. The X0637 Account, like Subject Account 1, was held in the name of Valencia Global Limited. Funds from the X0637 Account ultimately were transferred to Subject Account 1.

CONFIDENCE AND ROMANCE SCAM VICTIMS

16. As described in further detail below, fraud victims interviewed by the USSS have related similar stories about having been lured into online communication regarding crypto currency investment with people whom they had never met in person. The victims were then induced to transfer funds to a bank account for the purpose of investing in crypto currency, except the account is controlled by criminals.

17. **Victim B.R.:** In July 2024, I spoke to B.R. of Flower Mound, TX regarding a $360,000.00 wire transfer sent on March

25, 2024, to the X0637 Account. B.R. learned through the WhatsApp communication platform about an online cryptocurrency trading education seminar. The organization is called EIF (Excellence & Innovation Fortune) Business School. B.R. was contacted by a school administrator who said her name was Evelyn Smith and encouraged B.R. to join the seminar. The online seminar started out by illustrating how to trade normal stocks on the regular stock exchanges. The next avenue of making money taught at the seminar was learning how to trade digital coins on the ICH Coin website, www.Ichcoin.net. B.R.'s account was purportedly provided a free deposit of $500.00, which he was told was free to trade at his own discretion and could keep any profit.

18. After purportedly earning a profit on the $500.00 ICH Coin investment he was given, B.R. decided to invest some of his own funds. An EIF customer representative requested an initial $5,000.00 deposit into the account. B.R. was then told about several "VIP Groups" that he could join: "VIP 1" group was a $50,000.00 minimum investment; "VIP 2" group was a $300,000.00 minimum investment; and "VIP 3" group was a minimum $1.5 million investment.

19. B.R. was contacted by a person going by the name Elizabeth, who B.R. now believes was working as part of the fraud scam with EIF. Elizabeth contacted B.R. via WhatsApp and

encouraged him to join a VIP Group and would send B.R. trading advice and convinced B.R. that these investments were in legitimate companies. Elizabeth told B.R. he would be able to withdraw funds without any issues at any time and she showed B.R. the profits she was earning by investing. Elizabeth told B.R. that all his trades would be profitable and encouraged him to keep his principal balance at a large dollar amount so that his returns would yield a sizable investment return.

20. One investor posted a message on the EIF site that showed a $500,000.00 profit, which was a 1000% return on their investment. Other investors on the site would also post their percentage return in the group chat and B.R. was encouraged to invest in the higher VIP Group. Based on the investment returns that R.R. was being shown by other investors, B.R. decided to invest and made the following wire transfer investments to his Ichcoin.net account: 1) On February 28, 2024, $5,000.00 wire to Meridian International Sourcing Group, Green Dot Bank, account ending in 0016; 2) On March 6, 2024, $50,000.00 wire to Saludent Limited, Bank of America, account ending in 1270; 3) From March 7, 2024 to March 25, 2024, three wire transfers totaling $250,000.00 sent to Cypress Valley Trading USA Inc., Chase Bank, account ending in 2812; 4) On March 25, 2024, $360,000.00 wire to Subject Account 2; and 5) From April 23, 2024 to May 7, 2024, two wire transfers totaling $176,000.00 sent to Henca Trade

Limited, Bank of Communication, Hong Kong, account ending in 9901.

21. In April 2024, B.R. was told his Ichcoin.net account would be funded with a $100,000.00 loan, which B.R. never requested. B.R. does not know if the funds were ever credited to his account. In April 2024, B.R. checked his account balance and learned that his account balance was now purportedly worth $13 million. At this time B.R. requested through the Ichcoin.net website a withdrawal of some of his account balance funds. B.R. was told that prior to him withdrawing funds he must pay back the $100,000.00 loan. B.R. agreed and wire transferred funds to pay back the loan. A second withdrawal request was then made by B.R., and this time he was told he must join the investment group called the "Green Channel Investment," which required a $150,000.00 investment. B.R. agreed and once again wire transferred funds to cover the $150,000.00 required investment. A third request was made by B.R. for a fund withdrawal, and he was now told he must now send $130,000.00 to cover income taxes. Now realizing that he was a victim of fraud, B.R. did not send any additional funds and contacted his bank to recall some of the wire transfers he sent. Bank of America did return to his bank account the $360,000.00 wire he sent to X0637 Account in March 2024.

