AFFIDAVIT OF SPECIAL AGENT HEIDI L. ROBLES

I, Special Agent Heidi L. Robles, declare and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service ("USSS") and have been employed as such since August of 2021. Prior to becoming a Special Agent, I was a Uniformed Division Officer with the USSS from August 2017 to August 2021. I attended 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) and 18 U.S.C. § 1956 (Laundering of Monetary Instruments). In connection with these investigations, I have conducted or participated in numerous field interviews of suspects and witnesses, electronic and physical surveillance, and 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.

PURPOSE OF AFFIDAVIT

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

a. 193,169.0653 USDT[1] seized from a Binance account with user ID XXXX8768 in the name of Lim Hock Seng (hereinafter referred to as "**ACCOUNT-1**") on June 19, 2023.

[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.

b. 11,146.8079 USDT and 18.9649 BTC[2] seized from a Binance account with user ID XXXX1519 in the name of Yicheng Wang (hereinafter referred to as "**ACCOUNT-2**") seized on June 19, 2023

(collectively, the "Defendant Property").

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). Additionally, there is probable cause to believe that the Defendant Property also is property involved in a violation of 18 U.S.C. § 1956 (Laundering of Monetary Instruments) and is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A).

4. This affidavit is based on my personal knowledge, information provided by other law enforcement officers 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 May 8, 2023, the government sought and was granted, seizure warrants for the Defendant Property. On June 19, 2023, Binance, a cryptocurrency exchange platform, transferred the Defendant Property to a USSS-controlled cryptocurrency wallet, where the Defendant Property is currently being held.

[2] "BTC" is the abbreviation for Bitcoin.

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 (i) used as a substitute for fiat currency to buy goods or services, or (ii) exchanged for fiat currency or other cryptocurrencies.[3] Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although cryptocurrency is not usually stored in any physical form, the 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. Public and private keys are discussed in more detail below. 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.[4] 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

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

[4] 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.

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" in part by fiat currencies, or currencies issued by governments like the dollar and euro. Due to Tether's relatively stable nature, a fundamental strategy typically employed by wallet holders is to use Tether to hedge their cryptocurrency holdings because its value is not affected by the rest of the volatile cryptocurrency market.

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, 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, like fiat currencies, 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. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (*e.g.*, smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (*e.g.*, Trezor, Keepkey, or Nano Ledger). Paper wallets contain an address and a QR code[5] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up using, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application.

13. Cryptocurrency "exchangers" and "exchanges" are individuals or companies that exchange bitcoin for other currencies and cryptocurrencies, including U.S. dollars and Tether. According to Department of Treasury, Financial Crimes Enforcement Network ("FinCEN")

[5] A QR code is a matrix barcode that is a machine-readable optical label.

Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[6] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions.

14. 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 P.O. Box 472, Harbour Place, 2nd Floor, North Wing, 103 South Church Street, George Town, Grand Cayman, KY1-1106.

PROBABLE CAUSE

15. As set forth below, there is probable cause to believe that the Defendant Property represents proceeds obtained through violations of 18 U.S.C. § 1343 (Wire Fraud). Pursuant to 18 U.S.C. § 981(a)(1)(C), any property, real or personal, which constitutes or is derived from proceeds traceable to a "specified unlawful activity," or a conspiracy to commit such offense is subject to civil forfeiture. Pursuant to 18 U.S.C. § 1961(1), as incorporated by 18 U.S.C. § 1956(c)(7)(A), violations of 18 U.S.C. § 1343 are a specified unlawful activity.

16. In addition, there is probable cause to believe that the Defendant Property is subject to forfeiture as property involved in a transaction or attempted transaction in violation of 18 U.S.C.

[6] *See* "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," *available at* https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

§ 1956(a)(1)(B)(i) (Laundering of Monetary Instruments). Pursuant to 18 U.S.C. § 981(a)(1)(A) any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956(a)(1)(B)(i), or any property traceable to such property is subject to civil forfeiture. It is a violation of 18 U.S.C. § 1956(a)(1)(B)(i) (Laundering of Monetary Instruments), to engage in a financial transaction knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity. As set forth below, the proceeds from the fraudulent schemes that Victim-1 and Victim-2 were victims of were moved through a chain of transactions utilizing money laundering techniques and deposited into ACCOUNT-1 and ACCOUNT-2.

17. Accordingly, there is probable cause to believe that the Defendant Property is subject to forfeiture.

The Scheme to Defraud

18. On or around September 6, 2022, Victim-1 of Cambridge, Massachusetts contacted law enforcement and provided information indicating he was the victim of a cryptocurrency trading scam. Between October 3, and October 17, 2022, I communicated with Victim-1 via telephone and email. Victim-1 explained he was initially contacted on May 8, 2022 by an individual named "JOAN" through a messaging application called WeChat.

19. After connecting on WeChat, the individual or individuals purporting to be "JOAN" began communicating with Victim-1 through two messaging applications, WeChat and Line, installed on Victim-1's iPhone. Victim-1 received communications on these messaging applications from "JOAN" who utilized the phone number ending in 4567.

20. I conducted a thorough open-source search for the phone number ending in 4567 and was able to identify that the number came back to a voice over internet protocol (VOIP).

Based on my training and experience, as well as conversations with other investigators, VOIP numbers are commonly used in these types of scams to portray the scammer to be in a different location than the one they are in and to hide their identity.

