EXHIBIT A

AFFIDAVIT OF GARRETT FITZGERALD JR.

I, Garrett Fitzgerald Jr., being duly sworn state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Cyber Special Agent ("CSA") with the United States Secret Service ("USSS") and have been employed as such since March 13, 2019. Prior to becoming a Cyber Special Agent, I was employed with the United States Secret Service as a Special Agent for approximately 4 years. I attended the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia and the United States Secret Service Special Agent Training Course at the James J. Rowley Training Center in Beltsville, Maryland. I am currently assigned to the Boston Field Office where I conduct financial crime investigations, including investigations of violations of 18 U.S.C. § 1343 (Wire Fraud). In connection with these investigations, I have conducted or participated in numerous field interviews of suspects and witnesses, electronic and physical surveillance, researched bank account documents and documents relating to the wiring of monies between banks. Through my training and experience, I have become familiar with various financial frauds and schemes such as bank frauds, wire frauds and mail frauds. Further, as a federal agent, I am authorized to execute warrants issued under the authority of the United States.

PURPOSE OF AFFIDAVIT

2. I submit this affidavit in support of a Verified Complaint for Forfeiture *in Rem* against the following asset:

a. 73,586.17 USDT[1] seized from BINANCE account with user ID ending in 7402 (the "Defendant Property").

[1] "USDT" is the abbreviation for Tether, a blockchain-based cryptocurrency whose tokens operate as a stablecoin, indicating that each token is equivalent in value to one U.S. dollar.

3. As set forth below, there is probable cause to believe that the Defendant Property represents proceeds traceable to a violation of 18 U.S.C. § 1343 (Wire Fraud) and is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C). Pursuant to 18 U.S.C. § 1961(1), as incorporated by 18 U.S.C. § 1956(7)(A), violations of 18 U.S.C. § 1343 are a specified unlawful activity.

4. This affidavit is based on my personal knowledge, information provided by other law enforcement offices and government employees, and information gathered during this investigation including interviews of witnesses, the review of documents, and conversations with other law enforcement officers. This affidavit is not intended to set forth all of the information that I have learned during this investigation but includes only the information necessary to establish probable cause for the forfeiture of the Defendant Property.

PROCEDURAL HISTORY

5. On March 10, 2022, the government sought, and was granted, a seizure warrant for the Defendant Property. The warrant was executed via email to case@binance.com that same day. On May 4, 2022, Binance transferred the Defendant Property to a USSS-controlled cryptocurrency wallet.

BACKGROUND ON CRYPTOCURRENCY

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

7. 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.[2] Examples of

[2] Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or

cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries.

8. 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. 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.[3] Cryptocurrency is not illegal in the United States.

9. Tether ("USDT") is an alternative type of cryptocurrency or altcoin token. Payments or transfers of value made with Tether are recorded in the blockchain network, but unlike decentralized cryptocurrencies like bitcoin, Tether has some anatomical features of centralization. One centralized feature is that Tether is a Stablecoin or a fiat- collateralized token that is backed by fiat currencies, or currencies issued by governments like the dollar and euro. Tether is backed with a matching one to one fiat amount, making it much less violate than its counterpart, Bitcoin.

10. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number,

---

Japanese Yen.

[3] 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.

and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26–36 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

11. Although cryptocurrencies such as Bitcoin and Tether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering, and is an oft-used means of payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transactions.

12. Binance Capital Management Co., Ltd. ("BINANCE") is a Cryptocurrency exchange and custodian that allows users to buy, sell and store digital assets. They hold a Money Service Business Registration in the United States. Their registration shows an address of Level 3, Melita Court, Triq Giuseppe Cali, Ta'Xbiex XBX 1420, MALTA.

PROBABLE CAUSE

13. As set forth below, there is probable cause to believe that the Defendant Property is proceeds obtained through violations of 18 U.S.C. § 1343 (Wire Fraud).

The Scheme to Defraud

14. On January 26, 2022, W.Q. of Brookline, Massachusetts contacted USSS Boston Field Office providing information indicating she was the victim of a cryptocurrency trading

scam. Between January 26. 2022 and February 28, 2022, I communicated with W.Q. via telephone and email.

15. W.Q. explained she was initially contacted on October 20, 2021 by an individual named "Mingfeng QIAN" through a LinkedIn request she received via email. A subsequent search of LinkedIn was conducted for the individual who contacted W.Q. with negative results.

