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

UNITED STATES OF AMERICA Plaintiff, v. $1,188,164.23 IN UNITED STATES CURRENCY Defendant.	§ § § § § § § §	NO: 6:24-CV-00137

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. $625,624.40 in JP Morgan Chase (JPMC) Bank account 558190552 (Target Account 1);

b. $461,988.50 in JPMC Bank account 561088397 (Target Account 2);

c. $100,551.33 in JPMC account 561620116 (Target Account 3);

that totals $1,188,164.23 into Check No. 4557181617 and was seized on or about January 17, 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 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 "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 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 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. 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 pig butchering 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 pig butchering 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 a Citibank bank account 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 also 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 B.H.

19. USSS investigators interviewed victim B.H. regarding the $80,000.00 transaction he sent to the JPMC account in the name of SUNSHINES TRADING, account number ending in 8678. B.H. was victimized by this cryptocurrency investment scheme, and it all began by meeting a person on Facebook who used the name Mona Johnson Chen. Chen introduced B.H. to the OKEX platform, the same platform introduced to victim T.G. mentioned earlier in this affidavit. B.H. suffered a loss of approximately $352,000.00 as a result of this scheme to the following entities: SUNSHINES TRADING, ROYAL CHRONOS LIMITED, and BLUEWAVE TRADE LIMITED. B.H. recently attempted to withdraw his funds from OKEX, but was informed he would need to pay $19,000 in taxes and/or fees prior to receiving his funds.

INVESTIGATION OF ROYAL CHRONOS LIMITED

20. USSS investigators initiated an investigation of ROYAL CHRONOS LIMITED (RCL) which held bank accounts at JPMC Bank. USSS investigators learned

from JPMC employees that RCL operated bank accounts ending in 3726 and 2357 that were recently closed by JPMC. However, RCL was allowed to establish a new account, TARGET ACCOUNT 1 at JPMC Bank.

21. USSS investigators obtained Internet Crime Complain Center (hereafter known as IC3) reports regarding queries related to RCL. There were two reports by separate victims whose recent transactions totaled $183,000,00. A review of JPMC bank records regarding TARGET ACCOUNT 1 and other JPMC accounts in the name of RCL verified these deposits as reflected in these IC3 reports. These victims all reported similar incidents as the other victims who were interviewed by USSS investigators during this investigation.

TARGET ACCOUNT INFORMATION AND TRANSACTIONS

22. Investigators issued a Federal Grand Jury subpoena to JPMC and obtained the bank records for the JPMC Bank accounts ending in 0552 (TARGET ACCOUNT 1), 3726, 2357 and 3021. These bank records identified the signor on TARGET ACCOUNT 1 and accounts ending in 3726, 2357 and 3021 accounts held in the name of RCL as Junchao Duan. The records indicate that on or about July 26, 2023, Duan began establishing the business bank accounts at JPMC Bank identifying RCL as a C-Corporation. The records reflect that TARGET ACCOUNT 1 was opened by Duan on or

about October 11, 2023. The records reflect that Duan provided the business address of 1000 W. 8th Street, Apartment 828, Los Angeles, California 90015.[1]

23. USSS investigators familiar with the apartment building located at 1000 W. 8th Street, Apartment 828, Los Angeles, California confirmed that this location is in downtown Los Angeles, California. This area has significant business activity due to its location. However, USSS investigators were unable to identify any business activity related to RCL at this location.

24. Investigators were unable to locate an Internet business presence for RCL.

25. Analysis of the bank records for TARGET ACCOUNT 1 indicate the account's activity from October 11, 2023, to November 8, 2023, included several deposits via wire transfers and other payments, such as Zelle transactions, totaling approximately $1,189,720.00. These transactions resembled deposits from individuals that were similar to other accounts identified in this investigation as having received proceeds of the fraudulent cryptocurrency investment scheme. The most significant withdrawal from TARGET ACCOUNT 1 includes a $376,000.00 transfer to Paretone Capital, an entity that has received a large portion of the proceeds in this investigation.

