CV-23-147-TUC-MSA

AFFIDAVIT

I, Special Agent Nathan Wood (Affiant), Federal Bureau of Investigation, having been duly sworn, declare and state as follows:

INTRODUCTION

1. Based on the information in this affidavit, I believe there is probable cause to believe the cryptocurrencies seized from the following Target Binance Account were involved transactions or attempted transactions in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) (Money Laundering) and 1956(h) (Conspiracy to Commit Money Laundering), and constitute or were derived from proceeds traceable to violations of 18 U.S.C. §§ 1343 (Wire Fraud), 1349 (Conspiracy to Commit Wire Fraud), 1956(a)(1)(B)(i) (Money Laundering), and 1956(h) (Conspiracy to Commit Money Laundering), and are therefore subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (a)(1)(C).

Seized from Binance User ID 438672410:

Currency Name	Currency Code	Balance
USDT	TetherUS	1,150,049.51316
ETC	Ethereum Classic	59,939.992

BACKGROUND OF AFFIANT

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since May 2018. I have received training at the Basic Field Training Course in Quantico, Virginia, with the FBI. My current responsibilities include investigating complex financial crimes and other related fraud and financial crimes. I am currently assigned to the

Tucson, Arizona Resident Agency, which is part of the Phoenix Division Field Office of the FBI. Since graduating from the FBI Academy, my experience as an FBI agent includes conducting physical surveillance, debriefing informants, interviewing witnesses, subjects, and victims of crimes, as well as executing dozens of search and arrest warrants. I have coordinated and collaborated with other law enforcement agencies in ongoing investigations.

3. Prior to becoming a Special Agent with the FBI, I worked eleven years as a Trooper with the Utah Highway Patrol in different counties across the state. As a Trooper, my experience included investigating criminal offenses such as domestic violence, drug related offenses, and traffic violations. I have earned two bachelor's degrees, with one in Intelligence Studies/Counterintelligence in June of 2016, and the second in Computer Security/Cyber Security in November of 2020, both from American Military University.

4. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not set forth all of my knowledge about this matter. All dates are on or about the date specified. All amounts are approximate.

BACKGROUND ON CRYPTOCURRENCY

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

a. 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 (i.e. national currencies like the dollar, euro, yen, etc) currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. 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 (described below) 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. 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[1]. Cryptocurrency is not illegal in the United States.

b. Bitcoin[2] ("BTC") is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained

[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.

[2] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it's not completely anonymous, bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

c. Tether ("USDT"), USD Coin ("USDC"), Ethereum ("ETH"), Wrapped Bitcoin ("WBTC") and Ethereum Classic ("ETC") are types of cryptocurrencies.

d. 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, 26–25 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.

e. Although cryptocurrencies 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 on hidden services websites. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transfers, trades, purchases, and other financial transactions.

f. 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. Moreover, 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). In addition, paper wallets contain an address and a QR code[3] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, 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). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

g. "Exchangers" and "exchanges" are individuals or companies that exchange cryptocurrencies for other currencies, including U.S. dollars. According to Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services

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

businesses.[4] 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. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

h. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A

[4] 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.

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; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

i. Binance Holdings Limited ("Binance"), Coinbase, Inc. ("Coinbase"), Gemini Trust Company, LLC ("Gemini") and Foris Dax, Inc. ("Crypto.com") are cryptocurrency exchanges.

j. imToken is digital wallet with multi-chain asset management. Tokenlon is imToken's trading platform, which provides swapping of tokens.

