UNITED STATES DISTRICT COURT

for the

EASTERN DISTRICT OF WISCONSIN

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

APPROXIMATELY 39,500 TETHER (USDT), AND ANY OTHER CRYPTOCURRENCY ON DEPOSIT IN BINANCE ACCOUNT USER ID #78437498, HELD IN THE NAME OF RAHUL SETH

Case Number: 22 MJ 161

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

TO: **BRIAN WALLANDER, a Task Force Agent assigned to the United States Secret Service, and any Authorized Officer of the United States.**

An application by a federal law enforcement officer or an attorney for the government requests that certain property be seized as being subject to forfeiture to the United States of America. The property is described as follows:

Approximately 39,500 Tether (USDT), and any other cryptocurrency on deposit in Binance account user ID #78437498, held in the name of Rahul Seth

I find that the affidavit and any recorded testimony establish probable cause to seize the property.

YOU ARE HEREBY COMMANDED to search on or before 10/7, 2022
(not to exceed 14 days)

☒ in the daytime – 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night, as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to United States Magistrate Judge William E. Duffin.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. §2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person, who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days. *(not to exceed 30)*
☐ until, the facts justifying, the later specific date of _____

Date and time issued 9/23, 2022; 12:21 p.m.

William E. Duffin
Judge's signature

City and state: Milwaukee, Wisconsin

THE HONORABLE WILLIAM E. DUFFIN
United States Magistrate Judge
Name & Title of Judicial Officer

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of:		
Inventory of the property taken:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF WISCONSIN

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

APPROXIMATELY 39,500 TETHER (USDT), AND ANY OTHER CRYPTOCURRENCY ON DEPOSIT IN BINANCE ACCOUNT USER ID #78437498, HELD IN THE NAME OF RAHUL SETH

Case Number: 22 MJ 161

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, Brian Wallander, being duly sworn depose and say:

I am a Task Force Agent assigned to the United States Secret Service, and have reason to believe that in the Northern District of California there is now certain property, namely, approximately 39,500 Tether (USDT), and any other cryptocurrency on deposit in Binance account user ID #78437498, held in the name of Rahul Seth, that is civilly forfeitable under 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C) and 984, including cross-references to 18 U.S.C. §§ 1956(c)(7) and 1961(1), and criminally forfeitable under 18 U.S.C. §§ 981(a)(1)(C) and 982(a)(1) in conjunction with 28 U.S.C. § 2461(c), as property that (1) constitutes or is derived from proceeds traceable to specified unlawful activity, namely, wire fraud in violation of 18 U.S.C. § 1343; and (2) was involved in, or is traceable to funds involved in, money laundering transactions in violation of 18 U.S.C. §§ 1956 and 1957, and which property is therefore also subject to seizure for purposes of civil forfeiture under 18 U.S.C. § 981(b) and for purposes of criminal forfeiture under 18 U.S.C. § 982(b)(1) and 21 U.S.C. § 853(f).

The application is based on these facts:

✓ Continued on the attached sheet.

❑ Delayed notice of ____ days (give exact ending date if more than 30 days:_____ is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Signature of Affiant
Brian Wallander

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone and email.

9/23/2022 at 12:22 PM
Date and time issued

at Milwaukee, Wisconsin
City and State

William E. Duffin, U.S. Magistrate Judge
Name & Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEIZURE WARRANT

I, Brian Wallander, being first duly sworn, hereby depose and state as follows:

FUNDS TO BE SEIZED

1. I submit this affidavit in support of an application for a warrant to seize approximately **39,500 Tether (USDT), and any other crypto-currency on deposit in Binance Account User ID #78437498, held in the name of RAHUL SETH.**

2. For the reasons set forth below, I submit that probable cause exists to believe that approximately **39,500 USDT and any other crypto-currency on deposit in Binance Account User ID #78437498** are:

- Funds traceable to, and are therefore proceeds of, a wire fraud offense or offenses committed in violation of Title 18, United States Code, Section 1343.
- Funds involved in, or traceable to funds involved in, money laundering offenses, committed in violation of Title 18, United States Code, Sections 1956 and 1957.
- Subject to civil forfeiture under Title 18, United States Code, Sections 981(a)(1)(A), 981(a)(1)(C) and 984, and subject to criminal forfeiture under Title 18, United States Code, Section 981(a)(1)(C); Title 28, United States Code, Section 2461(c); and Title 18, United States Code, Section 982(a)(1); and
- Subject to seizure via a civil seizure warrant under Title 18, United States Code, Section 981(b), and via a criminal seizure warrant under Title 18, United States Code, Section 982(b)(1) and Title 21, United States Code, Section 853(f).

