

DECLARATION OF SENIOR SPECIAL AGENT TIMOTHY WILLIAMS

I, Timothy Williams, Senior Special Agent (SSA) of the United States Secret Service (USSS), assigned to the Raleigh Resident Office of the USSS, pursuant to 28 U.S.C. § 1746 and the laws of the United States, hereby declare under penalty of perjury that the following is true and correct to the best of my knowledge and belief:

INTRODUCTION

1. This declaration is made in support of a complaint to forfeit funds previously seized from a virtual currency (VC) address [hereafter referred to as the "Subject Address"]. This address contained proceeds of a wire fraud scheme, whereby one or more criminal fraudsters posed as technical support from a cryptocurrency exchange and induced a victim in the Eastern District of North Carolina, identified herein as L.S., to send money to a VC wallet controlled by the fraudsters. Once they received the VC, it was transferred to other VC addresses, converted to a different form of VC, and ultimately reconsolidated in a single address, which was subsequently frozen by the USSS. The USSS previously obtained a seizure warrant (Case No. 5:24-MJ-2581-RN) pursuant to 18 U.S.C. § 981(b) to bring traceable proceeds into government custody and now submit this declaration to support the funds' forfeiture

DECLARANT'S BACKGROUND AND EXPERTISE

2. I am a Senior Special Agent (SSA) with the United States Secret Service (USSS) assigned to the Raleigh (NC) Resident Office. I have been employed with the USSS as a Special Agent since June 2007. I have completed extensive training at both the Criminal Investigator Training Program at the Federal Law Enforcement Training Center, Glynco, GA and the Special Agent Training Course at the USSS training facility located in Beltsville, MD. This training included instruction in general law enforcement and criminal investigations to include violations of Title

18, United States Code, section 1343 (Wire Fraud). During my time with the Secret Service, I have conducted numerous financial crime investigations involving cryptocurrency and other financial instruments.

PURPOSE OF THE DECLARATION

3. I make this declaration in support of the civil forfeiture of the proceeds of a criminal scheme to defraud L.S. executed in violation of 18 U.S.C. §§ 1343 and 1349. Specifically, this declaration supports the civil forfeiture of the following assets that were previously seized and brought into government custody on January 16, 2025:

- a. 316,608.629433 USDT virtual currency (formerly held in address 0x6f9ede43ee7DA8C1ADF4A07a562D5720b871960D)

4. As explained below, the foregoing funds represent traceable criminal proceeds, which were derived from a criminal fraud scheme that successfully defrauded L.S. by impersonating a legitimate cryptocurrency exchange and inducing him to transfer VC to a wallet controlled by the fraudsters.

BACKGROUND OF CRYPTOCURRENCY

5. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

- a. *Cryptocurrency and Blockchain Generally*: Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Tether, USD Coin, and DAI. Each unit of cryptocurrency is often referred to as a “coin” or “token.” In general, most

cryptocurrencies are considered fungible assets. For example, Bitcoin is considered fungible because each unit of Bitcoin is equivalent to any other unit, meaning they have the same quality and functionality. Regardless of when a unit of Bitcoin was issued (“mined”), all Bitcoin units are part of the same blockchain and have the same functionality. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Users of cryptocurrency use public and private keys to transfer cryptocurrency from one person or place to another. A public key is typically a set of numbers and/or letters that a cryptocurrency user shares with other users to engage in a transaction in cryptocurrency, whereas a private key is typically a set of numbers and/or letters that the user of an account maintains privately to access his or her cryptocurrency. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. As such, most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.¹ Although many cryptocurrencies are or purport to be pseudonymous, often law enforcement and currency exchangers can use the blockchain to analyze transactions in cryptocurrency, identify individuals who are using cryptocurrency platforms for

¹ Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

illicit purposes, and trace fraud proceeds from victims to one or more exchanges or wallets.

