DECLARATION OF SPECIAL AGENT LOI H. CAO

I, Loi H. Cao, Special Agent with the Federal Bureau of Investigation ("FBI"), do hereby declare:

Introduction and Agent Background

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been employed with the FBI since October 2008. From November 2014 until the present, I have been assigned to investigate violations of federal law involving a range of white-collar criminal violations. I have completed several computer internet fraud in-service training courses. During these courses, I received training concerning the use of computers, cryptocurrency, Internet Protocol (IP) addresses, and email servers, among other things. I am also a Certified Public Accountant ("CPA") and have been trained in the use of numerous financial computer systems and databases. Over the course of several investigations, I have consulted with other cyber professionals in the law enforcement field regarding the evidentiary value of computers, storage devices, email, and cell phones in conjunction with financial and criminal investigations.

Purpose of this Declaration

2. This Declaration is submitted in support of the Verified Complaint for Forfeiture *In Rem* of Approximately 300 ether ("ETH") held in a privately-hosted wallet ending in D3E8 in the name of Noman Saleem (Asset ID 24-FBI-001570), seized on or about December 6, 2023. (the "Defendant Property").

3. I submit that there are sufficient facts to support a reasonable belief that the Defendant Property constitutes proceeds traceable to a violation of 18 U.S.C. § 1343 (wire fraud), and thus is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

Cryptocurrencies and Transaction Analysis

4. Ether (ETH) is a "cryptocurrency," also known as "virtual currency." Cryptocurrencies are not tied to any nation's fiat currency. The owner of cryptocurrency is assigned a mathematical encryption key pair, consisting of a "public key" and a "private key," with which to control the currency they own. The public key, also known as an "address," is visible to the public, and allows members of the public to verify the owner of virtual currency and other information. Public keys are also used to send and receive cryptocurrency. The private key, also known as a "secret key," is essentially a password used to execute cryptocurrency transactions. Secret keys are typically only shared with the owner of the public key.

5. A "wallet"[1] can hold multiple public keys for a user, and an "account" can hold multiple wallets for a user.

6. Cryptocurrency transactions can have multiple inputs and multiple outputs. While the ownership of any particular public key or wallet can be anonymous, all transactions of cryptocurrencies are recorded on a "blockchain," which is a series of "blocks" of transactions that establishes a verifiable, transparent record of the movement of virtual currency. Blockchains in this context are viewable by the public—they show all transactions, but do not reflect who owns a particular address. As cryptocurrency transactions are processed, they are assigned a unique identifier on the blockchain called a transaction hash.

7. A seed phrase, also known as a recovery phrase, is a group of random words that were generated when the owner set up their cryptocurrency wallet. Seed phrases cannot be changed nor customized later. The seed phrase serves as a master key for the owner of the wallet in case private keys are lost and the owner is not able to access their cryptocurrency. Seed phrases

[1] A cryptocurrency "wallet" is a device, physical medium, program, or a service which stores the public and/or private keys for cryptocurrency transactions.

are different from private keys in that they give access to all cryptocurrency contained in a wallet not just specific cryptocurrency. Typically, seed phrases are a list of 12 to 24 simple words from the dictionary. The standard method for seed phrases is called BIP-39, which is short for Bitcoin Improvement Proposal 39. BIP-39 was introduced in 2013 with a list of 2,048 words that could be used in seed phrases. There are 2,048 to the power of 12 (more than a decillion) possible seed phrase combinations. With such a large number, the odds of someone guessing the phrase are almost zero. In general, if a private key is comparable to an online account password, a seed phrase is like the security questions a user might answer when the user has lost or forgotten a password.

8. When law enforcement has obtained the seed phrase for a wallet, law enforcement may be able to use the seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the wallet to a law enforcement-controlled wallet. Law enforcement would transfer the available account balances as seized assets out of the wallets controlled by a target and into custody in wallets controlled by law enforcement.

Investigation Background

9. The FBI is investigating a cryptocurrency (crypto) staking awards scheme. Crypto staking involves locking up cryptocurrency holdings for a period of time to earn interest or rewards. Staking allows for certain blockchain networks to verify crypto transactions. Crypto staking is typically accomplished with groups of people or "pools." It allows the participants to earn passive income on their holdings, typically between 5 and 20 percent. In the situation under investigation, the staking scheme involves impersonating a popular online crypto 'influencer,' gaining the trust of the victim and finally convincing the victim to send crypto to virtual wallets controlled by the fraudster. Once the fraudster has control of the victim's crypto, all communications cease with the victim and the victim's crypto is not returned.

10. A victim whose initials are AW ("Victim A") is a resident of Olney, Maryland and is an amateur crypto investor. Victim A followed a popular crypto influencer called BitBoy Crypto ("BitBoy"), whose real name is Ben Armstrong ("Armstrong"). Victim A communicated directly with the subject of this investigation through various chat rooms on the messaging apps Discord and Telegram that Victim A believed were facilitated by Armstrong.