21. Victim-1 stated all messages with "JOAN" were typed in Chinese. Victim-1 stated he spoke Chinese as his native language.

22. "JOAN" introduced Victim-1 to a cryptocurrency exchange that Victim-1 was told was, and believed to be, Deribit, a large crypto options and futures exchange. "JOAN" sent Victim-1 screenshots showing the "profit gains" that "JOAN" received by investing in cryptocurrency. Victim-1 had never purchased or sold cryptocurrencies before he began communicating with "JOAN".

23. Victim-1 followed "JOAN's" instructions and opened an account both at the Crypto.com currency exchange and an exchange he believed was "Deribit.com". "JOAN" provided Victim-1 a website URL of "https://app.store.com.apple10store[.]com/OwxQK", [7] which he was told linked to the Deribit trading platform. "JOAN" sent Victim-1 screenshots of the steps to take to open an account on what Victim-1 believed was the "Deribit" mobile application.

24. Victim-1 made his first purchase of cryptocurrency on Crypto.com on July 2, 2022, and with "JOAN's" help, transferred that cryptocurrency to "Deribit.com". After this initial transaction Victim-1 noticed he lost $7,000. When he confronted "JOAN" about it, Victim-1 stated "JOAN promised me next time it will go up."

[7] Brackets, referred to as "blocks" are placed (e.g., "[.]com") within the URL to prevent inadvertent connections.

25. Victim-1 stated after ten days it appeared that he made a 40% profit from the first transaction. JOAN told Victim-1 "Try your best to get more money." Victim-1 informed her he did not have money, but JOAN insisted.

26. As evidenced by Victim-1's messages and statements, between July 2, 2022, and August 26, 2022, the individual or individuals identifying themselves as "JOAN" instructed Victim-1 to transfer approximately 477,804.81 USDT to various cryptocurrency wallets. Victim-1 stated he bought USDT on Crypto.com and sent ten cryptocurrency transfers from his account at Crypto.com to the destination wallet address detailed in Figure 1 below. Victim-1 also provided details of each of these transfers to law enforcement.

27. I conducted a review of the transfer details provided by Victim-1 and was able to verify these ten cryptocurrency transfers totaling 477,804.81 USDT transferred out of Crypto.com and ultimately, as described below, into **ACCOUNT-1** and **ACCOUNT-2.**

28. Victim-1 stated he conducted the first seven cryptocurrency transfers from his account at Crypto.com under the direction and instructions he received from JOAN.

29. Victim-1 stated that on August 5, 2022, he tried to withdraw money from what he believed to be the "Deribit" mobile application but had received a message from someone purporting to be customer service and was instructed he needed to pay "tax on earnings" in his account. These instructions caused Victim-1 to make the final three transfers of USDT from his account at Crypto.com to the destination wallet address provided by "Deribit" customer service. Even after making these transfers, Victim-1 was still unable to withdraw any money from the "Deribit" mobile application. Based on my training and experience, I am aware that telling a victim that they need to pay "taxes" to access funds is a common tactic used in online cryptocurrency fraud schemes to induce a victim to transfer additional funds to the perpetrators.

30. Victim-1 provided law enforcement screenshots of the "Deribit application" on his iPhone appearing to show a cryptocurrency portfolio, including a cryptocurrency deposit history and trading history. Screenshots provided by Victim-1 also appeared to indicate gains and losses of a cryptocurrency portfolio value.

31. After conducting a search on the Apple application store, I was not able to find a Deribit application. Furthermore, Deribit is not an exchange listed or operating within the United States.

32. I also conducted a thorough open-source search for the URL "https://app.store.com.apple10store[.]com/OwxQK" and was unable to identify or access the website which Victim-1 indicated he visited to download the "Deribit" application onto his iPhone. Furthermore, I queried the publicly available domain Wayback Machine[8] at web.archive.org to see if any historical snapshots of the website had been captured. There were none. 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 be accessed through a web browser and contain clearly outlined platform policies, company contact information, information regarding the platform's creation, company staff information, along with access for desktop and mobile computing.

33. During the course of my investigation, I was able to identify a platform known as Deribit, which can be accessed through the website Deribit.com/net. Investigators were able to contact a representative of Deribit and confirmed that Victim-1 did not hold an account there.

[8] The Wayback Machine is a 501(c)(3) non-profit based out of California, launched to the public in 2001 and its primary function is to build a digital library of internet sites and other cultural aspects in digital form. The Wayback Machine's Internet Archive is a useful open source tool to see if there used to be a website under specific domains.

Based on my conversations with other investigators, it is common to use real logos and names for fraudulent platforms.

34. In addition, when conducting open-source research on scams related to fraudulent Deribit platform and tax customer service-common scam, I identified multiple websites indicating that the website provided to Victim-1 to download the "Deribit" mobile application was a "scam". Another open-source report indicated nine security vendors flagged this URL as malicious.

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

36. Accordingly, I have probable cause to believe Victim-1 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

37. Subsequent analysis indicates that the funds in **ACCOUNT-1** and the funds in **ACCOUNT-2** can be traced to the transfers from Victim-1's Crypto.com account.

