

AO 108 (Rev. 06/09) Application for a Warrant to Seize Property Subject to Forfeiture

UNITED STATES DISTRICT COURT
for the
District of Colorado

In the Matter of the Seizure of)
(Briefly describe the property to be seized))
29264.913 USDT held in) Case No. 25-mc-00005-KAS
TPyXThfJJeYhCoyzDmtih9cHpxbHU92uUn)

APPLICATION FOR A WARRANT
TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the _____ District of _____
British Virgin Islands is subject to forfeiture to the United States of America under _____ 18 _____ U.S.C. §
981(a)(1)(A) and (C) (describe the property):

29264.913 USDT held in TPyXThfJJeYhCoyzDmtih9cHpxbHU92uUn

The application is based on these facts:

The facts to support a finding of Probable Cause for issuance of a Seizure Warrant are set forth in the attached affidavit which is continued on the attached sheet and made a part hereof.

☒ Continued on the attached sheet.

s/Eric Nebel
Applicant's signature

Eric Nebel, TFO FBI
Printed name and title

Sworn to before me and: ☐ signed in my presence. ☒ submitted, attested to, and acknowledged by reliable electronic means.

Date: January 10, 2025


Judge's signature

City and state: Denver, Colorado

Kathryn A. Starnella U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEIZURE WARRANT

INTRODUCTION AND AGENT BACKGROUND

I, Eric Nebel, being duly sworn, depose and state the following:

1. Your affiant, Task Force Officer Eric L. Nebel 97015, has been a Police Officer for over 28 years. Your affiant was assigned to the Denver Police Department Fraud Unit in 2007 as a detective. Your Affiant has conducted thousands of investigations involving Theft, Embezzlement, Identity Theft, Forgery, Computer Crime and On-Line scams. While still working in the Denver Police Department Fraud Unit, Your Affiant was assigned as a Task Force Officer to the Denver FBI Cyber Task Force in January of 2021. Your Affiant is a member of the Association of Certified Fraud Examiners. Your Affiant has training using Chainalysis and TRM software tools used for tracing various types of crypto currencies on the blockchain.

PURPOSE OF AFFIDAVIT

2. This affidavit is presented in support of an Application for Seizure Warrants to seize cryptocurrency in the following address ("Subject Addresses"):

- a. 31413.111 USDT to TTTA5YPSofZTksSzKPwzEbcDJRo2HQQG9AEJ;
- b. 29264.913 USDT to TPyXThfJJJeYhCoyzDmtih9cHpxbHU92uUn; and
- c. 29122.771 USDT to TKAiNaYevBfMZbMZFujK55PD8gbhhU1Sef.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all 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.

4. Based on the evidence described and detailed herein, there is probable cause to believe that the above-listed property constitutes or is derived from proceeds traceable to a specific unlawful activity, including violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1349 (conspiracy to commit wire fraud), and property involved in violations of 18 U.S.C. § 1957 (money laundering) and, therefore, are subject to seizure and forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (C), and § 981(b).

CRYPTOCURRENCY TERMS

5. Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank, like traditional fiat currencies such as the U.S. dollar, but are generated and controlled through computer software. Bitcoin (“BTC”) is the most well-known virtual currency in use.

6. Virtual currency addresses are the particular virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of alphanumeric characters.

7. The identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity.

8. Each virtual currency address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address’s private key can authorize a transfer of

virtual currency from that address to another address. A user of virtual currency can utilize multiple addresses at any given time and there is no limit to the number of addresses any one user can utilize.

9. A virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

10. Many virtual currencies publicly record all their transactions on what is referred to as the "blockchain." The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable and historical record of every transaction that has ever occurred utilizing that blockchain's specific technology. The blockchain can be updated multiple times per hour and record every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

11. USDT (also known as Tether) is a cryptocurrency that resides on multiple blockchains. The value of USDT is tied to the value of the U.S. dollar; therefore, one unit of USDT is equivalent to approximately one U.S. dollar, making it what is known as a "stablecoin." USDT is issued by Tether Ltd., a company headquartered in the British Virgin Islands. USDT is hosted on the Ethereum and Tron blockchains, among others.