16. After connecting on LinkedIn, the individual or individuals purporting to be QIAN then began communicating with W.Q. through two messaging applications, Whatsapp and Line, installed on W.Q.'s iPhone 11 mobile telephone. W.Q. received communications on these messaging applications from QIAN utilizing a specific phone number. W.Q. stated all messages with QIAN were typed in Chinese. W.Q. stated she understood Chinese and spoke Chinese as her native language.

17. QIAN told W.Q. that cryptocurrency trading was an easy way to make profits. W.Q. stated she had never purchased or sold cryptocurrencies before she began communicating with QIAN.

18. W.Q. provided investigators with screenshots of her communications with QIAN. The screenshots show messages typed in a language appearing to be Chinese and W.Q. provided translation to English. In one message on October 27, 2021, translated by W.Q., QIAN told her: "Market is looking good recently. 15-20% profit is not a problem if you follow my instructions." In a November 11, 2021 message, QIAN said: "I have been doing this for 7 years, never lost money."

19. As evidenced by W.Q.'s messages and statements, between November 12, 2021 and January 19, 2022, the individual or individuals identifying themselves as QIAN instructed W.Q. to transfer approximately 303,712.96 USDT to cryptocurrency wallets. W.Q. stated she

followed QIAN's instructions and opened an account at OKEX cryptocurrency exchange (OKEX rebranded to the name OKX in January of 2022).

20. W.Q. translated an additional screenshot of a message from QIAN on November 12, 2021: "you need to download a trading platform TMS." This screenshot also showed the website URL of "www.tmsfin.com".

21. W.Q. stated that she was unable to find an application named "TMS" after searching within the Apple App Store, and instead clicked on the website URL "www.tmsfin.com" from QIAN's message. W.Q. stated this opened a web browser on her iPhone 11 that navigated to the website URL www.tmsfin.com. From this website, W.Q. clicked a link that stated, "APPLE APP STORE". Following this, W.Q. stated she followed on screen instructions that installed an application titled "TMS" on her iPhone 11.

22. W.Q. provided a translated screenshot of a message from QIAN on November 20, 2021: "There will be good opportunities next week, if we add more capital, we can make more profit, hundreds of thousands of dollars is not a problem."

23. W.Q. stated that between November 12, 2021 and January 19, 2022, she bought USDT and RMB[4] cryptocurrencies on OKEX cryptocurrency exchange and sent nine (9) cryptocurrency transfers totaling 303,712.96 USDT from her account at OKEX to the destination wallet addresses detailed below.

24. I reviewed the transfer details provided by W.Q. and was able to verify these nine (9) cryptocurrency transfers totaling 303,712.96 USDT transferred out of the OKEX cryptocurrency platform.

[4] RMB is a digital form of Chinese renminbi, or yuan.

25. W.Q. conducted the first eight (8) cryptocurrency transfers from her account at OKEX under the direction of QIAN and instructions she received from the TMS application on her iPhone 11.

26. W.Q. stated that on January 7, 2022, she tried to withdraw money from the TMS application, but had received a message from this application stating she needed to contact "Tmsfin.com" customer service. On this date, she utilized the TMS application on her iPhone 11 to communicate with "Tmsfin.com" customer service and was instructed she needed to pay tax on earnings in her account. These instructions caused W.Q. to make the final (of 9) transfers of USDT from her account at OKEX to the destination wallet address provided by "Tmsfin.com" customer service. W.Q. made this transfer, but was still unable to withdraw any money from the TMS application.

27. W.Q. provided screenshots of the TMS application on her iPhone 11 appearing to show a cryptocurrency portfolio, including a cryptocurrency deposit history and trading history. Screenshots provided by W.Q. also appeared to indicate gains and losses of cryptocurrency portfolio value.

28. I conducted a thorough open-source search for "www.tmsfin.com" and identified the website from which W.Q. indicated she visited to download the TMS application onto her iPhone 11. Based on my training and experience, as well as conversations with other investigators familiar with cryptocurrency platforms, I would expect a legitimate cryptocurrency platform website to display clearly outlined platform policies, company contact information, information regarding the platform's creation, company staff information, along with access for desktop and mobile computing.