22. Based on my training and experience, I believe B.R. is a victim of a romance and confidence scam and the $360,000.00 wire transferred to the X0637 Account on March 25, 2024, and ultimately transferred to Subject Account 1, represented fraudulent proceeds of such a scam. Because the $360,000.00 transferred to X0637 was ultimately recalled, the Government is not including that $360,000.00 in the proceeds tracing calculation. However, the transfer serves as evidence of the fraud scheme and fraud proceeds originally being directed to an account with Kuo as the authorized signer.

23. **Victim W.P.:** In May 2024, I spoke to W.P. of Milwaukee, WI regarding a March 14, 2024, $100,000.00 wire transfer to Subject Account 4. In December 2023, W.P. was on his Facebook account where he learned about an online group where you could obtain tips and techniques about trading in crypto currency. At first, W.P. was skeptical about investing in crypto currency but was interested in learning about the investment possibilities. From messages he was reading in his Facebook group chat, he learned that many of the individuals who invested were reporting they had earned significant investment returns. By March 2024, W.P. felt comfortable to trade crypto currency and learned about a trading platform website called ICHcoin.net.

24. For his first investment, W.P borrowed from his 401K account, and wired $100,000.00 to Subject Account 4. W.P. would communicate with a customer service representative of ICH Coin via What's App or Telegram Messenger. W.P. sent another wire transfer for $400,000.00 to a bank in Australia. During the month of April 2024, W.P. checked his balance and it showed a purported value of $1.3 million. In total, W.P. sent approximately $700,000.00 in wire transfers to fund his account.

25. A week after sending the $400,000.00 wire transfer to the bank in Australia, an ICH Coin representative told him that the $400,000.00 wire was never received and as a result his account would remain frozen until the funds were received. W.P. checked with his bank multiple times to verify the funds were sent and received, and his bank confirmed receipt by the other bank in Australia. W.P. attempted to withdraw some of his funds from his purported account balance of $1.3 million, but the customer service representative he spoke to insisted he must first pay the $400,000.00 that ICH Coin claimed was never received by the bank in Australia. W.P. was told that that if he sends $250,000.00, ICH Coin would cover the remaining $150,000.00 to equal the $400,000.00. At this point W.P had invested his entire retirement savings and was unable to send additional funds; and began to realize that he was a victim of fraud and may never have his funds returned.

26. W.P. contacted his bank to recall some of the wire transfers he sent. Bank of America returned funds to him for the $100,000.00 wire transfer sent to Subject Account 4 in March 2024.

27. Based on my training and experience, I believe W.P. is a victim of a romance and confidence scam and the $100,000.00 wire transferred to Subject Account 4, on March 14, 2024, represents fraudulent proceeds of such a scam. Because the $100,000.00 transferred to Subject Account 4 was ultimately recalled, the Government is not including that $100,000.00 in the proceeds tracing calculation. However, the transfer serves as evidence of the fraud scheme and fraud proceeds being directed to an account with Kuo as the authorized signer.

28. **Victim R.M.:** In May 2024, I spoke to victim R.M. of Westerville, OH regarding a $100,000.00 wire transfer sent on March 13, 2024, to Subject Account 4. In January 2024, R.M. was on Facebook when he saw an advertisement for the purported crypto currency school called EIF Business School started by an individual named Linden Quatros ("Quatros"). R.M. was interested in learning about crypto currency and went to the website for EIF Business school. R.M. learned that the founder of EIF Business School, Quatros, was claiming to be using artificial intelligence software that would provide him special insights on when to buy and sell crypto currency for significant investment

returns. Quatros sent out text messages via internet communication application WhatsApp to all the people inviting them to participate in a statistical test to validate if his artificial intelligence software could predict prices of crypto currency. Quatros, told all the participants they he would purportedly put $500.00 in each person's account, and if the software made money, they could keep the profit. If the money was lost, they would not be responsible to repay the funds. To participate, R.M. was told to download from the app store an app called ICHcointradingcenter.com.