12. XRP is a digital asset and cryptocurrency token that was created in 2012 by Ripple Labs as a faster, cheaper alternative to Bitcoin. XRP is used on the XRP

Ledger, which is a distributed ledger system that uses a consensus protocol to verify transactions.

Criminal Investigation

13. On December 2, 2024, your Affiant received Denver Police Department case number 24-645882. The original Denver Police Department Incident Report was completed by Officer Moreno 23087.

14. The initial police report indicated between November 23, 2024, and November 24, 2024, the victim, G.F. residing in Denver, Colorado 80237, became a victim of a Coinbase Customer Support scam. G.F. stated he attempted to log into his Coinbase account and discovered it was locked. Shortly afterwards, he received a telephone call (408-676-9984) from a person “Steven Jones” purporting himself to be with Coinbase Customer Support. G.F. gave Jones control of his computer through remote access believing Jones would help him reset his Coinbase account. G.F. provided Jones with his driver’s license, passport, and google authentication password via the computer camera.

15. G.F. advised that Jones even had him repeat words for voice recognition and the process would take 12 hours for the account to be unlocked with the new password. G.F. related during this time; Jones transferred \$176,100.00 in crypto currency from G.F.’s Coinbase account onto crypto currency addresses not controlled by G.F. Jones did not return the crypto currency back to the control of G.F. causing him to suffer a financial loss of \$176,100.00.