38. The ten transfers from Victim-1's account at Crypto.com are reflected in Figure 1 below, with times shown in UTC[9]:

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

Date: 07-02-2022 02:06:25 AM
Amount USDT: 29,403.17
Sent to wallet address: 0x6CE2d91c9F91AEfa180E58A6bB9B9352D03994a9 **(Wallet ending in 994a9)**
Transaction Hash: 0x739c8e84f93d9f0dfc6cc64354db267e1f3017dfe8008f21cb0cee908182cad4
Date: 07-07-2022 09:32:11 PM
Amount USDT: 29,510.39
Sent to wallet address: 0x6CE2d91c9F91Aefa180E58A6bB9B9352D03994a9 **(Wallet ending in 994a9)**
Transaction Hash: 0x66012761da03dbeec33e6ff47faba16c18d96f1437a575b77b74f29cfea6b96a
Date: 07-08-2022 09:24:21 PM
Amount USDT: 77,978.04
Sent to wallet address: 0x6CE2d91c9F91Aefa180E58A6bB9B9352D03994a9 **(Wallet ending in 994a9)**
Transaction Hash: 0x7a7372d5ecb02f9047d47c42f62de6e2da57b06a7eac113db32dea0f3fcefbf9
Date: 07-12-2022 07:15:36 PM
Amount USDT: 58,506.55
Sent to wallet address: 0x6CE2d91c9F91Aefa180E58A6bB9B9352D03994a9 **(Wallet ending in 994a9)**
Transaction Hash: 0x16fcaa5402b27c5107dcfa0d2e12a5fada9e8e151d52366b8ca284ac086e0f6d
Date: 07-13-2022 07:49:19 PM
Amount USDT: 48,736.66
Sent to wallet address: 0x6CE2d91c9F91Aefa180E58A6bB9B9352D03994a9 **(Wallet ending in 994a9)**
Transaction Hash: 0xf9a8e01e8806e057f95e604d8ac4552779f428c060cc4a4300eefbb9cf370785
Date: 07-28-2022 08:08:40 PM
Amount USDT: 38,945
Sent to wallet address: 0x6CE2d91c9F91Aefa180E58A6bB9B9352D03994a9 **(Wallet ending in 994a9)**
Transaction Hash: 0xe7f8d3f414dc3fcafda36a4a15f64025ab22ef33e2b3985c9506508f8324cde7
Date: 08-01-2022 05:49:01 PM
Amount USDT: 63,295
Sent to wallet address: 0x6CE2d91c9F91Aefa180E58A6bB9B9352D03994a9 (**Wallet ending in 994a9)**
Transaction Hash: 0x7258a2779763d9f42468eb69b2a845f73360e7998a6da536b7ada9ffebda7890
Date: 08-10-2022 02:10:24 PM
Amount USDT: 59,975
Sent to wallet address: 0x6CE2d91c9F91Aefa180E58A6bB9B9352D03994a9 (**Wallet ending in 994a9)**
Transaction Hash: 0x8aef3c51450ff48d77e4eeb061303f6dd577f932973d4736feb43c59e2411d83
Date: 08-10-2022 10:21:14 PM
Amount USDT: 2,347
Sent to wallet address: 0x6CE2d91c9F91Aefa180E58A6bB9B9352D03994a9 (**Wallet ending in 994a9)**
Transaction Hash: 0x35266a6826a8cec1b79604b3562ebd8b25afe40e3543f76df7932db837c8b49f
Date:08-26-2022 01:27:26 PM
Amount USDT: 69,108
Sent to wallet address: 0x6CE2d91c9F91Aefa180E58A6bB9B9352D03994a9 (**Wallet ending in 994a9)**
Transaction Hash: 0x2ca9f830cc0ce8366db5c5d2a62b53740031d239c7e832680b1bcea9d19f7c29

Figure 1

39. After receiving 477,804.81 USDT in Victim-1's funds between July 2 and August 26, 2022 (see Figure 1), the controller of **wallet address ending in 994a9** remitted approximately 408,696.81 USDT of the funds and other comingled funds to **wallet address ending in 35A7E**.

40. A listing of these transactions are in Figure 2 below, with times shown in UTC:

Date: 07-07-2022 10:10:32 PM
Amount USDT: 280,000
Sent to wallet address: 0x1E8b3caeB54A15b0CA956273B58DC4d172135A7E **(Wallet ending in 35A7E)**
Transaction Hash: 0x1e86d7050a21633c4fd89419012b56495de0a5431b745e8a2e4b2969ee2e99fd
Date: 07-08-2022 09:34:20 PM
Amount USDT: 150,000
Sent to wallet address: 0x1E8b3caeB54A15b0CA956273B58DC4d172135A7E **(Wallet ending in 35A7E)**
Transaction Hash: 0xb3dda137c4219db1e40489e7f8448bdcb67fe4556f6df21bb45db09c4d20a8d3
Date: 07-13-2022 08:52:51 PM
Amount USDT: 75,895.22
Sent to wallet address: 0x1E8b3caeB54A15b0CA956273B58DC4d172135A7E **(Wallet ending in 35A7E)**
Transaction Hash: 0x929e6b489baa9108208c8e0bc3dc0c8d438ce827b05ee124d6e09d2d447bdc4d
Date: 07-29-2022 03:12:29 AM
Amount USDT: 38,945
Sent to wallet address: 0x1E8b3caeB54A15b0CA956273B58DC4d172135A7E **(Wallet ending in 35A7E)**
Transaction Hash: 0xf65cdf28755b27ad5f24ef93d17d7d662c5bafbe32a29a5e5213b5e64a58dee0
Date: 08-02-2022 02:55:46 AM
Amount USDT: 63,295
Sent to wallet address: 0x1E8b3caeB54A15b0CA956273B58DC4d172135A7E **(Wallet ending in 35A7E)**
Transaction Hash: 0x9eb41d0731d5d769a5c9ce2790654292338c0c95cd1941d485888bb4cb7a6a1a
Date: 08-12-2022 03:48:26 AM
Amount USDT: 68,152.61
Sent to wallet address: 0x1E8b3caeB54A15b0CA956273B58DC4d172135A7E **(Wallet ending in 35A7E)**
Transaction Hash: 0xb9ac1599a2da44757789cb7406e43bb4d7f095a8f61f7b2024345e313b8ac430