Telegram Communications

11. Through the chat rooms and direct communications, Victim A was convinced he was participating in a non-fraudulent staking awards program.

12. On December 28, 2020, Victim A sent the following Telegram message to the subject: "Hey BitBoy! I'm new to the VIP Squad. I saw you're the marketing advisor for YF-Dai. I know money right now is flowing from Bitcoin into the large cap altcoins but I was wondering if you're still bullish on YF-Dai for 2021 . . ." The subject replied, "I would focus on coins that are more established at the moment." It is evident Victim A incorrectly believed he was communicating with "BitBoy" as he initially stated "Hey BitBoy!" The subject (later identified as **NOMAN SALEEM**) did not deny that he was BitBoy, and advised Victim A to not invest in YF-Dai.

13. On January 14, 2021, Victim A texted the subject, "Watched your interview with "Ivan on Tech" and have to give a shout out for the great content . . . " The subject responded, "Ty." In this text exchange your Declarant believes Victim A was describing an interview in which "BitBoy" was interviewed on a YouTube channel called "Ivan on Tech." The subject responded "Ty," short for thank you, which based on your Affiant's training, knowledge and experience, further pushed the incorrect narrative that the subject was "BitBoy Crypto."

14. On February 11, 2021, the subject offered Victim A an opportunity to "stake" ETH. The subject texted the following to Victim A: "Eth 2 staking is what we do that gives members;

10% per 30 days; 15% per 60 days; 20% per 90 days." Victim A then responded, "Those are pretty awesome numbers. How do I participate?"

15. The subject then directed Victim A to send his crypto to specified crypto wallets. Between December 2020 (when Victim A paid a fee to join a related Telegram chat group) and March 2021, Victim A sent approximately $675,000 in ETH, OCEAN, ATOM, EWT and XTZ cryptocurrencies ("coins") to the subject. The subject impersonating BitBoy Crypto told Victim A that the funds would be returned after a three to four month staking period, during which time the funds would appreciate substantially in value. After Victim A sent 300 ETH, the subject texted Victim A, "Yah let's wait for it to arrive then we can stake it for 90 days right?" Victim A responded, "90 days please." The subject confirmed, "90 days 20%."

16. After the staking period passed, Victim A sent a message asking for his funds to be returned. The subject did not return the funds, but instead removed Victim A from the Telegram group and ceased all communications with Victim A. Around July 2021, Victim A tried to access the Telegram group, and an automated response appeared that read, "Sorry, this channel is private." On July 23, 2021, Victim A emailed the subject at the email address DollarVigilanteAdmin@protonmail.com regarding the inability to access the trading group. The email address DollarVigilanteAdmin@protonmail.com was an email address Victim A had successfully used to contact the subject posing as BitBoy in the past. In response, Victim A received an automated email message that read: "Your message wasn't delivered to DollarVigilanteAdmin@protonmail.com because the address couldn't be found, or is unable to receive mail."

18. After Victim A realized he had become a victim, he contacted Armstrong's (the real "BitBoy Crypto") social media team and was informed that Armstrong did not run the Telegram group Victim A had used to communicate with the subject. Victim A was also informed

that Armstrong's team was aware of numerous fraud schemes that involved the unauthorized use of Armstrong's name and online personality, BitBoy Crypto.

19. Over the course of the investigation, Victim A provided screenshots of the transaction histories and details for certain transactions from his various crypto accounts. The screenshots showed that Victim A transferred approximately $675,000 U.S. dollars' worth of various virtual currencies during the course of the fraud scheme, including one transaction of 300 ETH from Victim A's account at the Celsius Network exchange.

20. Investigators used blockchain analytics software to trace Victim A's crypto as depicted in the table:

DATE	AMOUNT[2]	SOURCE	DESTINATION
2/18/2021	300 ETH	Victim A (Celsius Network)	"Wallet 1": 0x4a6f894a89D70b7f826a593a75e939f8a7BaEb64
3/6/2021	334.6 ETH	Wallet 1	"Wallet 2": 0x390825dcB6344aD9571A94773d059e62f718D3E8

Between February 18 and March 6, 2021, the balance in Wallet 1 never dropped below 300 ETH. On March 6, 2021, Victim A's 300 ETH was sent as part of the above transaction from Wallet 1 to Wallet 2. Neither Wallet 1 nor Wallet 2 were owned or controlled by Victim A. Victim A transferred his crypto to Wallet 1 pursuant to instructions the subject provided to participate in the abovementioned staking scheme.

21. Through the use of commercially available tools, law enforcement conducted a tracing analysis on Wallet 2. The tracing analysis of Wallet 2 identified an additional deposit of crypto from Victim A into Wallet 2 on or about March 2, 2021. Wallet 2 then sent Victim A's additional crypto to an account held at the exchange KuCoin (the "KuCoin Account"). In response

[2] Unless indicated otherwise, all virtual currency amounts have been rounded to the nearest 0.1.

to an official records request, KuCoin provided customer information associated with that account, which included the following information:

USER ID	23719060
EMAIL	NOMY231@GMAIL.COM
REGISTRATION TIME	1/10/2018 2:09:09

22. Information obtained from Google, Inc. shows that the email account nomy231@gmail is controlled and operated by Noman Saleem (**SALEEM**). Usage logs for the KuCoin Account indicate the user accessed the account from an Android device and Chrome web browser from the cities of Elmhurst, Jackson Heights, and Brooklyn, in the State of New York.