16. G.F. completed a typed statement in which he related the following information:

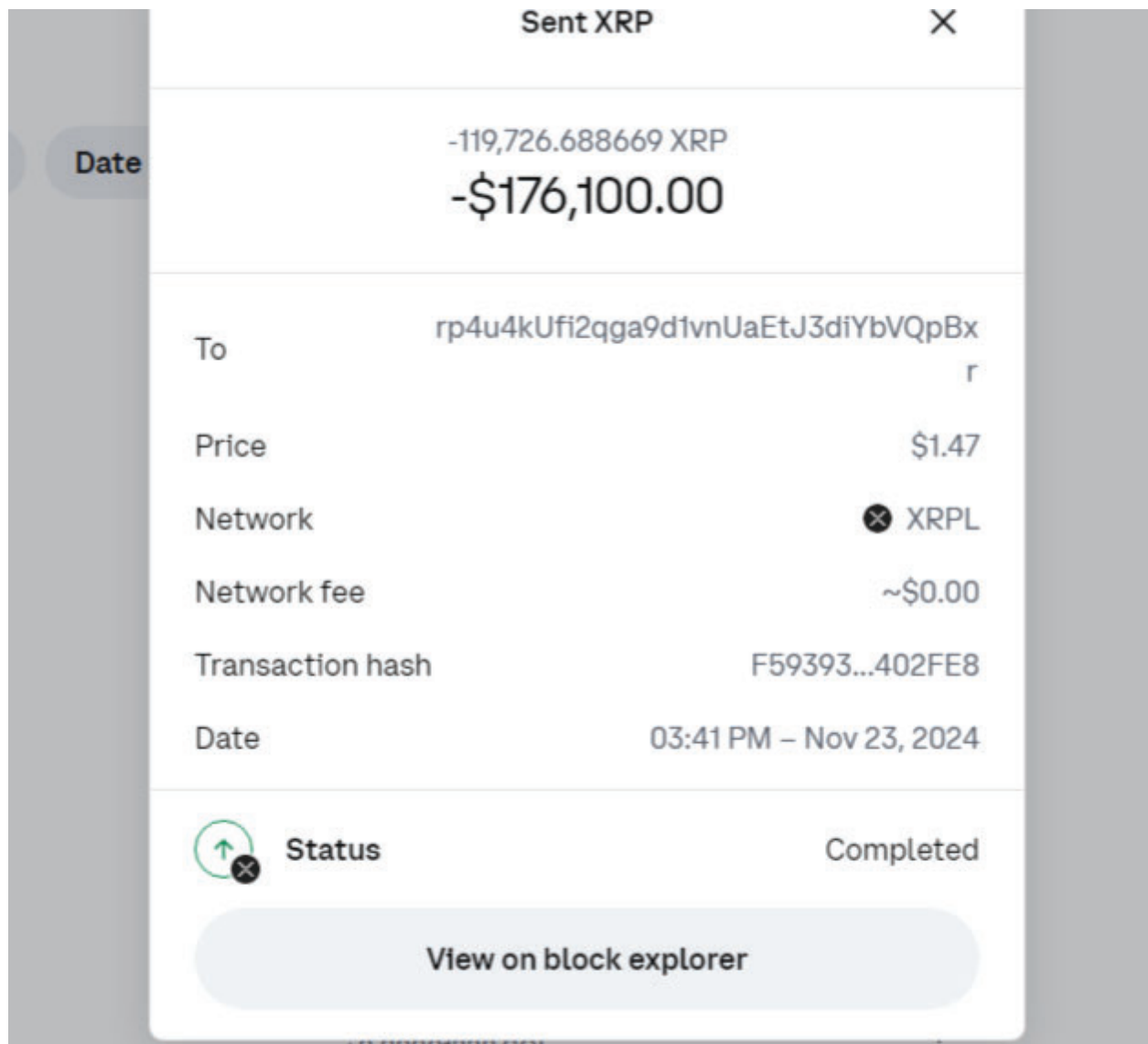
“ I reviewed my telephone call log from Steven Jones (Hacker) and realized he had first contacted me 11/22/24 immediately following my attempt to open my Coinbase account which appeared locked. This individual indicated that he was following up after my attempt to open my account and stated he was with Coinbase support. He called me multiple times stating he was multitasking with other customers and kept calling me back. During this initial call, he stated he would help me unlock my Coinbase account and indicated there was an attempt from Brazil to get into my account and that was the reason it was locked for security reasons. On 11/22 he indicated it would take approximately 12 hours after going through the online security verification process to reopen my account. He stated he could help me with that if I'd like and I thought that was considerate and normal and Coinbase had been reaching out to help. He guided me through the steps and somehow transitioned me to coinmarketcap.com. somehow, he was able to show me my crypto currencies and at the same time had control over my computer as he helped me upload and go through the motions of verification i.e., driver's license, passport, visual recognition on my computer's camera. During the conversation I had mentioned that in March my crypto had been stolen from my ledger nano s due to a mistake I had made by exposing my 24 words on my computer to print a couple of copies and then I deleted the photograph on my computer. Not realizing until later it was discovered in my deleted items file when my computer was unknowingly hacked a few years prior. Steven Jones indicated he be able to recover those funds by reversing the transaction as he had the sent address from the transaction. Within an hour he called me back and showed me approximately \$68,000 on coinmarketcap. He really had me believing he was helping me as an employee of Coinbase, particularly at that point. He

then stated that it would take approximately 12 hours after the verification process. He guided me through for my account to be unlocked. On 11/23/24 he called in the morning stating my account had been unlocked and he needed to complete the process with my Google authenticator code which he helped me install on my phone. He indicated that there was no reason to check or open my Coinbase account because all the assets had been moved to coinmarketcap which was owned by Coinbase, and my funds could be traded there. Then he proceeded to let me know that the support personnel were able to day trade for Coinbase customers generating profits and being compensated by Coinbase from the fees they were generating. While trading these accounts, he mentioned he had nine screens up helping multiple customers and that was the reason he was calling for brief periods of time and then getting back with me as he was so busy. On the 23rd he had already increased the recovered funds amount which I allowed him to trade by several thousand dollars and had me really believing he was real and doing this as a service through Coinbase. He called me regularly on a daily basis for several days telling me he was about to start a trade and would call me at the end of the day with the results which were always an increase in my recovered asset account. In the back of my mind, I felt some suspicion and asked him to send me an email from Coinbase with his contact info. I also asked him if he could put me in touch with other individuals, he was trading for with Coinbase. He said no problem, and within a few hours he had a three-way call with a supposed client named Gene. I asked Gene several questions about his relationship with Steven Jones and how long he'd been trading, and he answered about 2 months and had made substantial gains as a result of working with him. On November 27th, 2024, I contacted a trusted friend who was very familiar with