FACTS

6. The FBI Phoenix Division, Tucson Resident Agency ("TRA") field office is investigating an investment fraud scam, commonly referred to as "Pig Butchering,"

perpetrated on many victims throughout the Tucson, Arizona (United States) area as well as many victims located throughout the United States. The investment fraud scam typically begins when the victims are contacted through social media platforms or messaging services. From there, the scammer often establishes a more personal relationship with the victim using manipulative tactics similar to those used in online romance scams. The victims are directed to fraudulent websites and to download an application from the internet. The victims are then instructed to invest funds by making cryptocurrency purchases and transferring the cryptocurrency to wallet addresses controlled by the scammers. After the cryptocurrency transfers occur, the fraudulent investment platform website or application reflects the victims' deposits. For the next month or so, the fraudulent investment platform website or application appears to reflect large financial gains in the victims' accounts, often times causing the victims to invest additional funds. However, the investment gains displayed on the fraudulent investment platform website or application are fabricated. When the victims attempt to withdraw their funds, they are told they are unable to by the fraudulent investment platforms' "customer service" team, which gives the victims various excuses as to why the funds are unable to be withdrawn and, in some cases, instructs the victims to pay additional fees under the guise that such fees will allow a release of the victims' funds. After a period of time, the victims are locked out of their accounts and lose all of their funds, ultimately causing the victims financial and emotional ruin.

7. From the approximate dates of December of 2021 to present, the FBI TRA has identified at least 32 victims located throughout the United States that have lost at least $20 million in U.S. currency due to a Pig Butchering scam that uses multiple different fraudulent

websites and platforms. As outlined in detail below, money from 11 of these victims flowed into either the Target Binance Account or one of the primary intermediary accounts that funneled other fraud proceeds to the Target Binance Account. The victims are all linked together through the tracing of their funds to the same destination. One of the victims, R.T. lives in Tempe, Arizona and reported losing approximately $430,000 of his savings to the online investment scam. R.T. and the other victims were defrauded of funds which were laundered through the primary intermediary accounts before being seized from the Target Binance Account.

8. This affidavit supports the forfeiture of fraud proceeds extracted from at least 11 identified victims, which have been seized from Binance account User ID 438672410 in the name of HAIQIANG LU.

This seizure consists of cryptocurrencies in the amount of 1,150,049.51316 USDT and 59,939.992 ETC.

Tracing of Victims' Funds Through Various Cryptocurrency Accounts

9. An FBI Forensic Accountant traced the movement of the cryptocurrency transactions in this case. Cryptocurrency transactions are visible as opensource blockchain data on the internet. My affidavit does not include all of the blockchain analysis, but rather focuses on the tracing of the victims' funds. The cryptocurrency transactions included in this affidavit demonstrate the movement of the funds from the victims' exchange accounts, through multiple intermediary wallet addresses, to the identified Target Binance Account or two of the intermediary wallet addresses closely linked to the Target Binance Account, which I refer to as the two Malaysian Intermediary Accounts.

10. The intermediary wallet addresses often had multiple cryptocurrency transactions, but the cryptocurrency transactions shown in the below tables only include the deposit of the victims' funds into the wallet addresses and then withdrawals out of the wallet addresses that included the victims' funds. There are instances where the victims' funds are comingled with other funds in the intermediary wallet addresses; however, the transfer out of the wallet addresses includes the victims' funds. The movement of the victims' funds to wallet intermediary addresses are referred to as "hops" between wallet addresses. In my training and experience, these "hops," which often occurred on the same day and close in time to each other, are a common method to engage in concealment money laundering and attempt to thwart law enforcement efforts at tracing fraud proceeds.

Victim G.C. and L.L. and the Two Malaysian Intermediary Accounts

11. Two of the scam victims, one of whom was directed to make investments through the fraudulent massusa.com website, had their funds unwittingly transferred to the two Malaysian Intermediary Accounts closely linked to the Target Binance Account.

12. On April 21, 2022, the FBI TRA interviewed victim G.C., via telephone, as G.C. currently resides in Southbury, Connecticut. In January of 2022, G.C. met an Asian woman on the social platform, LinkedIn. G.C. began an online relationship with the Asian woman he knew as "Wendy Yu" (SUSPECT #1). SUSPECT #1 had pictures on her profile that depicted a lavish lifestyle which intrigued G.C. SUSPECT #1 told G.C. she was able to afford such a lifestyle by trading cryptocurrency and wanted to show G.C. how to do the same. SUSPECT #1 showed G.C. step-by-step on what software to download and how to use the cryptocurrency exchange Gemini. G.C. made a few small investments at first to become "comfortable" in

making cryptocurrency trades and made his trades by creating an account with the website: https://www.massusa.com, at the direction of SUSPECT #1. After seeing an immediate return on his investment, SUSPECT #1 pressured G.C. to invest even more, stating "the more you invest the bigger the return."