Figure 2

41. After receiving approximately 408,696.81 USDT in Victim-1's funds and other commingled funds between July 7 and August 12, 2022 (*see* Figure 2), the controller of **wallet address ending in 35A7E** remitted the funds and other comingled funds to **wallet address ending in 31f59**.

42. A listing of these transactions are in Figure 3 below, with times shown in UTC:

Date: 07-08-2022 11:48:33 AM
Amount USDT: 985,600
Sent to wallet address: 0x8A84F30e53beb251974c6C038AD863916eF31f59 **(Wallet ending in 31f59)**
Transaction Hash: 0xb3f3d6bb778f2c7c147ba192298ba50598e7ef14444c7cd45e3922f67452dd82
Date: 07-10-2022 01:26:46 PM
Amount USDT: 1,020,600
Sent to wallet address: 0x8A84F30e53beb251974c6C038AD863916eF31f59 **(Wallet ending in 31f59)**
Transaction Hash: 0xe0e64fd38b73af73d6732ffa4694e8273accdfca41d699cb7fb880233c2a272a
Date: 07-14-2022 04:38:07 AM
Amount USDT: 985,600
Sent to wallet address: 0x8A84F30e53beb251974c6C038AD863916eF31f59 **(Wallet ending in 31f59)**
Transaction Hash: 0x0c21f344ba886cf94de33dd3e7f0cf3b21c25e8c4e60537c4054327aee325c17
Date: 07-29-2022 05:26:15 PM
Amount USDT: 443,567
Sent to wallet address: 0x8A84F30e53beb251974c6C038AD863916eF31f59 **(Wallet ending in 31f59)**
Transaction Hash: 0xe1114852056447811e1a082c706dd89542a8a1aac7ee2c7e6d8f796e80d24bcd
Date: 08-02-2022 08:39:21 AM
Amount USDT: 835,940
Sent to wallet address: 0x8A84F30e53beb251974c6C038AD863916eF31f59 **(Wallet ending in 31f59)**
Transaction Hash: 0x5e180f09efeba8b73d0f812f52306ffecb281bf996633f5821d9963c1abd5414
Date: 08-12-2022 11:57:48 AM
Amount USDT: 883,260
Sent to wallet address: 0x8A84F30e53beb251974c6C038AD863916eF31f59 **(Wallet ending in 31f59)**
Transaction Hash: 0x1bef895c64ba712db1b9801bd8fa2e44a75faa3248fcacdbeb1a53835ef819d7

Figure 3

The Flow of Funds to ACCOUNT-1:

43. After receiving approximately 408,696.81 USDT of Victim-1.'s funds, the controller of wallet address ending in 35A7E remitted the funds first to the wallet address ending in 31f59, as described above, and then to a series of intermediary wallets along with other comingled funds, before 20,000 USDT was ultimately transferred to the **wallet address ending in B2DD3.** I contacted Binance for information relating to the transfer of Victim-1's funds into **wallet address B2DD3** and obtained account records from Binance indicating this transaction

corresponds to **ACCOUNT-1**, as described more fully 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 holders seeking to eventually cash out the illicitly obtained cryptocurrency and convert it into fiat currency.

44. A listing of the transactions to the intermediary wallets involving Victim-1's funds can be found in Figure 4 below, with times shown in UTC:

Date: 07-10-2022 12:48:42 PM
Amount USDT: 200,000
Sent to wallet address: 0x717c78C29E58B4cF18Aec4360a7D36fA3fE**9c574**
Transaction Hash: 0xc71e3ecbc54699a193e63dc2bef70436d22af62c930f2a618e1dc233e26d505f
Date: 07-12-2022 01:43:17 PM
Amount USDT: 20,000
Sent to wallet address: 0xf82A84DBC3e60de5E638501b08331e697B4**62285**
Transaction Hash: 0x248997b0a43021c30cb8d349ebb3f16ff064d5407572ece00269d9ff892be4a3
Date: 07-17-2022 01:11:31 PM
Amount USDT: 20,000
Sent to wallet address: 0xC73a403D83abd1B27C1b53eCb0E64CAD8C0B2DD3 **(wallet ending in B2DD3)**
Transaction Hash: 0x1272c0bf6de10931fa2066fb3fe5d6f6f2dd1bcab9b0d544d564414b40559d58

Figure 4

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

46. During the course of my investigation, I and other law enforcement were able to identify additional victims whose funds were commingled and transferred to **wallet address ending in B2DD3**. One such victim was Victim-2 of Holliston, MA. Victim-2 was induced to send over $2.4 million USDT of their personal savings through an account held at Crypto.com to a fraudulent investment platform called "bitcoinwin", which was provided to Victim-2 via the

URL chatlink.mstatik[.]com. When Victim-2 attempted to withdraw their investment, their account was "frozen", and Victim-2 was told that a payment of $3.3 million dollars would release the funds. Investigation of "bitcoinwin" found multiple reports of other victims having sent funds to a similar fraudulent investment platform only to find that they had to pay exorbitant "fees" to release their investments from the platform. Tracing analysis of the flow of funds identified approximately 254,054 USDT of Victim-2's funds were ultimately transferred to **wallet address ending in B2DD3** in three separate deposits.