- b. *Wallets*: Cryptocurrency is often stored in a virtual account called a wallet, which can exist in, among other forms, an external computer device, a computer, on an application, or online. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. Access to a wallet and the cryptocurrency therein is typically protected by a password only known to the owner or user of the wallet. Wallets can be either “custodial” or “non-custodial” (also referred to as “centralized/decentralized” or “hosted/non-hosted”). In the case of a non-custodial wallet, the owner of the wallet has sole control of the wallet’s private keys, which enable access to the wallet and any funds contained therein. With a custodial wallet, another party controls the private keys to the wallet. This is usually a cryptocurrency exchange, and the relationship between the exchange and the customer can be considered analogous to the relationship between a traditional bank and its customers, where the bank securely maintains funds deposited by a bank customer.
- c. *Seed phrase/Recovery phrase*: A seed phrase or recovery phrase is a sequence of random words, usually 12 or 24, that stores the data required to access or recover cryptocurrency on blockchains or crypto wallets. Most cryptocurrency wallets will automatically generate a seed phrase during the establishment of the wallet. The user is encouraged to write down the phrase or print it out and keep it in a safe location. In the event access to the wallet is lost, such as in the case of a phone

being lost or damaged, the user can reinstall the wallet app or software and regain access to their cryptocurrency by entering the seed phrase.

- d. *Exchanges/Exchangers*: Virtual currency “exchangers” and “exchanges” (also referred to as a “Virtual Asset Service Provider” [VASP]), such as Binance, Coinbase, Gemini, Kraken, and Crypto.com, are individuals or companies that exchange virtual currency for other currencies, including U.S. dollars. Exchanges facilitate the purchase, sale, and transfer of a variety of digital currencies.
- e. *Centralized/Decentralized Exchanges*: Centralized exchanges generally maintain a custodial role for the wallets of its customers, and function as trusted intermediaries in cryptocurrency transactions. Decentralized exchanges consist of peer-to-peer marketplaces where users can trade cryptocurrencies in a non-custodial manner, without the need for an intermediary to facilitate the transfer and custody of funds. Decentralized exchanges are often used to trade, or “swap”, one type of cryptocurrency for another, for which the user pays a transaction fee. Centralized exchanges that conduct business in the United States are required to verify their customers’ identities and abide by Know-Your-Customer/Anti-Money Laundering (KYC/AML) regulations.
- f. *Tether*: Tether, widely known as “USDT,” is a blockchain-based cryptocurrency whose tokens in circulation are backed by an equivalent amount of U.S. dollars, making it what is known as a “stablecoin.” USDT is issued by Tether Ltd., a company headquartered in Hong Kong. Tether is connected to Bitfinex, a cryptocurrency exchange registered in the British Virgin Islands. Tether can be

used on multiple blockchains, with two of the most popular being Ethereum and Tron.

g. Like other virtual currencies, USDT is sent to and received from USDT “addresses.” A USDT address is somewhat analogous to a bank account number, and is represented as a 26-to 35-character-long case-sensitive string of letters and numbers. Users can operate multiple USDT addresses at any given time, with the possibility of using a unique USDT address for every transaction. Although the identity of a USDT address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can sometimes be used to identify the owner of a particular USDT address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity. Unlike bitcoin, one of the most popular cryptocurrencies in use today, USDT is “centralized”, meaning that it is issued and controlled by a governing body. Most other cryptocurrencies are “decentralized” and have no such governing body.

FACTS SUPPORTING FORFEITURE

6. This case concerns a fraud scheme to steal cryptocurrency from a victim, L.S., residing in the Eastern District of North Carolina. The scheme was perpetrated through an unsolicited phone call in which the fraudsters impersonated security experts from the Coinbase cryptocurrency exchange.

7. L.S. is an 84-year old resident of Chocowinity, NC. He began investing in cryptocurrency in 2020 by opening an account at the Gemini cryptocurrency exchange and purchasing three different types of cryptocurrency which he stored in the account. These consisted of Bitcoin

(BTC), Ether (ETH), and ChainLink (LINK). After purchasing the cryptocurrency over a period of several months in 2020, L.S. maintained the funds in his Gemini account and did not conduct further trades or movement of these funds. On June 4, 2024, the day the scam began, the total value of L.S.'s Gemini account was approximately \$322,690.

8. On June 4, 2024, L.S. received a phone call on his personal cell phone from an unrecognized phone number with a 252 area code, which covers a large part of eastern North Carolina. The caller told L.S. that his name was "Victor Jusino" and that he was a security analyst with Coinbase, a cryptocurrency exchange based in San Francisco, CA. Jusino told L.S. that criminals had been attempting to access L.S.'s cryptocurrency account in order to steal the funds contained in it. During the discussion, Jusino added another person to the call who said his name was "Nishant Gupta", a Security Expert at Coinbase. Jusino and Gupta informed L.S. that there had been multiple attempts to access L.S.'s account and that he needed to improve the security on his account, which they offered to assist with. After this initial call, which lasted over two hours, Gupta called back and spoke to L.S. two additional times on the same day. These subsequent calls consisted of Gupta asking questions about his cryptocurrency accounts and the security measures in place to protect them. At some point during the calls, Gupta asked L.S. to install an app on his iPhone called "HelpDesk Host." Gupta claimed that this app would allow him to provide improved support to L.S. and improve their communication, but that he would not be able to see anything on L.S.'s screen. However, the sole purpose of the HelpDesk Host app is to allow someone to remotely view the screen that the app is installed on – the legitimate purpose of this app is for tech support personnel to view a customer's screen and assist them. Therefore, this app actually allowed Gupta to view everything on L.S.'s phone in real time, which L.S. was not aware of. L.S.

