THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA, Plaintiff, v. 5,680,000 USDT TOKENS STORED WITHIN VIRTUAL CURRENCY ADDRESS 0x7f6Ed26BB1488D1b420E10D722ef8bDf7D845B31 THAT ARE IN THE CUSTODY OR CONTROL OF THE UNITED STATES MARSHALS SERVICE, Defendants.	Civil Action No. 2:26cv87

VERIFIED COMPLAINT FOR FORFEITURE

The United States of America, through undersigned counsel, and respectfully represents as follows:

1. Plaintiff, the United States of America, brings this civil action *in rem* for forfeiture to the United States of 5,680,000 USDT tokens held in virtual currency address 0x7f6Ed26BB1488D1b420E10D722ef8bDf7D845B31 (the "Defendant Property"), pursuant to 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C), 981(b), 982(a)(1), 982(a)(2), and 853(f). Prior to January 13, 2026, Tether Limited ("Tether") burned the 5,680,000 USDT tokens held in virtual currency address 0xC1B68434D0Ef9A78E7f62e3b9850B70B3d0174bf ("Address 74bf"). On January 13, 2026, Tether caused the 5,680,000 UDT to be reissued to virtual currency 0x7f6Ed26BB1488D1b420E10D722ef8bDf7D845B31 controlled by the United States Marshals Service ("USMS"). Tether took these actions pursuant to the seizure warrant that the Honorable Kezia O. L. Taylor, United States Magistrate Judge for the Western District of Pennsylvania, issued at Magistrate Number 25-1589. As discussed below, the 5,680,000 USDT constitutes

property involved in money laundering in violation of 18 U.S.C. § 1956 and proceeds of wire fraud in violation of 18 U.S.C. § 1343.

2. Jurisdiction is predicated upon 28 U.S.C. § § 1345 and 1355(a). Venue is proper under 28 U.S.C. § § 1395 and 1355(b).

BACKGROUND

3. From February 2025 through July 2025, the Federal Bureau of Investigation ("FBI") investigated actors responsible for perpetrating a pig butchering scam[1] against a Pennsylvania victim, A.T., that resulted in a loss of approximately $585,000.

4. This complaint pertains to approximately 5,680,000 USDT that an unknown perpetrator stole from A.T. and at least 19 other victims located throughout the United States.

5. A.T. resides in the Western District of Pennsylvania. In February 2025, A.T. received a text message from an unknown number that stated, "Emily make sure you go to grandma's party." A.T. responded to the text message informing the unknown individual that the unknown individual had the wrong number and that A.T. is not Emily. A.T. and the unknown individual subsequently engaged in personal conversation. The unknown individual identified as "Miranda Lopez" ("Lopez"). After a few days, A.T. and Lopez began communicating on Telegram, an encrypted messaging application.

[1] A pig butchering scam is a term or metaphor used to describe an investment fraud scheme whereby the victim is gradually convinced by the perpetrator to make investments in cryptocurrency and then the perpetrator steals the victim's investment money.

6. Perpetrators involved in pig butchering scams use encrypted messaging applications, like Telegram, to communicate with their victims to evade law enforcement detection.

7. The communications between A.T. and Lopez on Telegram continued through in or around July 2025. In February 2025, to build A.T. confidence in Lopez's fraudulent investment scheme, Lopez explained her investment strategy to A.T. Additionally, to isolate A.T., legitimize her fraudulent investment scheme, and prevent A.T. from communicating with others to discover the fraudulent nature of the scheme, Lopez stated: "I hope you can keep this secret, do not disclose the information that you and I trade, because I do not want to share the trade nodes with you because I bring trouble to my aunt or myself, in the investment market about the market news is very important, once leaked will have a bad effect."

8. In February 2025, Lopez provided A.T. a domain. Lopez purported to A.T. that this domain would be where A.T. could access A.T.'s trading account and make trades. Lopez instructed A.T. on how to open A.T.'s trading account through the domain. Perpetrators involved in pig butchering scams, like Lopez, provide a domain to victims to establish the legitimacy of the cryptocurrency investment. In addition, the domain can be used as a mechanism to defraud the victim into believing their investment funds are growing when, in reality, the perpetrator is controlling and operating the domain. The domain also allows the perpetrators to provide victims with the illusion that their investments are growing when, in reality, the perpetrators have stolen the victims' funds, and the domains are entirely fraudulent.