23. Records obtained from Consenys, which is a private blockchain software company, revealed IP address 98.14.50.207 was used to transfer Victim A funds out of Wallet 2 and into the KuCoin Account. In August 2022, subscriber information was obtained from internet provider Charter Communications regarding the use of IP address 98.14.50.207 in connection with that transaction. The subscriber name on the IP address was Noorali Saleem, however the email address listed was NOMY231@GMAIL.COM, which is also listed as the subscriber email address for the KuCoin Account described above. Noorali Saleem is the father of the subject, **NOMAN SALEEM**. Charter Communications records also listed the service location as 8345 Broadway Apt. 526, which is in Elmhurst, New York, and the billing address as 44 Mill Lane, Levittown, New York (**SALEEM**'s residence).

24. In furtherance of the investigation into the crypto staking scheme, on April 7, 2022, your Declarant obtained a search warrant for the personal email account of target **NOMAN SALEEM**, Nomy231@gmail.com, maintained through Google, Inc. That search revealed **SALEEM** subscribed to a newsletter called The Dollar Vigilante, which was run by Jeff Berwick. The newsletter was sent from "Jeff Berwick noreply@dollarvigilante.com," which closely

resembles the email address DollarVigilanteAdmin@protonmail.com, which Victim A had used to contact the subject before July 23, 2021. Based on your Declarant's training, knowledge and experience, fraudsters will often mimic or copy legitimate business names and email addresses in this manner to further their scheme.

25. **SALEEM** is a resident of New York State and works as a Revenue Cycles Specialist for a healthcare organization. **SALEEM**'s Elmhurst, New York address listed above matches the locations from where the KuCoin account described above was accessed.

Related Search Warrants

26. On November 3, 2023, your Declarant obtained search warrants authorized by U.S. Magistrate Judge Steven L. Tiscione for the Eastern District of New York, for **SALEEM**'s residence, person, and safe deposit box (collectively the "Search Warrants"). **SALEEM**'s residence is located at 44 Mill Lane, Levittown, New York and Safe Deposit Box #557 is located at TD Bank – 999 Old Country Road, Westbury, NY 11590.

27. On November 8, 2023, FBI agents executed a search of **SALEEM**'s Mill Lane residence and seized numerous items of evidence, including a black notebook. The notebook was located in **SALEEM**'s bedroom at the time of the search. In the notebook, the phrase "Dollar Vigilante log in" was handwritten, and your Declarant knows "The Dollar Vigilante" was a moniker **SALEEM** used to perpetrate his scheme on Victim A. Written directly below "Dollar Vigilante log in" was the email address nomy231@gmail.com along with the notation "pw" and a string of characters that appeared to be the account password. Your Declarant knows through information obtained from Google, Inc., the email account nomy231@gmail.com is controlled and operated by **SALEEM**.

28. A further review of the notebook revealed names of cryptocurrency wallets as well as over a dozen batches of seed phrases. Seed phrases, described in more detail above, can be used

to restore cryptocurrency wallets to access cryptocurrency and therefore tend to be closely guarded by wallet owners.

29. Investigators, using cryptocurrency wallet software, were able to set up offline cryptocurrency wallets which mirrored known wallets connected to **SALEEM**. Using the 12 seed phrases listed as "Trust Wallet" in **SALEEM**'s notebook, investigators were able to determine the seed phrases were associated with Wallet 2 and if the phrases were used while online, would unlock the wallet and give investigators access to any cryptocurrency available in the wallet.

30. On or about December 6, 2023, the Honorable J. Mark Coulson, U.S. Magistrate Judge for the District of Maryland, signed a seizure warrant authorizing the government to seize the approximately 300 ETH from Wallet 2.

31. Later on or about December 6, 2023, acting on the above warrant, an FBI computer scientist – in the presence of FBI special agents and using the seed phrase identified above – transferred the abovementioned approximately 300 ETH from Wallet 2 to an FBI-controlled custody wallet.

32. Based on your Declarant's training, knowledge, and experience, the owner of the Wallet 2 is **SALEEM** and the approximately 300 ETH transferred from Wallet 2 into FBI custody were the proceeds of the fraud scheme perpetrated by **SALEEM** on Victim A.

CONCLUSION

33. Based on the forgoing, I submit that there is probable cause to believe that the approximately 300 ETH are proceeds of, or traceable to proceeds of violations of 18 U.S.C. §1343 (Wire Fraud), and therefore subject to civil forfeiture, pursuant to 18 U.S.C. § 981(a)(1)(C).

LOI H. CAO
SPECIAL AGENT, FBI