installed the app and followed Gupta's instructions to begin a remote session, which connected the phone to Gupta and allowed him to view the screen.

9. After a lengthy discussion of L.S.'s cryptocurrency accounts and holdings, Gupta reiterated to L.S. that his Gemini account was vulnerable, and recommended that he set up a new self-hosted wallet to hold his cryptocurrency. Gupta recommended the Exodus app, which is a legitimate and well-known self-hosted crypto wallet that would not have raised suspicions if L.S. researched it. Gupta walked L.S. through each step of downloading the app on his phone, setting up the wallet, and then transferring all of L.S.'s cryptocurrency from his Gemini account to the Exodus wallet. Less than one hour after these transfers were completed, all of the cryptocurrency in L.S.'s Exodus wallet was transferred, without L.S.'s knowledge or authorization, to other cryptocurrency addresses not connected to the Exodus wallet. It is not known for certain how the suspects accessed L.S.'s Exodus wallet in order to conduct this theft, but the most likely possibility is that the suspects were able to view the wallet's "seed phrase" during the creation of the wallet on L.S.'s phone (due to the suspects' use of the HelpDesk Host app). The suspects would then have been able to use the seed phrase to reconstitute the wallet on their own device and thereby gain access to all the funds in the wallet, allowing them to transfer the cryptocurrency to addresses under their full control.

10. Once L.S. realized that all of the cryptocurrency in his Exodus wallet was gone, he contacted Gupta and had another phone conversation with him. Gupta assured L.S. that his funds were safe. However, L.S. became suspicious and began to contact law enforcement on the morning of June 5, 2024. \

Tracing of Victim Funds to the Subject Address

11. Based on information provided by L.S. and verified using publicly available blockchain data, the cryptocurrency transactions described above were identified and traced. The subsequent movement of the funds was then traced, which led to the Subject Address. As there were three different types of cryptocurrency stolen from L.S.'s account (BTC, ETH, and LINK), the movement of each of these types is described separately below, although each of them ultimately end up in the Subject Address. The traces were conducted using the Last-In-First-Out accounting principle – meaning that the most recently deposited items are recorded as the next withdrawal. In some cases, the cryptocurrency amounts noted may not add up to the initial amount that was stated. This is due to the fee that each blockchain charges for a transaction, which will reduce the amount of cryptocurrency sent by a small amount. For clarity, all cryptocurrency addresses have been shortened to the first eight characters.

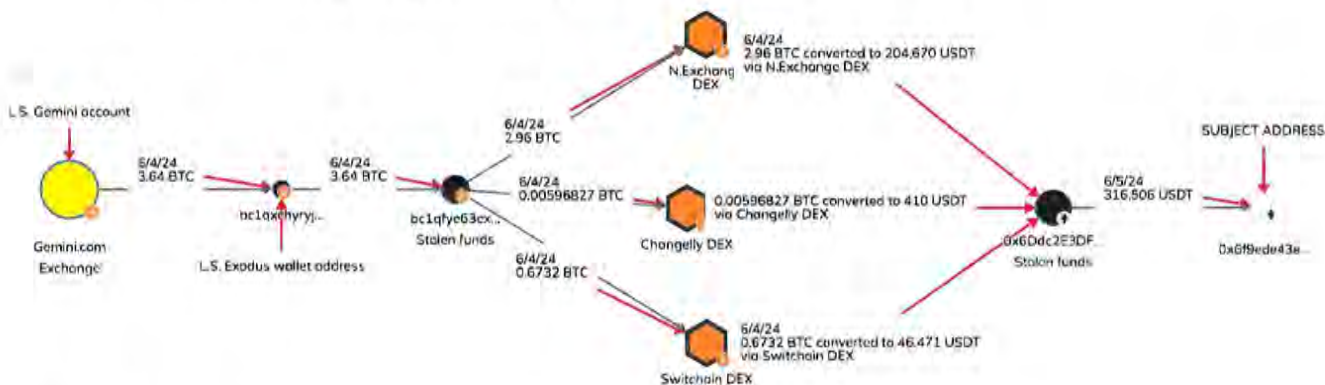
12. Bitcoin (BTC):