BACKGROUND AND EXPERIENCE

3. I am a Detective with the City of Greenfield Police Department and have been employed with that department since 1996. I am currently assigned to the United States Secret Service Milwaukee Resident Office Financial Crimes Task Force ("MFCTF"). I was federally deputized in December of 2015. My duties as a Detective and Task Force Agent with the Secret Service include investigating financial crimes, such as identity fraud, check fraud, credit card fraud, bank fraud, wire fraud, currency-counterfeiting offenses, and money laundering.

4. As a Detective and Task Force Agent, I have conducted investigations into wire fraud, money laundering, and other complex financial crimes. In the course of those investigations, I have used various investigative techniques, including conducting undercover operations, reviewing physical and electronic evidence, obtaining and reviewing financial records, and working with cooperating sources of information. In the course of those investigations, I have also become familiar with techniques that criminals use to conceal the nature, source, location, ownership, and control of proceeds of crime and to avoid detection by law enforcement of their underlying acts and money laundering activities.

5. During my tenure as a law enforcement officer, I have been involved in the investigation of wire fraud and multiple variations of online computer fraud in Milwaukee County, in the State of Wisconsin, across the United States, and internationally. I have received training in the investigation of wire fraud, money laundering, and computer crimes. My training and experience includes the following:

a. I am a member of the International Association of Financial Crime Investigators (IAFCI) and have received formal training in the use of crypto currencies by persons involved in fraud and have a basic understanding of how crypto currencies work.

b. I know that persons involved in wire fraud and internet scams often attempt to protect and conceal proceeds through money laundering, including but not limited to domestic and international banks, securities brokers, service professionals, casinos, real estate, shell corporations, business fronts, and otherwise legitimate businesses which generate large quantities of currency. I know that it is common for online fraudsters to obtain, secrete, transfer, conceal, or spend fraud proceeds using digital currency, also known as crypto-currency.

c. Digital currency is generally defined as an electronic sourced unit of value, which can substitute for fiat currency. Digital currency exists entirely on the Internet and is not stored in any physical form. Digital currency is not issued by any government, bank, or company and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network.

d. Bitcoin is one type of digital currency. Bitcoin payments are recorded in a public ledger maintained by peer-to-peer verification and is, therefore, not maintained by a single administrator or entity. Individuals can acquire bitcoins either by "mining" or by purchasing Bitcoins from other individuals. An individual can "mine" for Bitcoins by allowing his computing power to verify and record the bitcoin payments into a public ledger. Individuals are rewarded for this by receiving newly-created Bitcoins. An individual can send and receive Bitcoins through peer-to-peer digital transactions or by using a third-party broker. Such transactions can be performed on any type of computer.

e. Bitcoins are stored on digital "wallets." A digital wallet essentially stores the access code that allows an individual to conduct bitcoin transactions on the public ledger. To access bitcoins on the public ledger, an individual must use a public address (or "public key") and a private address (or "private key"). The public address is similar to an account number while the private key is similar to an account password. Even though the public addresses of transactors are recorded on the public ledger, the true identities of the individuals or entities behind the public addresses are not recorded. If, however, a real individual or entity is linked to a public address, an investigator could determine what transactions were conducted by that individual or entity. Bitcoin transactions are, therefore, described as "pseudonymous," or partially anonymous.