26. The following wire deposits were made into TARGET ACCOUNT 1 and are a sampling of the total deposits into TARGET ACCOUNT 1:

[1] Earlier in this investigation, USSS investigators identified the address utilized by RCL was also used by other shell companies in this investigation, including Stone Water Trading LLC, whose account was seized under seizure warrant number 6:23-MJ-270.

DATE	VICTIM	AMOUNT
11/1/2023	B.M.A.	$84,000
11/2/2023	R.M.J.	$68,000
11/2/2023	M.H.	$50,000
11/2/2023	C.L. TRUST	$20,000
11/3/2023	C.H.	$50,000
11/3/2023	A.M.	$27,000
11/6/2023	K.J.B.	$80,000
11/8/2023	T.M.N.	$400,000
11/8/2023	S.H.Y.	$71,500
11/8/2023	J.D.K.	$40,000
11/8/2023	V.M.B.	$40,000
11/8/2023	C.D.L.	$23,000
11/8/2023	T.F.L.T.	$50,000

INTERVIEWS OF ADDITIONAL VICTIMS THAT SENT FUNDS TO TARGET ACCOUNT 1

27. In addition to victims B.H. and J.G. who sent funds to a different account in the name of RCL, 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 A.M.

28. USSS investigators identified and interviewed victim A.M. regarding the $27,000 he sent to TARGET ACCOUNT 1. A.M. desired to invest in cryptocurrency and researched the topic on the Yahoo Financial website. On or about July 2023, A.M. discovered a link on the Yahoo Financial website for Fire Phoenix, which was advertised as an investment platform where individuals could invest in cryptocurrency based upon

market activity. A.M. was able to establish an account using the Fire Phoenix link and did so by providing his identification and contact information. A.M.'s initial investment was $5,000 and he was able to earn $1,300 in a short time period. A.M. was allowed to withdraw his earnings and was paid these earnings via his account at Crypto.com. As a result of A.M's quick investment success using the Fire Phoenix platform, A.M. eventually invested approximately $930,000.00 through a series of transactions.

29. A.M. recently attempted to withdraw a larger portion of his funds and was informed he would be required to pay a fee to conduct withdrawals. The purpose of the $27,000 transaction to TARGET ACCOUNT 1 was to pay for these fees. A.M. reported that once the fee was paid, he was then advised he needed to pay taxes on his earnings prior to withdrawing any funds. A.M. requested the taxes/fees be deducted from his balance in Fire Phoenix but was informed the taxes/fees must be prepaid. A.M. has not been able to recover any additional funds he lost as a result of this fraud scheme.

Victim C.D.L.

30. USSS investigators interviewed C.D.L. regarding the $23,000 transaction he sent to TARGET ACCOUNT 1 on November 8, 2023. C.D.L. recounted details very similar to several other individuals who have been victimized by this cryptocurrency investment fraud scheme. C.D.L. provided USSS investigators the following statements. C.D.L. came into contact with a person using the name Joanna Piechocka on or about September 30, 2023. C.D.L. explained how their conversation eventually turned to

investing in cryptocurrency, and Piechocka provided C.D.L. with a website that he could utilize to invest in cryptocurrency. C.D.L. stated the website advertised to its users that the greater the amount invested the greater the earnings its users would earn. C.D.L. cautiously made an initial investment of $1,000 by purchasing cryptocurrency via the Kraken exchange. C.D.L.'s investment account on the website continued to earn value rapidly, and he continued to purchase cryptocurrency via the Kraken exchange. Kraken eventually closed C.D.L's account, and he was prompted to fund his investment account by sending wire transactions to various bank accounts including TARGET ACCOUNT 1.[2]

31. C.D.L. recently attempted to withdraw a large portion of his investment account and was informed that he would be required to pre-pay a 10% fee prior to withdrawing any funds. Once he was prompted with this information, C.D.L. knew he had been defrauded and made attempts to recover his funds without success. C.D.L. stated he also completed an IC3 report and filed a local police report. C.D.L. advised he suffered a loss of approximately $145,000 as a result of this fraud scheme.

Victim V.M.B.