crypto and the trading process and asked him to view my account on coinmarketcap. I shared my screen with him on zoom and he asked me where is your crypto? He stated coinmarketcap doesn't hold crypto. It must be in your Coinbase account or hardware wallet. We then opened my Coinbase account together and he told me all my assets had been removed on 11/23/24. I then asked him to do a three-way call with me immediately to Steven Jones, the hacker. I was so stunned and embarrassed that I wanted him to confront this person and ask him proper questions in hopes that somehow my crypto was still somewhere I had access to. We contacted Steven Jones. My friend Matt confronted him. He stumbled and couldn't answer the questions and then hung up. I tried calling Steven Jones back later and the phone just rang and then ultimately disconnected. I then immediately locked my Coinbase account and contacted their support line. I spoke with the Coinbase support person and reported what had happened and he suggested I contact the local police and file a report with IC3 immediately."

17. Your affiant received an email from G.F. containing a screenshot of the crypto currency transfer out of his Coinbase account.

18.



19. Your Affiant used the Chainalysis Reactor software tool to trace the transfer out of G.F.'s Coinbase account. G. F.'s crypto currency, totaling approximately 119,726.688669 XRP was transferred out in two transactions to address: rp4u4kUfi2qga9d1vnUaEtJ3diYbVQpBxr (**Fraud wallet QpBxr**).

Transaction 1:

TX Hash
F59393F2CA8A8F3A5AC05E811D9A8DB3DC0ABCABE2A21B15AC8CB4CE4B402FE8

11/23/2024 11:47 PM 119726.688649 XRP rp4u4kUfi2qga9d1vnUaEtJ3diYbVQpBxr
From r4sRyacXpbh4HbagmgfoQq8Q3j8ZJzbZ1J

Transaction 2:

TX Hash
5570E8972625FA9C1F88049F101BBDFBF1DE5AF18D851942C298F727B5EBFA87
11/23/2024 11:57 PM 9173.688502 XRP rp4u4kUfi2qga9d1vnUaEtJ3diYbVQpBxr
From r4sRyacXpbh4HbagmgfoQq8Q3j8ZJzbZ1J

20. From **Fraud wallet QpBxr**, the XRP was transferred to a series of other wallet addresses. Eventually, the XRP was split up and sent to Fixed Float Exchange in six transactions. Fixed Float Exchange is a decentralized non-custodial exchange typically used for trading various types of crypto currency.

Transaction 1:

TX Hash
87B6A946BF06B80995B9A3968D018BAE5A694F57B69749D3CD8A7892865FC475
11/24/2024 10:32 PM 25000 XRP rffGCKC7Mk4cQ5aUGg8pfRe3MPC7Cy8gfe
From rwc9FsEbotZi3zTuDD7z992ADUNhRfkLXM

Transaction 2:

TX Hash
FEB603D0A96A34CF4948AC4813D39A5AD42A7F8AC87E8F0A8207A48E8D6662FB
11/24/2024 10:31 PM 20000 XRP rffGCKC7Mk4cQ5aUGg8pfRe3MPC7Cy8gfe
From rwc9FsEbotZi3zTuDD7z992ADUNhRfkLXM

Transaction 3:

TX Hash
21FC408B6B33B3979C4B67649463B96A719B5A2BED3A9459DB29AD7DA612DC6D
11/24/2024 10:58 PM 21184.99 XRP rffGCKC7Mk4cQ5aUGg8pfRe3MPC7Cy8gfe
From rfriLaW1kvjo4RXRuJy9mnpmTuteFjfbBR

Transaction 4:

TX Hash
567EF248C1397E67E9F1A14FEAC406DCBD81EBBB823188FDAD3A51F1AD2174F6
11/24/2024 11:04 PM 20194.999 XRP rffGCKC7Mk4cQ5aUGg8pfRe3MPC7Cy8gfe
From rsETJY9Ph92KGh2xEzDCPUwSjDqYMnnp64