f. A Binance account has multiple "wallets," sub-accounts, or sub-wallets for holding different currency (e.g., U.S. dollars, Bitcoin, Dogecoin, TetherUS, Bitcoin Cash, Bitcoin Gold), but all of the sub-wallets are within one account. The funds can be readily moved from one currency to another currency within the same account. The value of the cryptocurrency relative to the U.S. dollar is constantly changing so the exact value is unknown until

the funds are transferred out. Many Bitcoin companies allow the account holder to control the "key" for each wallet and that "key" is needed to transfer or remove funds. However, Binance controls the "key" to each of the wallets on its platform.

g. Online fraudsters often use enhanced cryptocurrency, such as Bitcoin, to protect their identities, launder money, and conceal drug proceeds, because of the anonymity provided by cryptocurrency. Bitcoin is a decentralized digital currency without a central bank or single administrator. Payments are sent from user-to-user on the peer-to-peer bitcoin network without the need for intermediaries. These services add layers of anonymity to financial transactions to evade law enforcement.

h. I know that persons involved in online fraud often use crypto currencies as a way of moving stolen funds very rapidly through electronic transfers into various crypto wallets. I know that crypto currencies are not backed by any government entity and that crypto currency is an international form of payment accepted throughout the world in the same format. For this reason, fraudsters can move large amounts of stolen funds internationally very rapidly in a digital universal format. Once the stolen funds are moved, comingled with other funds, and concealed, those funds can then be transferred to other forms of cryptocurrency or into fiat currency making it challenging for law enforcement to trace.

6. This affidavit is based upon my personal knowledge and upon information reported to me by other federal, state, and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. Throughout this affidavit, I refer to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom I have had regular contact regarding this investigation.

7. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

8. Under 18 U.S.C. § 984, a court may order the forfeiture of funds in a bank account into which monies subject to forfeiture have been deposited, without the need to trace the funds currently in the account to the specific deposits that are subject to forfeiture, up to the amount of

the funds subject to forfeiture that have been deposited into the account within the past one-year period.

9. I submit that a restraining order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the funds for forfeiture because I have been advised of cases in which, even after a restraining order or similar process has been issued to financial institution, the funds sought to be restrained were not effectively restrained by the financial institution. In my judgment, a seizure warrant would be the most effective way to assure the availability of the money sought to be seized for forfeiture by the accompanying seizure warrant.

PROBABLE CAUSE

10. Officers with the Greenfield Police Department are investigating a wire fraud scheme. The investigation concerns possible violations of, inter alia, 18 U.S.C. § 1343 (Wire Fraud) and 18 U.S.C. §§ 1956 and 1957 (Laundering of Monetary Instruments). This investigation has revealed that Binance account **User ID 78437498** held in the name of RAHUL SETH, received fraud proceeds from three different Bitcoin transactions that occurred on August 30, 2022, in this district.

11. On September 1, 2022, Greenfield Police Officer Tanner Kaczmarek spoke with J.K., who reported that she was recently defrauded out of approximately $40,000. J.K. explained that she wanted to obtain her bank statements to show law enforcement her financial information. Several days later, Officer Kaczmarek met with J.K., who explained that on August 30, 2022, she received an email that appeared to be from the "Geek Squad" which stated that a $404.00 payment was made from her bank account. Based on publicly available information, case agents are aware that the Geek Squad is a technical support service offered by Best Buy department store.

12. J.K. did not have an account with the Geek Squad so she called the telephone number on the email, which purported to be the number for the Geek Squad. J.K. was told by a person purporting to be a Geek Squad employee that they would look up the payment but needed J.K.'s personal information, including her name, address, phone number, Social Security Number, and bank account number. J.K. provided all of this information over the phone to the individual purporting to be a Geek Squad employee.

13. The individual purporting to be the employee then requested that J.K. give him permission to "remote in" to her computer, which J.K. granted. While on the phone, J.K. could see that her mouse cursor was moving on the computer screen without J.K. controlling it. J.K. was instructed to enter the amount of $404.00 on the screen because she was told that this is the amount that would be refunded to her account. The screen then showed $40,400.00. At the time, J.K. did not know if she accidentally typed that amount or if the individual purporting to be the Geek Squad employee entered it.