47. A listing of the transactions from Victim-2's Crypto.com account relating to the first deposit to **wallet address ending in B2DD3** is shown in Figure 5 below, with times in UTC.

Date: 06-21-2022 09:47:10 PM
Amount USDT: 196,103
Sent to wallet address: 0x08AD3a0211ba2EC5aC1B8fe79511feded77**90D77**
Transaction Hash: 0x457b364e59daf95efc1be494f5072e27174bd53c542daf524dae430947ed3a3b
Date: 06-21-2022 09:58:51 PM
Amount USDT: 196,000
Sent to wallet address: 0x9c60625E210f1Ba03575dC6271C42B7289E**6e133**
Transaction Hash: 0x84633eb4bfa0e5ca1b8f792a9eda266f35838f9d617dc0b2a94ad0fb22c56e37
Date: 06-23-2022 09:14:20 PM
Amount USDT: 199,500
Sent to wallet address: 0x7899E76489D037243f7e2796cc5A091E086**5a3c6**
Transaction Hash: 0x5fc826202610f8e0bdf62d9bd2ab273591eb1c45b2112f4610ec3ca58d0f8eab
Date: 06-29-2022 08:28:02 PM
Amount USDT: 20,000
Sent to wallet address: 0xCEE210747Af930b55643f369AbBe30A08ed**62FDc**
Transaction Hash: 0x41cd1e5c04b489831914c7c6d2dafabbbc65c1f7c0c0799c370c8a6a629b848a
Date: 06-30-2022 03:36:17 PM
Amount USDT: 20,000
Sent to wallet address: 0xC73a403D83abd1B27C1b53eCb0E64CAD8C0B2DD3 **(wallet ending in B2DD3)**
Transaction Hash: 0xf316acb5c6923428fbc6eb25afab3dfaee4556bdf38b9a63be230509b8456d69

Figure 5

48. A listing of the transactions from Victim-2's Crypto.com account relating to the second deposit to **wallet address ending in B2DD3** can be found in Figure 6 below, with times shown in UTC.

Date: 08-12-2022 04:58:01 PM
Amount USDT: 170,720.95
Sent to wallet address: 0x08AD3a0211ba2EC5aC1B8fe79511feded77**90D77**
Transaction Hash: 0x1cdb58d1702f6e1c997c630c6e8b3600276edd2e75674baa783515b88a88290e
Date: 08-12-2022 05:03:24 PM
Amount USDT: 175,000
Sent to wallet address: 0x9c60625E210f1Ba03575dC6271C42B7289E**6e133**
Transaction Hash: 0xca9c47d9f4aaf7e0302c8d3cb82920b764dd89f6de9dcdee2916466e39313295
Date: 08-16-2022 02:34:15 PM
Amount USDT: 250,000
Sent to wallet address: 0x7899E76489D037243f7e2796cc5A091E086**5a3c6**
Transaction Hash: 0xd8ec7f48312f7712b98ec6895cbb15a41fa3ecb932287e408927ce3fce9f85ab
Date: 08-25-2022 02:40:22 PM
Amount USDT: 200,000
Sent to wallet address: 0x73704d38dAF136760DD547D26FA06907b9f**6aEEc**
Transaction Hash: 0xb31723fc6331f3e766dd04db9a32c1a9b4997fcead0c22da7729ee6efd86a6b9
Date: 10-16-2022 09:43:35 AM
Amount USDT: 200,000
Sent to wallet address: 0xa9b66AfDf648e46Cc8dcB1e11d47750AD31**5Fa90**
Transaction Hash: 0x308de202af154072ec0e84bde689aee65c44796ac0e6b3f6f6a1b0fac79a55cd
Date: 10-16-2022 10:13:23 AM
Amount USDT: 134,054
Sent to wallet address: 0xC73a403D83abd1B27C1b53eCb0E64CAD8C0B2DD3 **(wallet ending in B2DD3)**
Transaction Hash: 0x46282a0388163d7ebbfafe7fd6bc226c47fd288811f1fea6484645d23b41ac07

Figure 6

49. A listing of the transactions from Victim-2's Crypto.com account relating to the third deposit to **wallet address ending in B2DD3** can be found in Figure 7 below, with times shown in UTC.