13. From February 17, 2022, to March 11, 2022, G.C., under the direction of SUSPECT #1, transferred $450,000 from his personal savings account into Gemini, purchased cryptocurrency, and then transferred the cryptocurrency into a wallet address controlled by massusa.com. Using the Gemini exchange, G.C. attempted to make a withdrawal from his massusa.com account, but he was told he was not able to withdraw his funds and shortly after his account balance was zero. G.C. made many unsuccessful attempts to contact SUSPECT #1 to confront her about his funds. G.C. made the following deposits at the direction of SUSPECT #1:

Date Wire Sent to Exchange	Dollar Amount of Wire Sent to Exchange	Name of Bank/Institution Wire Originated	Name of Exchange Wire Deposited Into
February 17, 2022	$ 50,000.00	Wells Fargo	Gemini
February 28, 2022	$100,000.00	Wells Fargo	Gemini
March 11, 2022	$300,000.00	Wells Fargo	Gemini

14. On July 1, 2022, the FBI New York Division interviewed L.L., in person at the FBI New York office along with L.L.'s husband. It was learned that on March 31, 2022, L.L. had a LinkedIn social profile and was approached by "Peter Lei" (SUSPECT #2). L.L. was from Changsha, China and SUSPECT #2 claimed he was also from Changsha, China and used

this as a way to connect with L.L. SUSPECT#2 claimed to work for a cryptocurrency company and urged L.L. to invest in cryptocurrency via the website: https://www.directedgebro.com. SUSPECT #2 explained to L.L. that directedgebro.com could trade in futures and taught L.L. how to trade using the website. SUSPECT #2 told L.L. the more she invested into directedgebro.com the more time she would have to place trades on the website.

15. From April 13, 2022, to May 9, 2022, SUSPECT #2 instructed L.L. to transfer approximately $865,000 from her savings and IRA accounts into Coinbase, purchase cryptocurrency, and then transfer the cryptocurrency into a wallet address controlled by directedgebro.com. On May 10, 2022, after making a profit, L.L. attempted to transfer her investment from directedgebro.com but was unsuccessful. L.L. contacted the website's customer service and was advised she needed to pay a 37% tax on profit to the website. On May 13, 2022, L.L. under the instruction of the directedgebro.com customer support representative, transferred another $100,000 U.S. currency to Coinbase to purchase cryptocurrency and then transfer the cryptocurrency to a wallet address controlled by directedge.com. All of L.L.'s cryptocurrency deposits were into wallet addresses provided to her by SUSPECT #2 and the website. After L.L. paid the "tax fees," she was then advised she still needed to pay an additional $277,000 in additional taxes before she could access her funds. When L.L. confronted SUSPECT #2, he denied having any part of the website and claimed he also had his funds stolen. L.L. lost a total of $965,000 in the investment scam. L.L. made the following deposits at the direction of SUSPECT #2:

Date Wire Sent to Exchange	Dollar Amount of Wire Sent to Exchange	Name of Financial Insitution	Name of Exchange Wire Deposited
April 13, 2022	$ 100,000.00	Merril Lynch IRA	Coinbase
April 20, 2022	$ 350,000.00	Merril Lynch IRA	Coinbase
April 20, 2022	$ 50,000.00	Bank of America	Coinbase
April 26, 2022	$ 50,000.00	Bank of America	Coinbase
April 29, 2022	$ 170,000.00	Charles Schwab	Coinbase
May 2, 2022	$ 80,000.00	Fidelity	Coinbase
May 6, 2022	$ 25,000.00	Charles Schwab	Coinbase
May 6, 2022	$ 40,000.00	Bank of America	Coinbase
May 13, 2022	$ 100,000.00	Bank of America	Coinbase
TOTAL	**$965,000.00**		

16. As outlined below, G.C.'s and L.L.'s "investments" through the fraudulent websites, including massusa.com, were transferred through various intermediary wallet addresses, including the two Malaysian Intermediary Accounts closely linked to the Target Binance Account.