14. The individual purporting to be the Geek Squad employee then asked J.K. to check her online banking account with Waterstone Bank. J.K. noticed that her bank statement appeared to reflect that a deposit of $40,400.00 had been made into her checking account. When J.K. told the individual purporting to be the employee that this was the wrong amount, and that it went to her checking instead of her savings account, J.K. was then transferred to another individual named "Raymond."

15. "Raymond" told J.K. that in order to return the money, she needed to withdraw $20,000 in cash from her savings account and an additional $19,500 and then deposit it in various Bitcoin ATM locations. J.K. was instructed to insert the cash into the Bitcoin ATMs and provide "Raymond" with the receipts.

16. J.K. provided the Bitcoin ATM receipts to law enforcement. They reflect that J.K. made the following Bitcoin purchases and deposits using a Bitcoin of America ATM located at the Mian's Citgo gas station, 5235 W. Loomis Rd, Greenfield, WI 53129:

- On August 30, 2022, at approximately 6:28 p.m., J.K purchased 0.62692697 BTC for $15,000 and sent it to the crypto address CJvdFdYMmRcUj4o79kruSECiYUav48N35.

- On August 31, 2022, at approximately 7 p.m., J.K purchased 0.01856658 BTC for $450.00 and sent it to the crypto address bc1q6l4u8jdeuwm6jmkqmpl3karkyq0f8elysc0q2g.

- During that same visit at Citgo, at approximately 8:08 p.m., J.K purchased 0.59772336 BTC for $14,500.00 and sent it to the crypto address bc1q6l4u8jdeuwm6jmkqmpl3karkyq0f8elysc0q2g.

17. J.K. informed law enforcement that she knows she had purchased more Bitcoin than these three receipts show but did not have those receipts. J.K. thought she had some information on her phone but after realizing she was scammed, she deleted this information from her phone. J.K. provided law enforcement consent to conduct a forensic search of her phone and laptop computer hard drive to obtain this missing information. The following transactions were discovered through a forensic examination of J.K.'S phone:

- On August 30, 2022, at approximately 4:19pm, J.K. used a Crypto Dispensers ATM in Southridge Mall at 5300 S. 76th St, Greendale, WI 53129 where she purchased 0.11375987 BTC for $2,500 and sent to the crypto address wallet bc1q...0q2g

- On August 30, 2022, at approximately 7:59pm, J.K. used a CoinFlip ATM at Azara Smoke N Vape at 3658 S. 27th St, Milwaukee, WI 532214 where she purchased 0.10900535 BTC for $2,500 and sent to the crypto address wallet bc1q….0q2g.

- On August 31, 2022, at approximately 11:05am, J.K. used a Crypto Dispensers ATM in Southridge Mall at 5300 S. 76th St, Greendale, WI 53129 where she purchased 0.11249594 BTC for $2,500 and sent to the crypto address wallet bc1q...0q2g

- On August 31, 2022 at approximately 7:42pm, J.K. used a CoinFlip ATM at Azara Smoke N Vape at 3658 S. 27th St, Milwaukee, WI 532214 where she purchased 0.10900535 BTC for $2,050 and sent to the crypto address wallet bc1q….0q2g

18. In total J.K. was instructed to purchase $39,500.00 Bitcoin (1.66769071 BTC). J.K. was instructed to send this BTC to two different bitcoin wallet addresses under false pretenses permanently depriving her of these funds.

CRYPTOCURRENCY TRACING FOR J.K.

19. According to Binance records, all three of J.K.'s Bitcoin purchases and transfers were eventually deposited into Binance wallet **bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h**. On August 30, 2022, the $15,000 was used to obtain .62692697 Bitcoin (BTC). The .62692697 BTC was transferred between four (4) other BTC addresses before being sent to Binance. The first two (2) transfers were the exact amount of .62692697. On the third transfer, the funds were comingled with other funds leading to a transfer of 4.44743256 BTC. On the fourth transfer, the funds were again comingled to total 8.9460459 BTC, which was deposited into Binance wallet **bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h** from the address 18kPX7rbYF8tSs4Jpy5hBnaeFy2T6kG5Y1. Specifically, the transfers were made as follows:

- On August 31, 2022, the second transfer of the .62692697 BTC was transferred from BTC address 1CJvdFdYMmRcUj4o79kruSECiYUav48N35. The transfer to the "1CJvdF" address was the only transfer to that address. Less than 1 minute later from the incoming transfer to the BTC address, the same .62692697 BTC was transferred from the "1CJvdF" address to the BTC address 34ki15tXZtY3xZYeAhXtcm7WpWJPMhEizr ("34kil5"). The was the only transaction occurring at this BTC address.