Date: 10-07-2022 04:51:35 PM
Amount USDT: 121,542
Sent to wallet address: 0x08AD3a0211ba2EC5aC1B8fe79511feded77**90D77**
Transaction Hash: 0x868bdd15f0d38596e7860e93f106046b5e029fd8b51740cdaf6f0514db294006
Date: 10-07-2022 04:54:59 PM
Amount USDT: 120,000
Sent to wallet address: 0xa9b66AfDf648e46Cc8dcB1e11d47750AD31**5Fa90**
Transaction Hash: 0x71f5446458c1c898d689ae40f31b7e61958e77389ad6f603f6e06c3888e7b05b
Date: 10-08-2022 07:27:23 AM
Amount USDT: 300,600
Sent to wallet address: 0x793ed27aEd299cFC1CBc41639aD807825e0**10096**
Transaction Hash: 0x907f0cafd506c359852152d7a3330b70c67d8429999ba7cb443879fa0f870f26
Date: 10-08-2022 08:07:23 AM
Amount USDT: 100,000
Sent to wallet address: 0xC73a403D83abd1B27C1b53eCb0E64CAD8C0B2DD3 **(wallet ending in B2DD3)**
Transaction Hash: 0xf07fed22a22cb40d97913ca63b383202c671aa72ff198400b08829b6f256a1c1

Figure 7

50. A visual depiction containing the transfers identified in Figures 5 through 7 are reflected in Attachment B.

51. After reviewing Attachments A and B and other facts of this investigation, I was able to identify that after multiple intermediary transfers, 20,000 USDT of Victim-1's funds and 254,054 USDT of Victim-2's funds were ultimately transferred to **wallet address ending in B2DD3**. I contacted Binance for information relating to these transactions of Victim-1. and Victim-2's funds into **wallet address ending in B2DD3** and obtained account records for one Binance account. The Binance records reflect that the transfers of Victim-1 and Victim-2's funds into **wallet address ending in B2DD3** (referenced in Figures 1 through 7 and Attachments A and B is attributable to Binance account user ID number XXXX8768, also known as **ACCOUNT-1**, and is held in the name of LIM HOCK SENG. The records include the email address nicholas@virtuecap[.]net and a Malaysia passport bearing the name of LIM HOCK SENG. **ACCOUNT-1** was opened on or about February 10, 2021.

52. Of the amounts held in **ACCOUNT-1**, the Government seized 193,169.0653 USDT. This is the remaining amount of the 274,054 USDT of Victim-1 and Victim-2's funds that were traced and transferred to **ACCOUNT-1**. The original Victim-1 funds were sent from Victim-1 between July 2, 2022 and August 26, 2022, traced through the analysis shown in Attachment A, transferred through several intermediary wallets identified in Figures 2, 3 and 4, with partial victim funds ending up in **ACCOUNT-1**. The original Victim-2 funds were sent from Victim-2 between June 21 and October 7, 2022, traced through the analysis shown in Attachment B, transferred through several intermediary wallets identified in Figures 5, 6, and 7, with partial victim funds ending up in **ACCOUNT-1**.

53. Based on the above analysis, and my training and experience, I have probable cause to the believe that 193,169.0653 USDT in **ACCOUNT-1** are proceeds of wire fraud in violation of 18 U.S.C. § 1343 and are subject to forfeiture.

The Flow of Funds to ACCOUNT-2:

54. After receiving approximately 477,804.81 USDT of Victim-1's funds, the controller of wallet address ending in 994a9 remitted the funds to a series of intermediary wallets via two separate paths before 865,449 USDT in commingled funds were transferred in four separate deposits to the **wallet address ending in 03005**. I later contacted Binance for information relating to the transfer of Victim-1's funds into **wallet address 03005** and obtained account records from Binance indicating this transaction corresponds to **ACCOUNT-2**, as described more fully below.

55. A listing of the transactions to the first path of intermediary wallets involving Victim-1's funds can be found in Figure 8 below, with times shown in UTC:

Date: 07-10-2022 12:48:42 PM
Amount USDT: 200,000
Sent to wallet address: 0x717c78C29E58B4cF18Aec4360a7D36fA3fE**9c574**
Transaction Hash: 0xc71e3ecbc54699a193e63dc2bef70436d22af62c930f2a618e1dc233e26d505f
Date: 07-14-2022 04:25:48 PM
Amount USDT: 700,000
Sent to wallet address: 0x66e8D371c62920d66Ce0856fE5B8d338F87**645B9**
Transaction Hash: 0x2345e9b194af7533041df10363d9292acad5d40e184ea7b64e39b9708b8816aa
Date: 07-12-2022 11:02:11 AM
Amount USDT: 30,000
Sent to wallet address: 0x89Fd8Af640206D834D026D1F61d36fcB40C**0FaD8**
Transaction Hash: 0x8a1640ccfa3c98e06781c0b65ae56b837f19b2984983ea027a249b39581058f9
Date: 07-15-2022 06:31:01 AM
Amount USDT: 173,833
Sent to wallet address: 0x89Fd8Af640206D834D026D1F61d36fcB40C**0FaD8**
Transaction Hash: 0x07e48049f12006dabd2c6c35a01f151fb629830f6a149ffd0735d6f179e57c59
Date: 07-15-2022 06:38:50 AM
Amount USDT: 100,000
Sent to wallet address: 0x89Fd8Af640206D834D026D1F61d36fcB40C**0FaD8**
Transaction Hash: 0xc3350cfd129d13cd0627a440a8795e47a2cd6204adda2a008485daa05362a57a
Date: 07-17-2022 02:14:26 PM
Amount USDT: 56,657
Sent to wallet address: 0x89Fd8Af640206D834D026D1F61d36fcB40C**0FaD8**
Transaction Hash: 0x5ee600a3979892d7464d24639abf55ac7fad8a5e86f6aa2199e782d4f94335f4
Date: 07-18-2022 11:19:56 AM
Amount USDT: 42,492
Sent to wallet address: 0x89Fd8Af640206D834D026D1F61d36fcB40C**0FaD8**
Transaction Hash: 0x80ee4301d045b76eaf809cd199706e71111364f4d1615a22fcbd06622b775bdf
Date: 07-12-2022 01:02:45 PM
Amount USDT: 277,777
Sent to wallet address: 0xaF9e1FF950337CB623A12467301d63c3ce803005 **(wallet ending in 03005)**
Transaction Hash: 0x9b2f552bd60321c6fb6f2997a3315de09007fe0771790eed9877cf989368cf0a
Date: 07-18-2022 01:38:01 PM
Amount USDT: 306,834
Sent to wallet address: 0xaF9e1FF950337CB623A12467301d63c3ce803005 **(wallet ending in 03005)**
Transaction Hash: 0xe3441d96ebb7a32fa760f1ac66d5d0e774eb4e9d3178480856358d5048e5e2c8