29. Approximately one week after his $500.00 was put into his account, his account balance and those of the other participants purportedly showed a significant investment return. Seeing the potential to make significant amount of money investing under this program, R.M. wanted to invest his own funds. R.M. was told about a program where the participants would be broken up into different groups, based on the amount of funds invested. "VIP 1" group was for individuals depositing up to $350,000; "VIP 2" group was for deposits between $350,000 and $1.5 million and "VIP 3" was for investments between $1.5 million and $3.5 million. Participants were told that investments made into VIP 3 would receive the artificial intelligence trading information first, which would result in the greatest investment returns.

30. R.M. decided to invest his own funds and was given banking routing information via the communication application Telegram Messenger. R.M. made the following investments: 1) On February 26, 2024, $8,000.00 wire to Yuan Industries, Bank of America account ending in 9087; 2) On March 4, 2024, $15,000.00 wire to Xcellent Trading Corp, JP Morgan Chase Bank account ending in 6003; 3) On March 6, 2024, $30,000.00 wire to Crypto.com; 4) On March 11, 2024, $53,000.00 wire to Crypto.com; 5) On March 13, 2024, $100,000.00 wire to Subject Account 4; and 6) On April 18, 2024, $50,000.00 wire to Crypto com.

31. R.M. learned about a second opportunity from the ICH Trading Platform that involved an opportunity to invest in tokens. R.M. was told that the tokens being issued were currently over-subscribed, which meant there was a huge demand for these tokens that would result in significant investment returns. R.M. was told the investment minimum to participate is $500,000.00. R.M. only had $100,000.00 to invest and was told the platform would provide him a $400,000.00 loan to make up the difference. R.M was sent via email loan documents, which he signed and returned.

32. A few weeks after obtaining the loan, R.M checked his balance on the ICH Trading Platform and learned he owned 23,000 tokens and his account balance was purportedly worth $48 million. R.M. attempted to withdraw some of his investment

gains, however, was told that he must wire $400,000.00 to pay back the loan or his account would be frozen. R.M. did ask to have the $400,000.00 subtracted from his purported loan balance of $48 million but was told his "account will be frozen until loan is repaid with external funds."

33. R.M. received numerous messages from other purported participants in the trading platform encouraging him to pay back the loan. Many of those other participants were posting photos of homes, cars, and jewelry they had purchased after their loans were paid and were able to withdraw their investment returns. R.M. now feels that these people were most likely involved with the company and were simply trying to get him to send additional funds. R.M. never sent additional funds and now feels he is a victim of fraud. In April 2024, R.M. was surprised to learn that the wire transfer he sent for $100,000.00 to Subject Account 4 was returned to his account. R.M. did not request a recall of the wire and was told by his bank that Bank of America suspected that account of fraud so began to return funds to the originator.

34. Based on my training and experience, I believe R.M. is a victim of a romance and confidence scam and the $100,000.00 wire transferred to Subject Account 4 on March 13, 2024, represents fraudulent proceeds of such a scam. Because the $100,00.00 transferred to Subject Account 4 was ultimately

recalled, the Government is not including that $100,000.00 in the proceeds tracing calculation. However, the transfer serves as evidence of the fraud scheme and fraud proceeds being directed to an account with Kuo as the authorized signer.

35. **Victim R.C.** In May 2024, I spoke to victim R.C. of Lynn, MA regarding a $40,025.00 wire transfer sent on March 13, 2024, to Subject Account 2. In January 2024, R.C. was on the internet application Instagram and was involved in a group chat room that was purportedly associated with Elon Musk, called Excellent Innovation Fortune. The group chat room was promoting a crypto currency trading application named HCH Coin, website address H5.Hchcoin.com. R.C. researched the group and learned the platform guaranteed a return on his investment and would reimburse his losses. In hindsight, R.C. now feels that a guaranteed rate of return and the agreement to cover his losses on trades should have been a red flag for him not to invest funds.