29. Further examination of the website identified several discrepancies, which based on my training and experience, indicate that this website does not appear to be a legitimate cryptocurrency platform. These discrepancies include the following:

a. When navigating to this website utilizing a Microsoft Edge web browser, I received a security warning stating "This site has been reported as unsafe".

b. When navigating to this website, the user is instructed to click a link titled "APPLE APP STORE" and are prompted to open a file titled: tms-2021100801.mobileconfig. The user also has the option to click a link titled "GOOGLE PLAY STORE" after which a different file titled: "tms-2021100801.apk." is prompted to open and download. Based on my training and experience this is not the standard method of installing a legitimate iPhone application.

c. I have not been able to identify or determine an address for the company headquarters. I have not been able to identify any employees shown on the website. Additionally, I have not located any privacy policy posted on the website nor any type of webpage indicating regulatory oversight or additional tabs showing career opportunities to work for this company, as one would expect for a legitimate company.

d. The text and graphics on the website are misaligned. Additionally, there was a notice stating "The purpose of this website is only to show relevant TMS information about the products and services available on the app. Information about the products and services available on the app. It has no intention of providing access to any such products and services. You can access such products and services on the app."

30. In addition to these indications, when conducting open-source research on this website, I identified multiple websites indicating this website was a "scam". Another open-source report indicated nine security vendors flagged this URL as malicious.

31. Based on my training and experience, the discrepancies identified above are not typical for a legitimate cryptocurrency platform.

32. The messages from QIAN were electronic messages sent via interstate wire communication in furtherance of a scheme to defraud WQ by means of false representations and promises. Accordingly, I have probable cause to the believe W.Q. was fraudulently induced to

transfer funds to a scam cryptocurrency platform, *i.e.*, wire fraud, in violation of 18 U.S.C. § 1343.

The Flow of Funds, Generally

33. Subsequent analysis indicates that the Defendant Property can be traced to the transfers from W.Q.'s OKEX account.

34. The nine (9) transfers from W.Q.'s account at OKEX are reflected in Figure 1 below, with times shown in UTC[5]:

Date: 11-12-2021 22:23:58
Amount USDT: 762.47
Sent to wallet address: 0xb7bb948bad8d02957701b04d3a1802e3988ce196 **(Wallet ending in ce196)**
Transaction Hash: 0x54f283322d28d9a2dcf8a688d3d221cce6c29c895817e957769a90a8ec2fb17d
Date: 11-17-2021 01:21:57
Amount USDT: 7696.05
Sent to wallet address: 0xb7bb948bad8d02957701b04d3a1802e3988ce196 **(Wallet ending in ce196)**
Transaction Hash: 0xa79626faf98a5378e897099ebe3758307ff3381680364a3810235217af497a48
Date: 11-19-2021 19:05:05
Amount USDT: 38147.92
Sent to wallet address: 0xb7bb948bad8d02957701b04d3a1802e3988ce196 **(Wallet ending in ce196)**
Transaction Hash: 0x376ac7625bc99333081f655533da456e9a4fe735f41d06b296b87f1a9f3ca9c3
Date: 12-03-2021 03:02:45
Amount USDT: 20420.25
Sent to wallet address: 0x53cca147bada66e6915157534554550c69942756 **(Wallet ending in 42756)**
Transaction Hash: 0xd5189c0eb1117f181c6def485c5b439243c7c843a5db8ab05865451fc68a07ee
Date: 12-20-2021 05:39:07
Amount USDT: 24596.17
Sent to wallet address: 0x6e44154ac822ad00ff3534d332a0d5d611f5aacd **(Wallet ending in 5aacd)**
Transaction Hash: 0x6d5bd600709def9f76acba3c058e098536114d685b90eb1c2ee13fbf5ab9fbb2
Date: 12-25-2021 04:25:48
Amount USDT: 46131.36
Sent to wallet address: 0x6e44154ac822ad00ff3534d332a0d5d611f5aacd **(Wallet ending in 5aacd)**
Transaction Hash: 0xc1a90a31d5280eb4e9dc128f5a5271f55a34468c08cd55c39f14a55c50158ac8

[5] UTC is Universal Time Coordinated, also known as Coordinated Universal Time. This is also known as Greenwich Mean Time.