- a. On June 4, 2024, L.S. sent 3.64276527 BTC from his Gemini account to his Exodus wallet address of bc1qxchy. Later on June 4, 3.64276527 BTC was sent from his Exodus wallet to BTC address bc1qfy6. This address is not part of L.S.'s Exodus wallet and is not an address he had control over.
- b. Continuing on June 4, all of the BTC was sent to three decentralized exchanges (DEX) where it was converted to USDT. 2.96336207 BTC was sent to the N.Exchange DEX where it was converted to 204,670 USDT and sent to address 0x6Ddc2E. 0.6732469 BTC was sent to the Switchchain DEX where it was converted to 46,471 USDT and sent to address 0x6Ddc2E. 0.00596827 BTC was sent to the

Changelly DEX where it was converted to 410 USDT and sent to address 0x6Ddc2E.

c. On June 5, 2024, all of the USDT described above was sent as part of a 316,506 USDT transaction to address 0x6f9ede (Subject Address).

d. The following is a graphical representation of these transactions:



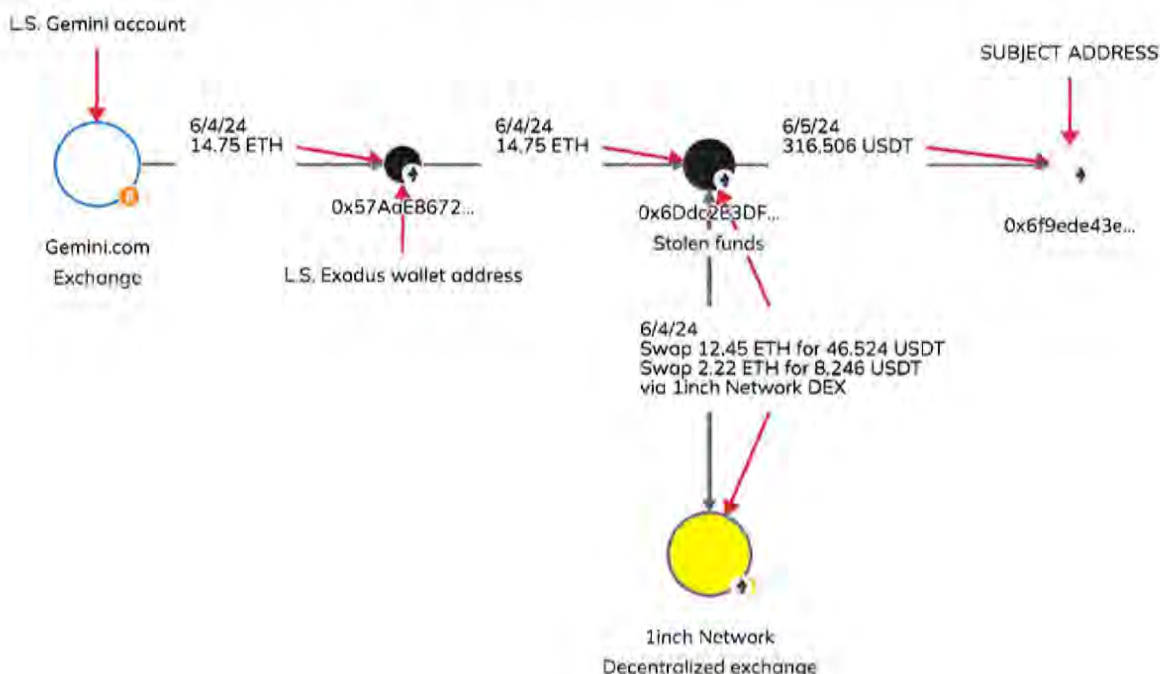
13. Ether (ETH):

a. On June 4, 2024, L.S. sent 14.75912659623818115 ETH from his Gemini account to his Exodus wallet address of 0x57AaE8. Later on June 4, 14.758143968950455648 ETH was sent from his Exodus wallet to ETH address 0x6Ddc2E. This address is not part of L.S.'s Exodus wallet and is not an address he had control over.