17. G.C.'s transfer on or about March 11, 2022, from his Gemini account in ETH was to wallet address 0xD9f2...e18F.:

Transaction Hash	Timestamp	Amount	Wallet Address
0x6c1ac6003acc48aeed855b0d75145db3afb0c50be9238144cd8b52516316eeba	03/11/2022 9:28:18 PM	115.068333	0xD9f2...e18F
0xbd5989d7bdc734882179a3949324c73fb6b2c7f195a91fb5540feb6a53e0ab6d	03/11/2022 10:23:52 PM	(115.0683)	0x8462...Bcb6

a. The next hop with G.C.'s funds in ETH was:

Transaction Hash	Timestamp	Amount	Wallet Address
0xbd5989d7bdc734882179a3949324c73fb6b2c7f195a91fb5540feb6a53e0ab6d	03/11/2022 10:23:52 PM	115.0683	0x8462...Bcb6
0x731532af7d9827f5ac1436a25f99beb13e15edb454404403ca1b24bf6dbb0b5f	03/11/2022 10:37:52 PM	(115)	0x03f3...9659

b. G.C.'s funds in ETH were then swapped for USDT by using Tokenlon in wallet address 0x8462...Bcb6 as shown below:

Transaction Hash	Timestamp	Amount	Wallet Address
0x731532af7d9827f5ac1436a25f99beb13e15edb454404403ca1b24bf6dbb0b5f	03/11/2022 10:37:52 PM	294,948.357205	0x8462...Bcb6
0xb8c3db2cfe50f444f347e0c02a69c848255cc262e391e3f9115632e3f19d6866	03/11/2022 11:46:25 PM	(297,895.7302)	0x5a49...B3fE

c. The next hop with G.C.'s funds in USDT was:

Transaction Hash	Timestamp	Amount	Wallet Address
0xb8c3db2cfe50f444f347e0c02a69c848255cc262e391e3f9115632e3f19d6866	03/11/2022 11:46:25 PM	297,895.7302	0x5a49...B3fE
0x2526356c0c0efd39cb843ea9de66ea7c807bfe614eaef24695598f5c2a7092e8	03/12/2022 7:01:55 AM	(1,028,648)	0xB0d1...fBC9

d. The next hop with G.C.'s funds in USDT was:

Transaction Hash	Timestamp	Amount	Wallet Address
0x2526356c0c0efd39cb843ea9de66ea7c807bfe614eaef24695598f5c2a7092e8	03/12/2022 7:01:55 AM	1,028,648	0xB0d1...fBC9
0x3c444768123c7d46c1f37d218c231430611e9338b0df9a78f5ec3fb4488ec0fd	03/12/2022 5:31:19 PM	(500,000)	0x949A...207e

18. According to records obtained from Binance, the deposit address 0x949A5293D487621184AE45A0E7cCF8d77a6D207e (0x949A...207e), that received some of G.C.'s funds, belongs to the following:

User ID: 421799405
Name: SIEW JIN WEI
KYC Document Issuer: Malaysia
Account Registration: March 12, 2022

According to the Deposit History report and Withdrawal History report provided by Binance for User ID: 421799405, from approximately March 12, 2022, through approximately June 18, 2022, the account demonstrated a recurring pattern of deposit of USDT followed by rapid withdrawals to external addresses. This account has no material remaining balance. As outlined below, this is one of the Malaysian Intermediary Accounts closely linked to the Target Binance Account.