Date: 12-28-2021 05:06:50
Amount USDT: 19972.03
Sent to wallet address: 0x6e44154ac822ad00ff3534d332a0d5d611f5aacd **(Wallet ending in 5aacd)**
Transaction Hash: 0x3e5edbe6d2fc981045368878a08036a4e8f1ccd4b4309a9211ceb04576b2a03c
Date:01-05-2022 03:56:49
Amount USDT: 70424.17
Sent to wallet address: 0x6e44154ac822ad00ff3534d332a0d5d611f5aacd **(Wallet ending in 5aacd)**
Transaction Hash: 0xb2edf72b36a8de62dab0d2bb3ef63630c671562bcf5969afdabb9664adeeccd9
Date: 01-19-2022 02:03:54
Amount USDT: 75562.54
Sent to wallet address: 0x47a850ccf8f4b7a8ed9bc89966067da51897c624 **(Wallet ending in 7c624)**
Transaction Hash: 0xc889b022c517df11dbb7e81a6c9374a9571ecf19634805d5924ddd8a92f37771

Figure 1

The Flow of Funds to the Binance Account

35. After receiving 20,420.25 USDT of W.Q.'s funds on December 3, 2021, the controller of wallet address ending in 42756 remitted the funds to a series of intermediary wallets before all of these funds (20,420.25 USDT) were ultimately transferred to the **wallet address ending in e8e09**. I later contacted BINANCE for information relating to the transfer of W.Q.'s funds into **wallet address ending in e8e09** and obtained account records from BINANCE indicating this transaction corresponds to the account with user ID ending in 7402, as described more below. Intermediary wallets are typically private wallets or non-exchange wallets that obfuscate transactions on the Blockchain. Intermediary wallets support the movement of illicitly obtained funds as they help to conceal and disguise the source of the USDT by layering and severing straight line coordinates of transaction activity on the Blockchain to cash out exchangers.

36. A listing of the transactions to the intermediary wallets involving W.Q.'s funds can be found in Figure 2 below, with times shown in UTC:

Date: 12-03-2021 03:24:46
Amount USDT: 22395.25
Sent to wallet address: 0x8180ad7cbcba8884978ea1ccd63cdd4c4933f2e0
Transaction Hash: 0x7f441a4d1dfea9dcdfa96f5533ef1db4b85c062af88a435c9dc3b8ac102105d1
Date: 12-06-2021 17:44:13
Amount USDT: 49000
Sent to wallet address: 0xcf46b6dd28710e101b3a7ea80df297551cba5466
Transaction Hash: 0xfe3079abbc5698316f62f23e4152f8a4e8e177d30ef593f22d40b3546d2b79ae
Date: 12-22-2021 09:42:41
Amount USDT: 224000
Sent to wallet address: 0x34dd4b3ce98cde6b0be21f3cdde3e19ca8326391
Transaction Hash: 0xe33e43d4a1bd5bdbc3400b86936309662f55f8d2c4f6015b22cdf3c4aa221c70
Date: 12-25-2021 08:45:23
Amount USDT: 239163
Sent to wallet address: 0x19ba39c8a4e3213c3d69100829eb2d060efe8e09 **(wallet ending in e8e09)**
Transaction Hash: 0xb7b6d759f3db3c02fec87c585110688e21ce51b82ecf2b3da9631c40ca165ca7

Figure 2

37. After receiving 46,606.44 USDT in W.Q.'s funds from November 12 to 19, 2021 (see Figure 1), the controller of **wallet address ending in ce196** remitted the funds to a series of intermediary wallets before 28,579.75 USDT was ultimately transferred to the account with user ID ending in 7402.

38. A listing of these transactions can be found in Figure 3 below, with times shown in UTC:

Date: 11-17-2021 21:22:25
Amount USDT: 37591.348986
Sent to wallet address: 0x8180ad7cbcba8884978ea1ccd63cdd4c4933f2e0
Transaction Hash: 0x522de15ac4e1bdb74901c7b55d82b0eef1c30a364f306fac0b88ab2bd7304981
Date: 11-19-2021 19:07:26
Amount USDT: 38622.92
Sent to wallet address: 0x8180ad7cbcba8884978ea1ccd63cdd4c4933f2e0
Transaction Hash: 0x3756ec4a7e6d61523a76b283f4dc4559038a9c6e12058587c8d99a1fcc99fbfd
Date: 12-06-2021 17:44:13
Amount USDT: 49000

Sent to wallet address: 0xcf46b6dd28710e101b3a7ea80df297551cba5466
Transaction Hash: 0xfe3079abbc5698316f62f23e4152f8a4e8e177d30ef593f22d40b3546d2b79ae
Date: 12-22-2021 09:42:41
Amount USDT: 224000
Sent to wallet address: 0x34dd4b3ce98cde6b0be21f3cdde3e19ca8326391
Transaction Hash: 0xe33e43d4a1bd5bdbc3400b86936309662f55f8d2c4f6015b22cdf3c4aa221c70
Date: 12-25-2021 08:45:23
Amount USDT: 239163
Sent to wallet address: 0x19ba39c8a4e3213c3d69100829eb2d060efe8e09 **(wallet ending in e8e09)**
Transaction Hash: 0xb7b6d759f3db3c02fec87c585110688e21ce51b82ecf2b3da9631c40ca165ca7