b. Continuing on June 4, all of the ETH was sent to the 1inch Network DEX where it was converted to USDT. 12.45194987 ETH was converted to 46,524 USDT and sent back to address 0x6Ddc2E. 2.228971164395482314 ETH was converted to 8,246 USDT and sent back to address 0x6Ddc2E.

c. On June 5, 2024, all of the USDT described above was sent as part of a 316,506 USDT transaction to address 0x6f9ede (Subject Address)

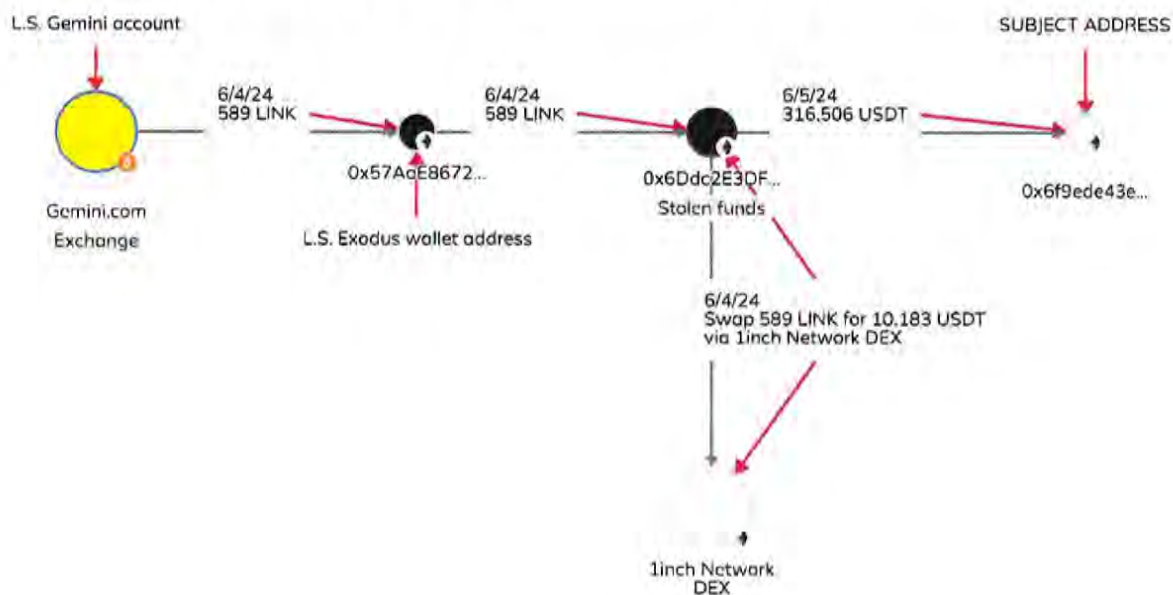
d. The following is a graphical representation of these transactions:



14. ChainLink (LINK):

- On June 4, 2024, L.S. sent 589.465590462434152704 LINK from his Gemini account to his Exodus wallet address of 0x57AaE8. Later on June 4, 589.465590462434152704 LINK was sent from his Exodus wallet to address 0x6Ddc2E. This address is not part of L.S.'s Exodus wallet and is not an address he had control over.
- Continuing on June 4, all 589.465590462434152704 LINK was sent to the 1inch Network DEX where it was converted to 10,183 USDT and then sent back to address 0x6Ddc2E.
- On June 5, 2024, the USDT described above was sent as part of a 316,506 USDT transaction to address 0x6f9ede (Subject Address)

d. The following is a graphical representation of these transactions:

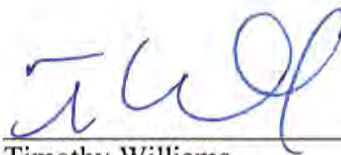


CONCLUSION

15. Based on information derived from the foregoing investigation, there is probable cause to conclude that the 316,608.629433 USDT virtual currency constitutes the proceeds of a wire fraud scheme in violation of Title 18, United States Code, Sections 1343 and 1349 (wire fraud and conspiracy to commit wire fraud) and is therefore forfeitable to the United States pursuant to 18 U.S.C. § 981(a)(1)(C).

16. The foregoing facts are furthermore sufficient to support a reasonable belief that the defendant property is forfeitable to the United States pursuant to 18 U.S.C. § 981(a)(1)(C).

Executed this 11th day of April, 2025.



Timothy Williams
Senior Special Agent
United States Secret Service