Figure 8

56. A listing of the transactions to the second path of intermediary wallets involving Victim-1's funds can be found in Figure 9 below, with times shown in UTC:

Date: 08-26-2022 01:34:35 PM
Amount USDT: 69,108
Sent to wallet address: 0x7B9a5d1bd2Fbc798288d464Be5a5d9DC3a5**781F4**
Transaction Hash: 0xab03a5575fc55f7d02bfc3ae9b92ca5378b9f71a8a209832d278886f73bc0bc5
Date: 08-27-2022 03:53:36 AM
Amount USDT: 761,490
Sent to wallet address: 0x3C9c8419Dc58DCB42E25244c9e9f415DA7C**C450B**
Transaction Hash: 0x5176ad21f8aa74245aa68bbbd52c5d3d5c6b0781bd5683838bf9ee80138f9c88
Date: 08-29-2022 12:16:02 PM
Amount USDT: 500,000
Sent to wallet address: 0xf83805F87B87762A7D2212535345FD27181**FfE12**
Transaction Hash: 0x0ea7c1c0854f6b81e98abc0b305a49d88dc1707a9a808a80d409d6aef741ba7c
Date: 08-29-2022 12:38:09 PM
Amount USDT: 141,242
Sent to wallet address: 0x77dD8AfBAcab3Ee5dee9d87922bfc79E5E1**7FB5B**
Transaction Hash: 0xa5ed01bf8f895671a8f1cf423083829965aed90395d2c36d553afd600463e5d2
Date: 08-29-2022 12:41:53 PM
Amount USDT: 141,242
Sent to wallet address: 0x387A2C6497A92F792020EE4c5a309e97650**B4fA8**
Transaction Hash: 0xecf2415866babe7dcb3529467c5a66345a11e9851ac4f2df30fe98472a5a24a2
Date: 08-30-2022 05:16:11 AM
Amount USDT: 83,033
Sent to wallet address: 0xaF9e1FF950337CB623A12467301d63c3ce803005 **(wallet ending in 03005)**
Transaction Hash: 0x3f98df688c5d0989a05806cbbd0da40edb0454c88bf01f85e8ec2655ac60eb74
Date: 08-30-2022 09:59:34 AM
Amount USDT: 600,000
Sent to wallet address: 0x1843F862226a572Ba981E6181e472C1Bc7B**7f33D**
Transaction Hash: 0x1c8f86af0dce5ddb7f8dedf446ddae98972c42eb9789b163704db95b4d2686cc
Date: 09-02-2022 04:02:12 PM
Amount USDT: 197,805
Sent to wallet address: 0xaF9e1FF950337CB623A12467301d63c3ce803005 **(wallet ending in 03005)**
Transaction Hash: 0xfe1312f7db965b1401f704d8fc26cd3650f4742d77f8971beec9a38ca4bd4ad3

Figure 9

57. A visual depiction containing the transfers identified in Figures 8 and 9 above, are reflected in Attachment C.

Laundering the Fraud Proceeds to ACCOUNT-2:

58. The scam detailed in this affidavit is largely consistent with a criminal organization employing an emerging fraud trend involving promising victims high returns in cryptocurrency investments, coined as "Pig Butchering". This type of scheme often begins with a scammer sending a victim a message, initiating contact through various social media platforms like LinkedIn, Match.com, and Facebook. The scammer then quickly establishes a personal relationship with the victim, using emotionally manipulative tactics similar to those used in online romance scams.

59. The scammers will use elaborate storylines to convince the victim into believing they are in a relationship. Once the victim reaches a certain point of trust, they are brought into a cryptocurrency investment scheme and are provided with fabricated information to bolster the scheme's legitimacy. The fabricated information includes, but is not limited to:

a. A fake investment platform via a website or mobile application that displays fictious investment options. In reality, the website or application has limited functionality and does not allow the user any access to a cryptocurrency wallet.

b. Fabricated investment gains that are displayed on the investment platform website or mobile application. In actuality, the investment platform does not exist.

c. A demand to pay the fake investment platform "taxes" or "fees" on the value of the account before they can withdraw funds (and, even if they pay these "taxes" or "fees", the victims will be unable to withdraw the funds).