Figure 3

39. After receiving 161,123 USDT in W.Q.'s funds between December 20, 2021 and January 5, 2022 (see Figure 1), the controller of **wallet address ending in 5aacd** remitted the funds to a series of intermediary wallets before 24,596.17 USDT was ultimately transferred to the account with user ID ending in 7402.

40. A listing of these transactions can be found in Figure 4 below, with times shown in UTC:

Date: 12-20-2021 05:41:40
Amount USDT: 34680.77511
Sent to wallet address: 0x680b5fd7361232f447ae0a9355a4f4fd42c1c871
Transaction Hash: 0x115753705262026bd916f5bb50e00bcc8fec3fc44bf1b93647edd832ef0a39b4
Date: 12-20-2021 15:47:54
Amount USDT: 70000
Sent to wallet address: 0xcf46b6dd28710e101b3a7ea80df297551cba5466
Transaction Hash: 0x6676f58df85431bf07ef45b3e238fce415b2208bb7fe7b530ba8e476746713e4
Date: 12-22-2021 09:42:41
Amount USDT: 224000
Sent to wallet address: 0x34dd4b3ce98cde6b0be21f3cdde3e19ca8326391
Transaction Hash: 0xe33e43d4a1bd5bdbc3400b86936309662f55f8d2c4f6015b22cdf3c4aa221c70
Date: 12-25-2021 08:45:23
Amount USDT: 239163

Sent to wallet address: 0x19ba39c8a4e3213c3d69100829eb2d060efe8e09 **(Wallet ending e8e09)**
Transaction Hash: 0xb7b6d759f3db3c02fec87c585110688e21ce51b82ecf2b3da9631c40ca165ca7

Figure 4

41. A visual depiction containing the transfers identified in Figures 1 through 4 above, are reflected in Attachment A.

42. After reviewing Attachment A and other facts of this investigation, I was able to identify that after multiple intermediary transfers, 73,596.17 USDT of W.Q.'s funds were ultimately transferred to **wallet address ending in e8e09**. I contacted BINANCE for information relating to this transaction of W.Q.'s funds into **wallet address ending in e8e09** and obtained account records for one BINANCE account. The BINANCE records reflect that the transfer of W.Q.'s funds into **wallet address ending in e8e09** is attributable to BINANCE account user ID number ending 7402. Records indicate that this account is associated with a Taiwanese (Republic of China) passport holder.[6]

CONCLUSION

43. Based on my knowledge, training, and experience, and the foregoing information set forth in this affidavit, there is probable cause that the Defendant Property constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1343 (Wire Fraud) and is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C).