- On August 31, 2022, less than 1 minute from the previous transaction, the third transfer occurred of the same .62692697 BTC. The BTC that was sent to the "34kil5" address was sent to the BTC address 15E8GMzDk1v7GFs7ZzJsNL4GpDy6751RLk ("15E8GM"). The only transaction occurring within the "15E8GM" address was the transfer of .62692697 BTC from "34kil5." The BTC address "15E8GM" then sent the funds to BTC address

18kPX7rbYF8tSs4Jpy5hBnaeFy2T6kG5Y1 ("18kPX7"), where the funds were comingled to total 4.44743256 BTC.

- On September 1, 2022, the fourth and final transfer occurred between BTC address "18kPX7" and **bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h**. The total amount of the transfer was 8.9460459 BTC. Based on their training and experience, and the investigation to date, case agents are aware that all funds and addresses sent to Binance **bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h** during this transfer were controlled by the same person. Case agents further believe that the funds sent from "18kPX7" were commingled to total 8.9460459 BTC.

20. The BTC deposit into Binance **bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h** occurred on September 1, 2022 at 04:32:31. That same day, at 05:52:20 UTC, the BTC was used to purchase Tether cryptocurrency (USDT). Based on their training and experience, and the investigation to date, case agents believe that once the funds were inside User **ID 78437498** account, the account owner engaged in Over-the-Counter trading within Binance and exchanged the BTC for Tether. Currently, no BTC is visible in the account.

IDENTIFYING THE BINANCE ACCOUNT OF USER 78437498

21. On or about September 6, 2022, law enforcement requested the account information associated with Binance wallet **bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h**. Binance confirmed the addresses existed with Binance and provided the Binance User ID associated with each address. A review of the records showed only one account in **bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h** had available assets. The User **ID 78437498** was identified as having 285,330.50357975 in the crypto currency Tether (USDT) in available assets.

22. According to Binance records, Binance User **ID 78437498** is in the name RAHUL SETH, whose account was registered on or about February 10, 2021, using India passport (passport number: Z6175564). Analysis of the Binance user's account activity for September 1, 2022, shows

a deposit of 4.447443256 BTC into Binance User **ID 78437498** account utilizing a receiving address of **bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h** and transaction hash 3c4747c4d84cdaa5bb743f11804886e3510f8de967f52ceddc880d3eeeac43ff.

23. Based on analysis of IP addresses utilized to access the user's account, the user's account is primarily access utilizing IP addresses that geolocate to India. Based on the user's account information, as well as identity documents and access logs, l.aw enforcement does not believe the individual resides inside the United States.

CONCLUSION

24. Based on the facts and circumstances set forth in this affidavit, I submit that there exists probable cause to believe that approximately **39,500 Tether (USDT), and any other crypto-currency on deposit in Binance Account User ID #78437498, held in the name of RAHUL SETH** are:

- Funds traceable to, and are therefore proceeds of, a wire fraud offense or offenses committed in violation of Title 18, United States Code, Section 1343.
- Funds involved in, or traceable to funds involved in, money laundering offenses, committed in violation of Title 18, United States Code, Sections 1956 and 1957.
- Subject to civil forfeiture under Title 18, United States Code, Sections 981(a)(1)(A), 981(a)(1)(C) and 984, and subject to criminal forfeiture under Title 18, United States Code, Section 981(a)(1)(C); Title 28, United States Code, Section 2461(c); and Title 18, United States Code, Section 982(a)(1); and
- Subject to seizure via a civil seizure warrant under Title 18, United States Code, Section 981(b), and via a criminal seizure warrant under Title 18, United States

Code, Section 982(b)(1) and Title 21, United States Code, Section 853(f).

# # #