Transaction 5:

TX Hash

D5DE0732E5511856F93963617E2710A0003BD981672BC127E60A590DB850CC0A
11/24/2024 10:50 PM 22084.99 XRP rffGCKC7Mk4cQ5aUGg8pfRe3MPC7Cy8gfe
From rLbGEdoPM33RKKx4kfDHpu34XEhgF1PiwQ

Transaction 6:

TX Hash

BB0A71A1E6E19C26D7CDD46B28FD343C53FDEBA710A1E9FB74F185095F5FC3C
B
11/26/2024 4:34 AM 20350.35 XRP rffGCKC7Mk4cQ5aUGg8pfRe3MPC7Cy8gfe
From r3xWfVhseVPJwfMNH1ocNS5wcXvTXW7RvX

21. On December 3, 2024, your Affiant received an email from Fixed Float Exchange containing Excel Spreadsheets for the requested transactions. Based on the information provided, G.F.'s cryptocurrency, which was 128,815.329 Ripple (XRP) when it was transferred out of the Coinbase account, was subsequently traded for 184,498.998 Tether (USDT).

Transactions from Fixed Float:

FF Transaction 1:

TX Hash

7d0d566d9c6703b04a9d762bd72f1cb65f25782650b5b31e873e4c9309eb2494
11/24/2024 10:51 PM 31413.111 USDT
TTTA5YPSofZTksZKPwzEbcDJRo2HQQG9AEJ
From FixedFloat; TDoXUNZ6PajKuiUkcYg3EDSV9bnqGqsbcf

FF Transaction 2:

TX Hash

715bca25053cb33679c34c80ff20b9922364a60474a4119510ba5e5bad14463e
11/24/2024 10:59 PM 30403.254 USDT
TBkjJddSHrF3bY9T7g1WGmB2FcdbXQGshr
From FixedFloat; TDoXUNZ6PajKuiUkcYg3EDSV9bnqGqsbcf
These funds were subsequently transferred to
TBR5AM2ch6xdECXn1m7eDfxSeqSi7ooQPE

FF Transaction 3:

TX Hash

178c4b1ec18fee2ed51f4aa0efc2a1671160ebb1c85a2b4e514edd72f08b0cfb

11/26/2024 4:35 AM 29264.913 USDT

TPyXThfJJJeYhCoyzDmtih9cHpxbHU92uUn

From FixedFloat; TDoXUNZ6PajKuiUkcYg3EDSV9bnqGqsbcf

FF Transaction 4:

TX Hash

b439adb825b40c557aff50415c492c3a3ebf0b90abbf821c349f9d80d8469514

11/24/2024 10:32 PM 28557.591 USDT

TZEuofsAEY9XEtHcqku49q2deQDecCWYzc

These funds were subsequently transferred to

TBR5AM2ch6xdECXn1m7eDfxSeqSi7ooQPE

FF Transaction 5:

TX Hash

27a8f86895918b274970deaf390ac7809e3239cf0785b30748294a5a9b3b2cc9

11/24/2024 10:33 PM 35737.358 USDT

TZEuofsAEY9XEtHcqku49q2deQDecCWYzc

From FixedFloat; TDoXUNZ6PajKuiUkcYg3EDSV9bnqGqsbcf

These funds were subsequently transferred to

TBR5AM2ch6xdECXn1m7eDfxSeqSi7ooQPE

FF Transaction 6:

TX Hash

fe33b0dad8ffc73af724ff561a9d05b12fd0dce2866762677cd9f4fec7efa911

11/24/2024 11:05 PM 29122.771 USDT

TKAiNaYevBfMZbMZFujK55PD8gbhhU1Sef

From FixedFloat; TDoXUNZ6PajKuiUkcYg3EDSV9bnqGqsbcf

22. Your Affiant reviewed the Fixed Float Exchange transactions on the blockchain. As described above, your affiant learned approximately 89,799 USDT was then transferred to the following addresses in the following amounts:

- a. 31413.111 USDT to TTTA5YPSofZTkSzKPwzEbcDJRo2HQQ9AEJ (**FF**

Transaction 1);

- b. 29264.913 USDT to TPyXThfJJJeYhCoyzDmtih9cHpxbHU92uUn (**FF Transaction 3**); and
- c. 29122.771 USDT to TKAiNaYevBfMZbMZFujK55PD8gbhhU1Sef (**FF Transaction 6**).