9. In April 2025, Lopez explained to A.T. how to open an account at Coinbase, a legitimate U.S.-based cryptocurrency company, and invest in cryptocurrency. Based upon this, A.T, attempted to open a Coinbase account. However, Coinbase had to review A.T.'s account

before A.T. could access it.

10. Lopez instructed A.T. to reach out to Coinbase customer service to solve the issue. Lopez messaged A.T. and instructed A.T. to contact Coinbase as follows: "'Why can't I deposit funds to my Coinbase account?' Send that sentence to customer service to ask, honey." Lopez further instructed A.T., "'I am unable to deposit any funds into my Coinbase account and I was hoping you could help me resolve my issue.' Send it."

11. Ultimately, A.T. successfully opened an account at Coinbase. Separate from Coinbase, A.T. was provided with a cryptocurrency address where A.T. could deposit A.T.'s purported investment funds. Lopez represented to A.T. that the funds that A.T. invested through A.T.'s Coinbase account into the cryptocurrency address would be deposited into the trading platform to execute Lopez's investment strategy.

12. In April 2025, Lopez provided A.T. with explicit instructions on how to "invest" A.T.'s funds once they were moved into the trading platform. At the direction of Lopez, A.T. sent the following amounts to crypto trading platforms: (1) approximately $25,000 on or about April 10, 2025, and (2) approximately $242,000 on or about May 10, 2025. The total was approximately $267,000.

13. On May 20, 2025, A.T.'s balance on the investment platform provided by Lopez appeared to be approximately $2,685,315. The same day, when A.T attempted to withdraw a portion of A.T.'s funds from the fraudulent investment platform and transfer it into his personally controlled wallet, A.T. was instructed to pay a withdrawal fee in the amount of $232,000.

14. On June 10, 2025, A.T. paid the approximately $232,000 withdrawal fee to access A.T.'s funds. However, A.T. still could not withdraw any funds. On June 17, 2025, the investment platform customer service informed A.T. that A.T.'s account had been flagged for

insider trading, and, therefore, A.T. owed an additional fee of $320,000.

15. On June 24, 2025 and July 1, 2025, A.T. paid approximately $50,000 and $35,000, respectively, towards the insider trading fee. A.T. did not have the funds to complete the full payment. Following this, A.T. was still unable to access A.T.'s funds and realized A.T. may have been the victim of a scam. A.T. then contacted law enforcement.

16. A.T. provided the FBI with images from A.T.'s email account that included notifications from Coinbase. One of the images depicted a completed transaction from A.T.'s Coinbase account to virtual currency address 0xfa0a50dc366e2f0a5381e4d4b5fede589ab633a9 for 242,209.53 USDC, which was worth approximately $242,209.00. This was the previously described transaction that A.T. made at Lopez's direction on or about May 10, 2025.

17. Investigators traced approximately $230,000 of those stolen funds from A.T.'s Coinbase wallet to Address 74bf. A.T.'s funds were laundered through multiple virtual currency addresses and converted into a different type of cryptocurrency before being deposited into this address.

18. Address 74bf contained cryptocurrency worth approximately $5,680,000. Therefore, investigators performed additional cryptocurrency tracing to determine the other sources of funds held in the address. This resulted in the identification of at least 19 other victims. Each of these victims' funds moved through some of the same private virtual currency addresses used to launder A.T.'s funds prior to being deposited into Address 74bf. The following chart depicts the identified victims, their total estimated losses, and the method in which they were verified as victims of a cryptocurrency investment fraud scheme. These victims were either

interviewed by the FBI and/or filed an IC3 complaint[2] confirming them as victims. The estimated loss figures were compiled based on victim interviews and a review of the victims' cryptocurrency account records:

Victim	Estimated Loss	Contact
A.T.	$584,000	FBI interviewed
M.D.	$1,400,000	FBI interviewed
R.W.	$1,050,000	FBI interviewed
G.A.	$1,700,000	FBI interviewed
G.T.	$175,000	FBI interviewed
C.P.	$550,000	FBI interviewed
A.M.	$3,200,000	FBI interviewed
P.F.	$850,000	FBI interviewed
R.X.	$593,000	FBI interviewed
C.F.	$40,000	FBI interviewed
M.M.	$700,000	FBI interviewed
R.D.	$500,000	FBI Interviewed
V.M.	$20,000	FBI interviewed
R.N.	$800,000	FBI interviewed
T.N.	$140,000	FBI interviewed
M.E.	$100,000	FBI interviewed
N.B.	$1,080,000	IC3 filed
R.C.	$425,000	FBI interviewed
J.E.	$4,200,000	FBI interviewed
R.R.	$413,000	IC3 filed
TOTAL LOSS	**$18,520,000**	