19. L.L.'s transfer on or about April 13, 2022, from her Coinbase account in USDC was to wallet address 0x5274...f9a8:

Transaction Hash	Timestamp	Amount	Wallet Address
0x3d036ede8e84834f2e1460a85b5e38805c907c38d0daffd1827ac311369567ed	04/13/2022 6:04:58 PM	99,981.847646	0x5274...f9a8
0xf09eb292803f2a4f0805f157f3a1e23304f945b1092c632e893e6ab554e6475c	04/13/2022 6:10:11 PM	(99,981.847646)	0x60F6...26f4

a. The next hop with L.L.'s funds in USDC was:

Transaction Hash	Timestamp	Amount	Wallet Address
0xf09eb292803f2a4f0805f157f3a1e23304f945b1092c632e893e6ab554e6475c	04/13/2022 6:10:11 PM	99,981.847646	0x60F6...26f4
0xa8242974dea0ed7f44486db77926a03aa6727e38e1b1cdb80013911ebe8c493d	04/13/2022 6:16:10 PM	(99,981.8476)	0x4a14...650d

b. L.L.'s funds in USDC was then swapped for USDT by using Tokenlon in wallet address 0x60F6...26f4 as shown below:

Transaction Hash	Timestamp	Amount	Wallet Address
0xa8242974dea0ed7f44486db77926a03aa6727e38e1b1cdb80013911ebe8c493d	04/13/2022 6:16:10 PM	99,927.054565	0x60F6...26f4
0x95f87fb79e5b49aef57f9cf2400e8f08e19e2a4a96da9f0a30b1b832ab2b56c6	04/13/2022 6:28:39 PM	(99,927.054565)	0x3Edc...8330

c. The next hop with L.L.'s funds in USDT was:

Transaction Hash	Timestamp	Amount	Wallet Address
0x95f87fb79e5b49aef57f9cf2400e8f08e19e2a4a96da9f0a30b1b832ab2b56c6	04/13/2022 6:28:39 PM	99,927.054565	0x3Edc...8330
0x78452f4b24da0ec583c588b9531e7625e76512d8f6af272ac90448cd3f8bea75	04/14/2022 12:50:04 PM	(999,900)	0x681d...602D

d. The next hop with L.L.'s funds in USDT was:

Transaction Hash	Timestamp	Amount	Wallet Address
0x78452f4b24da0ec583c588b9531e7625e76512d8f6af272ac90448cd3f8bea75	04/14/2022 12:50:04 PM	999,900	0x681d...602D
0xc3fc596a6e62d5b68d518ec40ed0f402aed43c2e06f1cb717e106dacc7f72d6a	04/24/2022 2:25:36 PM	(300,000)	0x949A...207e
0xe4587831e7da27223d81569bb5860d8a1256f31823e9b8bf5fcedeea94606162	04/24/2022 2:26:35 PM	(300,000)	0xCE11...91C8
0x677d19c26b193efa5fb8d3c0708e56acfa7af2079ba6b3782cffb79e3a86ea4a	04/24/2022 2:36:14 PM	(350,000)	0x949A...207e
0x0b0779f66d09e975713f36775f1a7b5a983e34f191c1a0e76b38edf922e618e3	04/24/2022 2:37:19 PM	(350,000)	0xCE11...91C8

20. As shown above, some of L.L.'s funds were deposited into 0x949a...207e, which is the deposit address for Binance User ID: 421799405. This is the same Binance account that some of G.C.'s funds were deposited into. In addition, some of L.L.'s funds were deposited into 0xCE11...91C8.

21. According to records obtained from Binance, the deposit address 0xCE11d194D57A093C62Fb638b907394fdC97091C8 (0xCE11...91C8) belongs to the following:

User ID: 421798906
Name: LAY FOOK CHUEN
KYC Document Issuer: Malaysia
Account Registration: March 12, 2022

According to the Deposit History report and Withdrawal History report provided by Binance for User ID: 421798906, from approximately April 24, 2022, through approximately May 20, 2022, the account demonstrated a recurring pattern of deposit of USDT followed by rapid withdrawals to external addresses. This account has no material remaining balance. This is the other Malaysian Intermediary Account closely linked to the Target Binance Account.