60. The scam culminates once the victim assets are stolen by the criminals. In this instance, both Victim-1 and Victim-2 were each contacted by different online personas who claimed to have investment experience and knowledge of lucrative cryptocurrency trading opportunities. Based on my knowledge and experience conducting cryptocurrency fraud investigations, I know that criminal organizations often operate in multiple tiers of responsibility. Most often, the individual that communicates directly with the victim is on a lower tier of responsibility in the criminal organization, whereas individuals receiving funds at the end of the scheme are those who profit the most and are typically higher in the criminal organization's hierarchy.

61. Based on my knowledge and experience, and conversations with other investigators familiar with these types of cyber fraud schemes, the online personas that contacted Victim-1 and Victim-2 are not likely the individuals they portrayed themselves to be, rather a persona that can, and often is, played by more than one person.

62. Though originating in China, law enforcement has determined that criminal organizations utilizing "Pig Butchering" type tactics are more recently located in Southeast Asia, including Hong Kong, Myanmar, Cambodia, Malaysia, Thailand, and Singapore. In this case, the Binance account records of **ACCOUNT-2** receiving the victim funds detailed in this affidavit, show IP access logs for **ACCOUNT-2** were accessed by Thailand, Singapore, and Hong Kong-based IP addresses.

63. Additional review of Binance account records indicate **ACCOUNT-2** had approximately 14 approved devices. These are devices that have accessed the account. This is indicative of money laundering, as criminal organizations will often have one member of the group set up an account utilizing their identification documentation for KYC to obtain access to the

platform account. Once the access is obtained, the account will be shared amongst several different devices, by different group members who host different roles in the organization, much like the use of a money mule.

64. A review of the transactions containing victim funds show the organization's controllers over the provided wallets displayed tactics typically used in money laundering transactions for the purpose of attempting to conceal the origin of fraud proceeds. Specifically, the fraudsters obfuscated linear lines of blockchain transactions, separated victim proceeds, and co-mingled victim proceeds with other funds of unknown origin. **ACCOUNT-2** received four separate deposits totaling 865,449 USDT, containing victim proceeds obtained from Victim-1. of approximately 176,350 USDT.

65. The organization controlling the movement of fraud proceeds utilized private wallet addresses for the token movements, which is also indicative of money laundering tactics that are used to conceal and disguise the source of originating victim funds. Private wallets are non-custodial wallets, meaning the owner, as opposed to an exchange, application, or provider, controls the private keys and therefore all associated funding. Private, non-custodial wallets can be held in numerous forms such as, wallet applications on computers and cell phones, cold storage devices not connected to the internet, and paper wallets.

66. Additionally, the number of movements between accounts in these transactions appear to lack ostensible business purpose, with several movements between accounts occurring in rapid succession, which further establishes probable cause to believe that the transfers were coordinated and intended to obscure the control, ownership, source, and purpose of the funds involved in said transfers.

67. Further, a search of law enforcement databases yields numerous fraud reports associated with many of the intermediary wallets that transferred Victim-1's funds, as well as the "Deribit" application Victim-1 was instructed to utilize.

68. Finally, additional activity indicative of money laundering is found upon review of the deposit history of **ACCOUNT-2**, indicating the account received tokens from cryptocurrency addresses associated with fraud reports found in law enforcement databases.

Review of Binance Records relating to ACCOUNT-2:

69. After reviewing Attachment C and other facts of this investigation, I was able to identify that after multiple intermediary transfers, 865,449 USDT of Victim-1's commingled funds were ultimately transferred to **wallet address ending in 03005**. I contacted Binance for information relating to these transactions of Victim-1's funds into **wallet address ending in 03005** and obtained account records for one Binance account. The Binance records reflect that the transfer of Victim-1's funds into **wallet address ending in 03005** (referenced in Figures 8, 9 and Attachment C) is attributable to Binance account user ID number XXXX1519, also known as **ACCOUNT-2**, which was registered utilizing the email address 13950006006@qq[.]com. **ACCOUNT-2** was opened on or about November 28, 2020. Account records show that from account opening to present, 765 transfers totaling approximately 906,309,928 USDT were deposited into the account. In addition, 133 transfers totaling approximately 62.4821 BTC were deposited into the account. This level of activity is indicative of an account controlled by a criminal organization for the purpose of laundering stolen funds.

70. Of the amounts held in **ACCOUNT-2**, the Government seized 11,146.8079 USDT and 18.9649 BTC. As stated above, 176,350 USDT is attributable to proceeds of wire fraud that

were traced and transferred from Victim-1 and the additional funds have been co-mingled in this money laundering transaction, and therefore, are involved in money laundering.

71. Based on the above analysis, and my training and experience, I have probable cause to the believe that 11,146.8079 USDT and 18.9649 BTC in **ACCOUNT-2** are proceeds of wire fraud and/or funds involved in money laundering, in violation of 18 U.S.C. § 1343 and 18 U.S.C. § 1956(a)(1)(B)(i) respectively, and are subject to forfeiture.

CONCLUSION

72. Based on the information set forth above, I believe there is probable cause that the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) and 18 U.S.C. § 981(a)(1)(A) because it represents proceeds traceable to a scheme to defraud in violation of 18 U.S.C. § 1343 (Wire Fraud) and property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (Laundering of Monetary Instruments) or property traceable to such property, all as part of an online cryptocurrency investment scam.

Pursuant to 28 U.S.C. § 1746, I declare under the penalties of perjury that the foregoing is true and correct to the best of my knowledge, information, and belief.

Executed this 20th day of November, 2023.

Heidi Robles

Special Agent Heidi Robles
United States Secret Service