19. The victim interviews and IC3 complaints revealed multiple commonalities with the investment fraud scheme and methods perpetrated against A.T. For the identified victims, these commonalities included, but were not limited to, the following: (1) the perpetrator initiating contact with the victim through a misdirected text message; (2) communications between the perpetrator and the victim moving to an encrypted messaging platform; (3) the perpetrator

[2] IC3 stands for the Internet Crime Complaint Center, a public-private partnership of the FBI that serves as a central hub for reporting suspected Internet-enabled criminal activity. An individual may file a complaint on www.ic3.gov on behalf of oneself or others affected by an incident.

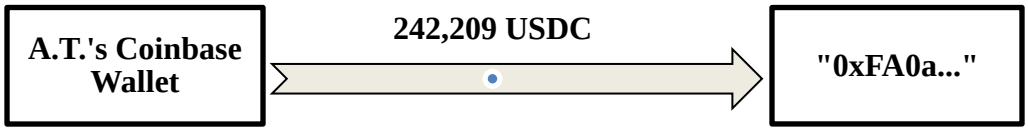
referencing an aunt, uncle, or other relation who had profitable information on making investments; (4) the victim's belief that the victim's cryptocurrency deposits were related to an investment in gold or options trading; (5) the perpetrators instructing the victim to establish an account on a legitimate cryptocurrency platform, from which the perpetrator further instructed the victim to send cryptocurrency to virtual currency addresses the perpetrator provided; (6) the perpetrator providing a fraudulent domain to the victim for supposed investment activities, which reflected bogus profits; (7) an inability of the victim to withdraw funds from the fraudulent investment platforms; and (8) efforts by the perpetrator to further defraud the victim by prompting the victim to pay taxes, fines, or other amounts before the victim could receive the money reflected in the victim's purported investment accounts.

20. As of September 15, 2025, Address 74bf contained 5,680,000 USDT. As described in more detail below, funds from A.T. and at least 19 other identified victims comprised approximately 2,495,000 USDT of that balance. Additionally, Address 74bf contained 991,000 USDT from Huione Pay, a Cambodia-based financial institution identified by the U.S. Treasury Department for laundering fraud proceeds. When combined, the victims' funds (2,495,000 USDT) and the Huione Pay funds (991,000 USDT) comprised 3,486,000 USDT that was stored within Address 74bf, or approximately 61.37 percent of the 5,680,000 USDT. The identified victims' losses significantly exceed the amount of funds that were traced to this address, together having lost approximately $18,520,000.

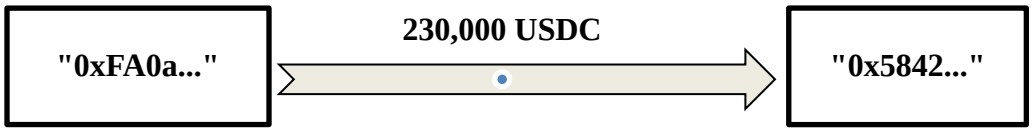
TRACING VICTIM A.T.'S STOLEN FUNDS

21. Investigators traced the 242,209 USDC A.T. sent from A.T.'s Coinbase wallet at Lopez's direction. A portion of those funds were combined with funds from other identified victims and ultimately deposited into Address 74bf.