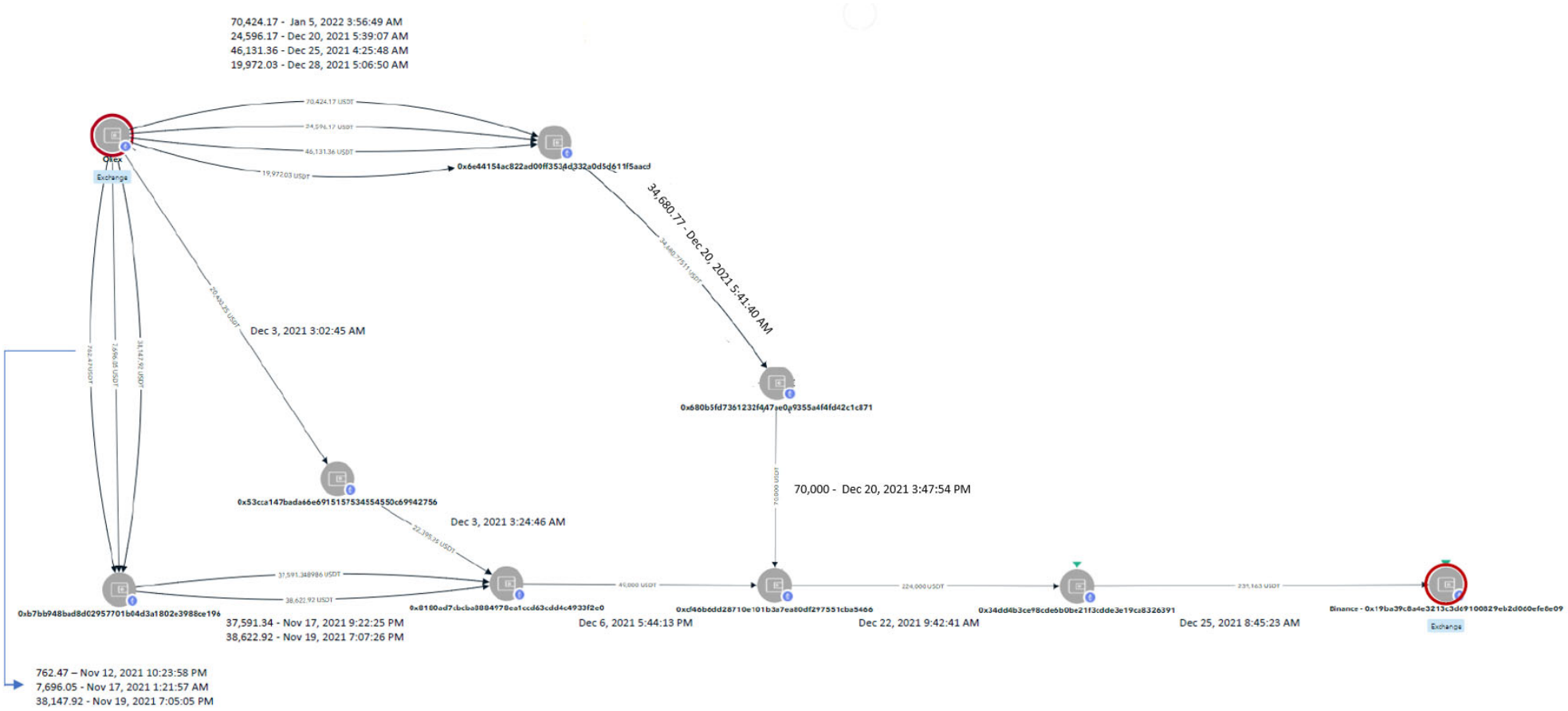
Signed under the penalty and pains of perjury on August 3, 2022.

Garrett Fitzgerald Jr.

Cyber Special Agent Garrett Fitzgerald Jr.
United States Secret Service

[6] The name of the individual is known to law enforcement.

ATTACHMENT A


70,424.17 - Jan 5, 2022 3:56:49 AM
24,596.17 - Dec 20, 2021 5:39:07 AM
46,131.36 - Dec 25, 2021 4:25:48 AM
19,972.03 - Dec 28, 2021 5:06:50 AM
70,424.17 USDT
24,596.17 USDT
46,131.36 USDT
19,972.03 USDT
Okex
Exchange
0x6e44154ac822ad00ff353d4d332a0d5d611f5aacd
34,680.77 - Dec 20, 2021 5:41:40 AM
34,680.77411 USDT
20,443.25 USDT
Dec 3, 2021 3:02:45 AM
0x680b5fd7361232f4f47ae0a9355a4f4fd42c1c871
762.47 USDT
7,696.05 USDT
38,147.92 USDT
70,000 USDT
70,000 - Dec 20, 2021 3:47:54 PM
0x53cca147bada66e69151575345545550c69942756
Dec 3, 2021 3:24:46 AM
22,398.24 USDT
37,591.348986 USDT
38,622.92 USDT
0xb7bb948bad8d02957701b04d3a1802e3988ce196
37,591.34 - Nov 17, 2021 9:22:25 PM
38,622.92 - Nov 19, 2021 7:07:26 PM
0x8180ad7cbcba888497ea1ccd63cdd4c4933f2c0
Dec 6, 2021 5:44:13 PM
0xcf46b6dd28710e101b3a7ea80df297551cba5466
Dec 22, 2021 9:42:41 AM
0x34dd4b3ce98cde6b0be21f3cdde3e19ca8326391
Dec 25, 2021 8:45:23 AM
Binance - 0x19ba39c8a4e3213c3de9100829eb2d060efe0e09
Exchange
762.47 – Nov 12, 2021 10:23:58 PM
7,696.05 - Nov 17, 2021 1:21:57 AM
38,147.92 - Nov 19, 2021 7:05:05 PM