36. In March 2024, R.C. decided to invest funds and sent a $40,025.00 wire transfer to Subject Account 2. All communication between R.C. and Hchcoin website was via the Telegram Messenger application. R.C. did question why he was sending funds to an account titled Galaxy Trading Limited and not Hchcoin. R.C. was told that banks are suspicious of crypto currency trading sites.

37. In April 2024, R.C. checked his account balance on the Hchcoin website and learned his account balance was purportedly now worth $72,000.00. R.C. decided to invest the entire funds on the Hchcoin platform by trading crypto currency options and lost his entire purported balance of $72,000.00. R.C. does not know if his funds were ever invested in legitimate trading options, and his account now showed a zero balance.

38. In May 2024, R.C. was contacted by a customer service representative of Hchcoin via text message and was told about an investment in U.S.D.T coins that would yield significant returns. R.C. decided to invest and wire transferred $8,000.00. A few weeks after his $8,000.00 investment, R.C. checked his balance and learned his account was purportedly worth $17,000.00. R.C. was then encouraged by a customer service representative to invest more funds and that you "can't lose money on this investment." R.C. communicated to the customer service representative that he no longer additional funds to invest. R.C. was then told about a loan program where he could borrow funds. R.C. was emailed loan documents that he signed for a loan of $300,000.00, that was purportedly deposited into his account. A few weeks after the loan was obtained, R.C. checked his account balance and learned it was now purportedly worth approximately $13 million. R.C. attempted to withdraw funds from his account but was told he must first pay back the $300,000.00

loan or his account would be frozen. R.C. asked if the funds could be subtracted from his $13 million account balance but was told the $300,000.00 could not be subtracted from his account balance. R.C. did not have any funds to pay back the $300,000.00 loan.

39. R.C. was told by the customer service representative that his employer would be contacted if he could not pay back the loan. Shortly after his last communication with the Hchcoin representative, R.C. was no longer able to access the Hchcoin website or the Telegram Messenger application.

40. Based on my training and experience, I believe R.C. is a victim of a romance and confidence scam and the $40,025.00 wire transferred to Subject Account 2 on March 13, 2024, represents fraudulent proceeds of such a scam.

TRACING FRAUD PROCEEDS INTO THE SUBJECT ACCOUNTS

41. From my review of the Subject Accounts and the X0637 Account bank records, the following fraudulent proceeds described above were deposited into the Subject Accounts and the X0637 Account:

a. On March 25, 2024, a $360,000.00 wire transfer to X0637 Account[3], from victim B.R.;

[3] Because this transfer was successfully recalled, the $360,000.00 is not being included in the final tracing calculation.

b. On March 13, 2024, a $40,025.00 wire transfer to Subject Account 2, from victim R.C.;

c. On March 13, 2024, a $100,000.00 wire transfer to Subject Account 4[4], from victim R.M;

d. On March 14, 2024, a $100,000.00 wire transfer to Subject Account 4[5], from victim W.P.

42. In addition, the USSS has identified additional suspicious deposits into Subject Accounts 2, 3, 4 and the X0637 Account but has been unsuccessful in contacting and interviewing the individuals associated with the deposits/transfers, who I believe to be victims of this scheme. These other potential victims made approximately $1,574,650.00 in suspicious deposits into Subject Accounts 2, 3, 4 and the X0637 Account (the "Additional Deposits"). Of the $1,574,650.00 in Additional Deposits, approximately $503,100.00 was deposited into the X0637 Account, approximately $600,350.00[6] was deposited into Subject Account 2, approximately $56,600.00 was deposited into Subject

[4] Because this transfer was successfully recalled, the $100,000.00 is not being included in the final tracing calculation.