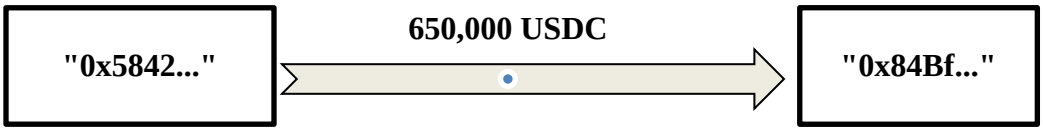
22. On May 10, 2025, A.T. sent approximately 242,209 USDC from A.T.'s Coinbase wallet to virtual currency address 0xFA0a50Dc366E2F0a5381E4d4b5fEdE589Ab633A9 at Lopez's direction. The virtual currency address beginning "0xFA0a…" is a private virtual currency address that is not hosted at a cryptocurrency exchange such as Coinbase. Less than one hour later, 230,000 USDC of those funds were transferred from the virtual currency address beginning "0xFA0a…" to private virtual currency address 0x5842b2E75D3566bD0D3F9F520E71c1f3b30B99a1. An illustration of the transaction is depicted below:



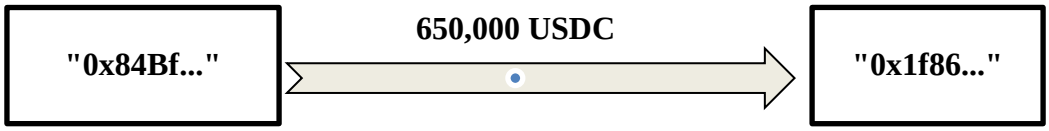
23. Less than one hour later, 230,000 USDC of those funds were transferred from the virtual currency address beginning "0xFA0a…" to private virtual currency address 0x5842b2E75D3566bD0D3F9F520E71c1f3b30B99a1, as depicted below:



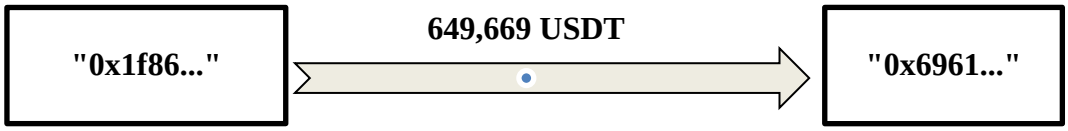
24. Over approximately the following hour, the address beginning "0x5842…" received funds from three other identified victims – M.D, J.E., and R.W. – causing the balance in the address beginning "0x5842…" to exceed 650,000 USDC. Less than three hours later, the address beginning "0x5842…" withdrew 650,000 USDC of those fraudulent funds to private virtual currency address 0x84Bf0c2B81538A81bF74c7312A0d9c8ba7DE9EA6, as depicted below:



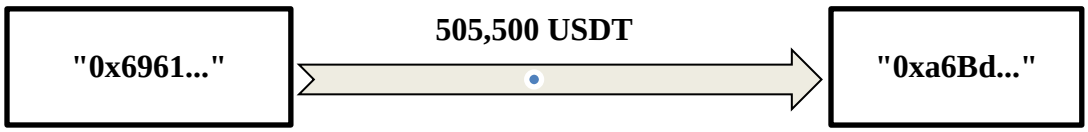
25. Approximately 25 minutes later, the address beginning "0x84Bf…" transferred the 650,000 USDC of fraudulent funds to private virtual currency address 0x1f86f1d03Fa55Ba95ed66a5Fd511D8e9532763D9, as depicted below:



26. Within 10 minutes of being deposited into the address beginning "0x1f86…", the 650,000 USDC of fraudulent funds was converted into approximately 649,669 USDT and then transferred to private virtual currency address 0x696158c731eA6627064bBb1f8622707c73B3E4D3, as depicted below:

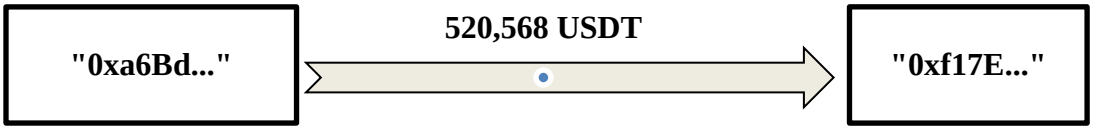


27. Approximately nine hours later, 505,500 USDT of those fraudulent funds were transferred from the virtual currency address beginning "0x6961…" to private virtual currency address 0xa6Bd877115cb261d355A6D26007606f496dd416A, as depicted below:

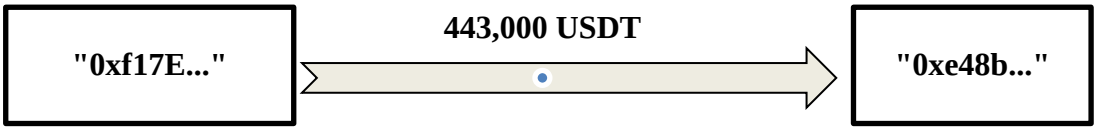


28. The address beginning "0xa6Bd…" contained approximately 15,068 USDT at the time it received the aforementioned deposit of 505,500 USDT of fraudulent funds. Approximately three minutes later, the entirety of the funds, approximately 520,568 USDT, were