23. The above transfers were the only deposits to those addresses and the funds were still there as of January 8, 2025.

24. The approximately 94,697 USDT transferred to the other two addresses (TBkjJddSHrF3bY9T7g1WGMb2FcdbXQGshr (30403.254 USDT) and TZEuofsAEY9XEtHcqku49q2deQDecCWYzc (35737.358 USDT / 28,557 USDT) were transferred out of those addresses and co-mingled with other funds, such that they could not be recovered.

25. On December 5, 2024, Tether Compliance voluntarily froze Tether addresses TKAiNaYevBfMZbMZFujK55PD8gbhhU1Sef (29122.771 USDT), TTTA5YPSofZTkSzKPwzEbcDJRo2HQG9AEJ (31413.111 USDT), and TPyXThfJJJeYhCoyzDmtih9cHpxbHU92uUn (29264.913 USDT) based on allegations of fraud, pending further legal process.

26. To date, no one has contacted Tether regarding the freezing of these accounts.

CONCLUSION

27. Based on the records and blockchain analysis, there is probable cause to believe that the funds held by Tether 89,800.795 USDT were directly involved in the receipt of funds linked to the fraud against the victim.

28. Based on the facts stated above there is probable cause to believe that the **Subject Addresses: TKAiNaYevBfMZbMZFujK55PD8gbhhU1Sef, TTTA5YPSofZTkSzKPwzEbcDJRo2HQG9AEJ, and TPYXThfJJJeYhCoyzDmtih9cHpxbHU92uUn** received the proceeds of a wire fraud, conspiracy to commit wire fraud and money laundering scheme performed in violation of 18 U.S.C. §§ 1343, 1349 (wire fraud and conspiracy to commit wire fraud), and 18 U.S.C. §§ 1957 (money laundering). Those proceeds are subject to seizure pursuant to Title 18 U.S.C. § 981(b)(2) and (3) and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and (C).

29. The Court has authority to issue seizure warrants for property located outside the District of Colorado, pursuant to Title 18, United States Code, Section 981(b)(3). Section 981(b)(3) provides that a seizure warrant may be issued by a judicial officer in any district in which a forfeiture action may be filed under Title 28, United States Code, Section 1355(b), “and may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement.” 18 U.S.C. § 981(b)(3). In turn, Title 28, United States Code, Section 1355(b) provides that a forfeiture action may be brought in any district where any of the underlying acts or omissions occurred upon which the forfeiture is based.

30. Therefore, I request the issuance of a seizure warrant for the following cryptocurrency in the following wallet addresses based on the forfeiture provisions of 18 U.S.C. §§ 981(a)(1)(A) and (C), pursuant to 18 U.S.C. § 981(b):

- a. 31413.111 USDT to TTTA5YPSofZTkSzKPwzEbcDJRo2HQG9AEJ;

- b. 29264.913 USDT to TPyXThfJJeYhCoyzDmtih9cHpxbHU92uUn; and
- c. 29122.771 USDT to TKAiNaYevBfMZbMZFujK55PD8gbhhU1Sef.

Reviewed and submitted by Tonya Andrews Assistant United States Attorney.
Subscribed and sworn to before me on 10 January 2025.

Respectfully submitted,

s/Eric Nebel

Eric Nebel
Task Force Officer
Federal Bureau of Investigation

Attested to by the applicant in
accordance with the requirements
of Fed. R. Crim. P. 4.1 by
telephone on this 10 day of
January, 2025.



HONORABLE KATHRYN A. STARNELLA
UNITED STATES MAGISTRATE JUDGE