[5] Because this transfer was successfully recalled, the $100,000.00 is not being included in the final tracing calculation.

[6] Because $50,750.00 of this $600,350.00 in Additional Deposits transferred to Subject Account 2 was successfully recalled, only $549,600 of the $600,350.00 is being included in the final tracing calculation.

Account 3, and approximately $414,600.00[7] was deposited into Subject Account 4.

43. The Additional Deposits into the Subject Accounts share similarities with the above-described fraud victim transfers into Subject Accounts 2, 4 and the X0637 Account, in that they (1) were made in the same time period as the above-described transfers of fraud proceeds; (2) were made from individuals in locations throughout the United States without the kind of geographic patterns which might be expected from a legitimate business; (3) were made from people who had not previously deposited funds into Subject Accounts; and (4) were often made in large round-dollar amounts, which are inconsistent with normal business transfers (which typically reflect taxes and other costs). Also, Subject Accounts 1, 2, 3, 4 and the X0637 Account are controlled by the same individual or entity as evidenced by the fact that (1) Subject Accounts 2, 3, and 4 share Kuo as the authorized signer; (2) Subject Accounts 2, 3, 4 and the X0637 Account use Arcadia Address 1 as the identified account address; (3) Subject Accounts 2, 3, and 4 are held in the name of businesses with state registered addresses using

[7] Because $295,000.00 of this $414,600.00 in Additional Deposits transferred to Subject Account 4 was successfully recalled, only $119,600.00 of the $414,600.00 is being included in the final tracing calculation.

Arcadia Address 2; and (4) the X0637 Account, like Subject Account 1, was held in the name of Valencia Global Limited with funds from the X0637 Account ultimately being transferred to Subject Account 1. Accordingly, and based on my training and experience, I believe the Additional Deposits are also fraud proceeds from victims whose identity the USSS has yet to confirm.

44. As described above, approximately $503,100.00 was sent in Additional Deposits to the X0637 Account. On July 30, 2024, Subject Account 1 received tainted funds from the X0637 Account when a $500,480.00 cashier's check drawn on the X0637 Account was deposited into Subject Account 1, which the government seeks to seize from Subject Account 1. Approximately $40,025.00 was sent by identified victims to Subject Account 2 and approximately $549,600.00 not ultimately recalled by the originator bank was sent in Additional Deposits to Subject Account 2, for a total of $589,625.00, which the government seeks to seize from Subject Account 2. Approximately $56,600.00 was sent in Additional Deposits to Subject Account 3, which the government seeks to seize from Subject Account 3. Approximately $119,600.00 not ultimately recalled by the originator bank was sent in Additional Deposits to Subject Account 4, which the government seeks to seize from Subject Account 4.

V.

CONCLUSION

45. Based upon the foregoing, there is probable cause to believe that the Subject Funds represent proceeds derived from violations of 18 U.S.C. § 1343 (Wire Fraud), which constitutes "specified unlawful activity" pursuant to 18 U.S.C §§ 1956 (c)(7)(A) and 1961 (1)(B). Therefore, the Subject Funds are subject to seizure under 18 U.S.C § 981 (b)(2) and forfeiture pursuant to 18 U.S.C § 981 (a)(1)(c).

46. In addition, there is probable cause to believe that the Subject Funds are subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 982(b) and 21 U.S.C. § 853(f) because the funds would, in the event of conviction on the alleged underlying offenses, be subject to forfeiture, and an order under section 21 U.S.C. § 853(e) would not be sufficient to assure the availability of the property for forfeiture.

//

//

47. To the extent that the Subject Funds are not the actual monies traceable to or involved in the illegal activities identified herein, these funds are identical property found in the same account as such property, rendering these funds subject to forfeiture pursuant to 18 U.S.C. § 984.

Fred Apodaca
Fred Apodaca
Special Agent
United States Secret Service

Attested to by the applicant in
accordance with the requirements
of Fed. R. Crim. P. 4.1 by telephone
on this _____ day of August 2024

_____
UNITED STATES MAGISTRATE JUDGE