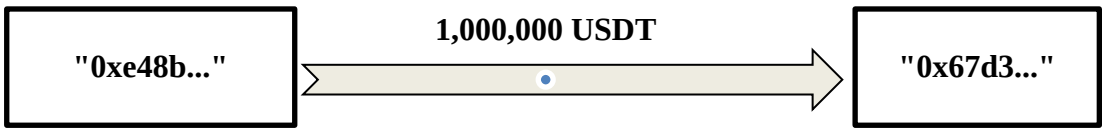
transferred from the virtual currency address beginning "0xa6Bd…" to private virtual currency address 0xf17E04068dd253C172e3Ada593DB379d1Bc36947, as depicted below:



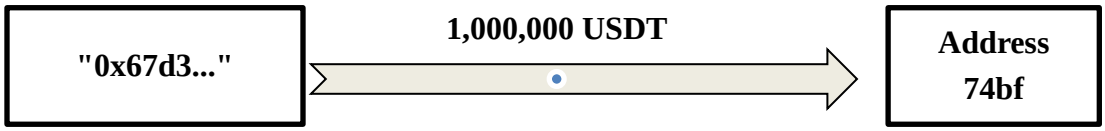
29. Over the next 40 minutes, the address beginning "0xf17E…" transferred 443,000 USDT of those funds in two transfers to private virtual currency address 0xe48b7069C06Cd32ad023F874E3089b757A7A7027, as depicted below:



30. Over the following approximately 15 hours, the address beginning "0xe48b…" received funds from multiple other identified victims – including approximately 272,000 USDT from G.A. and approximately 78,000 USDT from G.T. – that caused the balance in the address beginning "0xe48b…" to approximate 1,000,000 USDT, which was almost exclusively composed of identified, fraudulent funds. Less than three hours later, the address beginning "0xe48b…" withdrew the approximately 1,000,000 USDT to private virtual currency address 0x67d34102E9DCce008E121f34fd7d48D22349915d, as depicted below:



31. Within five minutes of being deposited into the address beginning "0x67d3…", the 1,000,000 USDT was transferred to Address 74bf, as depicted below:



32. In summary, the 1,000,000 USDT deposit into Address 74bf was comprised of victim funds from the grouping of A.T., M.D., J.E., and R.W. (approximately 430,000 USDT); G.A. (approximately 272,000 USDT); G.T. (approximately 78,000 USDT); and other identified victims.

IDENTIFICATION OF ADDITIONAL VICTIMS

33. As explained, Address 74bf contained 5,680,000 USDT. Of that, 5,000,000 USDT was deposited into the address in the span of one week. This includes the previously described 1,000,000 USDT deposit attributable to A.T., M.D., J.E., R.W., G.A., G.T., and other identified victims.

34. FBI investigators conducted cryptocurrency tracing on Address 74bf to identify the origin of the other funds held in this address. Investigators performed this tracing similar to the tracing of A.T.'s funds, but instead, the funds were traced in reverse. Using Address 74bf as a starting point, investigators worked backwards from this address to trace funds ultimately back to cryptocurrency exchanges that are responsive to U.S. legal process. Investigators obtained records from the cryptocurrency exchanges that identified the accountholders who originated the transfers of funds.

35. This methodology resulted in the identification of 19 additional victims whose funds are held in Address 74bf, as depicted in the chart above. Investigators conducted interviews and reviewed IC3 complaints for all 19 of these victims to confirm that they were victims of cryptocurrency investment fraud schemes.