32. USSS investigators interviewed victim V.B.M. regarding the $40,000 transaction he sent to TARGET ACCOUNT 1 on November 8, 2023. V.B.M. provided

[2] Based on my experience conducting investigations involving cryptocurrency, cryptocurrency exchanges will close accounts as they discover the addresses transacting within that account have been reported and confirmed to be receiving criminal proceeds.

the following statements regarding his involvement in this fraud scheme. V.B.M.'s friend referred him to an individual with whom he reported to have been earning a substantial return by investing in cryptocurrency. V.B.M.'s friend personally showed him how to invest by connecting with a web-based platform identified as Curve.

33. V.B.M. accessed the customer support function of the Curve platform and engaged in conversation with an unknown subject. The website advertised the investment included purchasing USDT to be able to trade short options of BTC. After V.B.M. made the transaction, the customer support representative contacted him to recall his wire transaction and indicated they would direct him to send funds to another account. By that point, V.B.M.'s wire transaction was already processed, and he was not able to recover his funds. V.B.M. has suffered a loss of $40,000 as a result of this fraud scheme, and his friend also suffered a loss of approximately $200,000.

INVESTIGATION IDENTIFIES TARGET ACCOUNT 2 AS RECEIVING VICTIMS' FUNDS

34. USSS investigators identified TARGET ACCOUNT 2 held in the name of LEGENDEL INC. 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.

35. Bank records reveal that TARGET ACCOUNT 2 was opened on or about October 27, 2023, and the signor on the account is Junchao Duan, the same signor as on

TARGET ACCOUNT 1. The address utilized for this account is 811 W. 7th Street, Suite 1200, Los Angeles, California 90017.

36. Investigators located business records for Legendel Inc. were filed with the State of Delaware Secretary of State on or about August 24, 2023.

37. Analysis of the bank records for TARGET ACCOUNT 2 indicate the account received deposits totaling approximately $769,651.00. Most of the transactions resembled wire and Zelle deposits from individuals that were similar to other accounts identified in this investigation as having received proceeds of the fraudulent cryptocurrency investment scheme, as well as an additional deposit of $168,000.00. Similar to TARGET ACCOUNT 1, the most notable withdrawal included a $298,000 wire to Paretone Capital.

38. The following wire deposits are examples of the deposits that were made into TARGET ACCOUNT 2:

DATE	VICTIM	AMOUNT
11/8/2023	T.M.N.	$400,000
11/8/2023	K.G.K.	$62,000

INTERVIEW OF VICTIM WHO SENT FUNDS TO TARGET ACCOUNT 2

39. When reviewing the deposits for TARGET ACCOUNTS 1 AND 2, USSS investigators identified victim T.M.N. as sending $400,000 to each account on November 8, 2023.

Victim K.G.K.

40. USSS investigators identified and interviewed victim K.G.K. regarding the $62,000.00 transaction he sent to Target Account 2. K.G.K. was very interested in investing in cryptocurrency and was engaged in an online chat group regarding cryptocurrency investments. K.G.K. does not have any knowledge about investing in cryptocurrency and was looking for advice in the chat group. K.G.K. communicated with an unknown subject in the chat group who referred him to crypto.com to purchase cryptocurrency. K.G.K. was not able to establish an account, and the unknown subject offered to assist K.G.K.

41. K.G.K. stated that the unknown subject provided him TARGET ACCOUNT 2. Initially, K.G.K. was comfortable investing $3,000, but the unknown subject persuaded K.G.K. that he could earn larger profits by investing a larger amount. As a result, K.G.K. sent $62,000 to TARGET ACCOUNT 2. K.G.K. was naïve and did not ask the unknown subject about an expected rate of return or how he would receive the earnings from his investment. K.G.K. transferred the funds from his bank account to TARGET ACCOUNT 2 on November 8, 2023. Shortly after his funds were sent, K.G.K. received a text message from the unknown subject that advised K.G.K. to respond to his bank and request a wire recall.[3] K.G.K. explained that his banker told him that TARGET ACCOUNT 2 was frozen and a recall was not possible.

[3] On or about November 7, 2023, USSS investigators submitted a freeze request to JPMC for the funds in TARGET ACCOUNT 2. Based on my experience conducting fraud investigations, once fraudsters are

42. USSS investigators reviewed IC3 and other victim reports submitted by individuals who sent funds to other bank accounts associated with Legendel Inc. The individuals reported to IC3 similar incidents as other victims that sent funds to Target Account 2. The reports were dated from on or about August 29, 2023 to October 16, 2023, and indicate that at least one victim sent funds to bank accounts in the name of Legendel Inc. at Bank of America as well as to other known shell companies totaling approximately $295,600.

43. USSS investigators contacted Bank of America employees regarding the bank account held in the name of Legendel Inc. and was informed the account was previously closed by bank employees for unspecified reasons.

INVESTIGATION IDENTIFIES TARGET ACCOUNT 3 AS RECEIVING VICTIMS' FUNDS

44. USSS investigators identified TARGET ACCOUNT 3 held in the name of JUNCHAO DUAN. DUAN was also the signor on TARGET ACCOUNTS 1 and 2. USSS investigators reviewed the bank records for TARGET ACCOUNT 3 and discovered that the account was also utilized to receive funds from victims of this cryptocurrency investment fraud scheme.

45. Bank records reveal that TARGET ACCOUNT 3 was opened on or about October 27, 2023 and was frozen by USSS investigators on or about November 8, 2023.

---

made aware their bank accounts are not accessible, they will direct the vicitm to recall their funds and subsequently provide the victims with a different bank account so that they do not lose the vicitm's funds to bank and or law enforcement intervention.

The address utilized for this account is 1000 W. 8th Street, Apartment 828, Los Angeles, California.

46. Analysis of the bank records for TARGET ACCOUNT 3 indicate the account received deposits totaling approximately $121,950.00. These transactions resembled wire deposits from individuals that were similar to other accounts identified in this investigation as having received proceeds of the fraudulent cryptocurrency investment scheme. According to the records, there were no notable withdrawals from TARGET ACCOUNT 3.

47. During the short time period TARGET ACCOUNT 3 was operational, the following wire deposits were made into Target Account 3 and reflect most of the total deposits into Target Account 3:

DATE	VICTIM	AMOUNT
11/6/2023	J.G.	$48,500
11/8/2023	J.G.	$51,500
11/8/2023	K.S.C	$21,400

INTERVIEW OF VICTIM WHO SENT FUNDS TO TARGET ACCOUNT 3

Victim J.G.

48. USSS investigators interviewed victim J.G. regarding the two transactions he sent to TARGET ACCOUNT 3, totaling $100,000.00. J.G. was involved with a fraudulent investment scheme and wanted assistance with recovering his funds he sent as a result of the scam. J.G. was contacted by someone on Facebook who used the name Anna Lee. J.G. explained how his conversations with Lee turned to the subject of

investments in cryptocurrency and how Lee and her friends were earning 1.2% per day on their investments. J.G. communicated with Lee via WhatsApp. J.G. was sent photos and also participated in video calls with Lee. J.G. requested a photo of Lee's driver's license and was sent a photo of a California driver's license bearing the name of Anna Lee, DL number Y4155677.

49. J.G. has suffered a loss of $300,000 by purchasing cryptocurrency via crypto.com and then sent wires in the amounts of $48,000 and $52,000 to TARGET ACCOUNT 3.

50. J.G. provided USSS investigators numerous emails containing screenshots of communications, images of Lee, and the California DL mentioned above and other information including an additional bank account.

51. USSS personnel queried California DL number Y4155677 which returned to a different individual than Lee. This verified the California DL sent to J.G. is fictitious.

CONCLUSION

52. I submit that this affidavit supports probable cause for a warrant to forfeit all funds, monies, and other things of value up to $1,188,164.23 seized from JPMC Bank accounts:

a. $625,624.40 in JP Morgan Chase (JPMC) Bank account 558190552 (Target Account 1);

b. $461,988.50 in JPMC Bank account 561088397 (Target Account 2);

c. $100,551.33 in JPMC Bank account 561620116 (Target Account 3);

53. Based on my experience and the information herein, I have probable cause to believe that the seized $1,188,164.23 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).

54. I also have probable cause to believe that the seized $1,188,164.23 constitutes proceeds traceable to a violation of 18 U.S.C. § 1343 and/or 18 U.S.C. § 1349, and are therefore 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: 2024.04.12 16:58:51 -05'00'

Brad Schley, Special Agent
U.S. Secret Service