36. Cryptocurrency tracing performed on Address 74bf also identified Huione Pay, an affiliate of the Cambodia-based financial institution Huione Group, as one of the sources of funds paid into Address 74bf. In May of 2025, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued a finding and notice of proposed rulemaking (NPRM) pursuant to Section 311 of the USA PATRIOT Act that identified Huione Group as a financial institution of primary money laundering concern and proposed to sever its access to the U.S. financial system. FinCEN issued a release that states, in part:

> Huione Group serves as a critical node for laundering proceeds […] for transnational criminal organizations (TCOs) in Southeast Asia perpetrating convertible virtual currency (CVC) investment scams, commonly known as "pig butchering" scams, as well as other types of CVC-related scams […] As described in the NPRM, for years, Huione Group has laundered proceeds of CVC scams, including CVC investment scams, and heists. Huione Group has set up a network of businesses, each playing a different role in its money laundering enterprise, that includes Huione Pay PLC […] The risks presented by Huione Group's association with illicit actors and transactions linked to illicit activity are compounded by either an absence of, or ineffective, anti-money laundering/know your customer (AML/KYC) policies and procedures among Huione Group's components.[3]

On October 14, 2025, FinCEN announced that it "finalized a rule under section 311 of the USA PATRIOT Act to sever the Cambodia-based financial services conglomerate, Huione Group, from the U.S. financial system." FinCEN explained that "[f]or years, Huione Group has laundered proceeds of virtual currency scams and heists on behalf of malicious cyber actors."

37. Approximately 991,000 USDT of the funds held in Address 74bf were traced to Huione Pay. Records are unable to be obtained from Huione Pay to identify the source of these funds. However, investigators believe that these funds are derived from cryptocurrency

3 FinCEN, *FinCEN Finds Cambodia-Based Huione Group to be of Primary Money Laundering Concern, Proposes a Rule to Combat Cyber Scams and Heists*, May 1, 2025, https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-based-huione-group-be-primary-money-laundering-concern.

investment fraud schemes. Notably, cryptocurrency tracing did not identify any legitimate sources of income in Address 74bf.

38. In total, approximately 3,486,000 USDT of funds held in Address 74bf were traced to identified victims (2,495,000 USDT) and Huione Pay (991,000 USDT). This represents approximately 61.37% of the total funds held in this address. While a precise loss figure attributable to the identified and suspected victims is unknown, investigators obtained information through (1) victim interviews, (2) IC3 complaints, and (3) legal process that establishes the identified victims lost approximately $18,520,000 through the fraudulent cryptocurrency investment schemes. That loss significantly exceeds the 5,680,000 USDT that were held in the Address 74bf, which has an approximate U.S. Dollar value of $5,680,000.

39. Therefore, on September 9, 2025, the Honorable Kezia O. L. Taylor, United States Magistrate Judge for the Western District of Pennsylvania, issued a warrant to seize all USDT held in Address 74bf. *See* Magistrate Number 25-1589. At that time, 5,680,000 USDT remained in Address 74bf. On September 22, 2025, FBI investigators served the seizure warrant on Tether. Tether complied with the warrant and burned the 5,680,000 USDT. On January 13, 2026, Tether reissued the 5,680,000 USDT to virtual currency address 0x7f6Ed26BB1488D1b420E10D722ef8bDf7D845B31 controlled by the USMS.

40. Based on the foregoing, there is probable cause to believe that the 5,680,000 USDT are subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C), 981(b), 982(a)(1), 982(a)(2), and 853(f) because the USDT are property involved in money laundering in violation of 18 U.S.C. § 1956 and proceeds of wire fraud in violation of 18 U.S.C. § 1343.

WHEREFORE, the United States of America respectfully requests that Judgment of Forfeiture be entered in favor of the United States for the 5,680,000 USDT and that the United States be granted such relief as this Honorable Court may deem just and proper, together with the costs and disbursements of this Action.

Respectfully submitted,

TROY RIVETTI
First Assistant United States Attorney

/s/ Jill L. Locnikar
JILL L. LOCNIKAR
Assistant U.S. Attorney
Joseph F. Weis, Jr. U.S. Courthouse
700 Grant Street, Suite 4000
Pittsburgh, PA 15219
(412)894-7429
(412)644-6995 (fax)
jill.locnikar@usdoj.gov
PA ID No. 85892 (AFF)

VERIFICATION

I am a Special Agent of the Federal Bureau of Investigation, Department of Justice, and the case agent assigned to this case.

I have read the contents of the foregoing complaint for forfeiture and the statements contained therein are true and correct to the best of my knowledge and belief.

I verify under penalty of perjury that the foregoing is true and correct.

Executed on this 15th day of January, 2026.

s/Travis Reece
Travis Reece, Special Agent
Federal Bureau of Investigation