22. As noted above, the two Malaysian Intermediary Accounts both have an account registration date of March 12, 2022. In addition, Binance provided the approved devices that have accessed these Binance accounts. According to Binance, device_uuid is the UUID for the app installation on MacOS or iOS. If a user uninstalls and reinstalls the app, the UUID will change. Also, bnc-uuid is a unique identifier Binance calculates for Android and other clients (non-web) to detect the same device between small changes in device characteristics. Below

is some of the information that Binance provided about the approved devices for the two Malaysian Intermediary Accounts:

	SIEW JIN WEI (User ID: 421799405)	LAY FOOK CHUEN (User ID: 421798906)
app_install_date	2022-03-12 20:06:24	2022-03-12 20:06:24
device_uuid	6ED08D02-D86C-4350-89D6-A8104F3A7159	6ED08D02-D86C-4350-89D6-A8104F3A7159
bnc-uuid	6ED08D02-D86C-4350-89D6-A8104F3A7159	6ED08D02-D86C-4350-89D6-A8104F3A7159
brand_model	iPhone 11	iPhone 11

The same account registration date and the same approved device information shown above indicates that the same individual controls both Malaysian Intermediary Accounts.

23. A review of the Withdrawal History report for the two Malaysian Intermediary Accounts revealed that both Binance accounts withdrew funds to an external address TBgsF7BuW2fksDx4wLgExgUHvtC1s75cgy (TBgsF7...5cgy). The transactions in TBgsF7...5cgy showing the transfers from the two Malaysian Intermediary Accounts were:

Transaction Hash	Timestamp	Amount	Wallet Address
c4f8b0d3ee1100672a43d4fe6dfacfbb12ae904fb51f06c3f807dbb810e0d54c	05/05/2022 7:09:33 AM	200,434	TBgsF7...5cgy
521b675de9063ed4aa4c0be2a33043d377dd5e27d824bd8fec1baaadb1c9fff2	05/05/2022 7:10:42 AM	200,499	TBgsF7...5cgy
2dd8681a492abdb9a7e3f9e40614e8c500d865e8f7c5a4ac9bebb8434b473e9f	05/05/2022 4:12:57 PM	174,426	TBgsF7...5cgy
b72e46e57da401e1912aeb4cb1874db76cd92bad6570708dfb02f340086ed7b5	05/05/2022 4:14:33 PM	(558,133)	TPbxGy...d4CL

24. As shown in this table, the funds from TBgsF7…5cgy were, in turn, transferred to wallet address TPbxGy…d4CL. According to records obtained from Binance, the deposit address TPbxGyY2cHc4ie1pWZmQ1Z4kBwtMgQd4CL (TPbxGy...d4CL) belongs to the following:

User ID: 438672410
Name: HAIQIANG LU
KYC Document Issuer: Vanuatu
Account Registration: April 15, 2022

This is the Target Binance Account, which had a balance of 1,150,049.51316 USDT and 59,939.992 ETC.

25. The Target Binance Account has two wallet addresses associated with the account: TPbxGy…d4CL (as shown above), and 0xc4a31336a25602cccf86db9a692059354d950a16 (0xc4a3…0a16). As outlined in detail below, through review of the Deposit History report for the Target Binance Account, blockchain analysis, obtaining records from exchanges, and interviews conducted, the FBI was able to determine that the Target Binance Account received stolen funds from at least 4 victims into deposit address 0xc4a3…0a16 totaling 1,104,882 USDT, or approximately $1.1 million U.S. dollars. In addition, the FBI was able to determine that the Target Binance Account received stolen funds from at least 7 additional victims which were routed through the two Malaysian Intermediary Accounts before being transferred into the Target Binance Account's deposit address TPbxGy...d4CL totaling 558,133 USDT, or approximately $558,000 U.S. dollars.

4 Victims' Stolen Funds Transferred to Target Binance Account Wallet Address 0xc4a3…0a16

26. On September 29, 2022, the FBI TRA interviewed D.C., who is 81 years old, via telephone, as D.C. currently resides Irvine, California. In April of 2022, D.C. was contacted by someone named "Coco" who also went by "Alice" (SUSPECT #3) on an online application called Line. D.C. and SUSPECT #3 communicated for several weeks. SUSPECT #3 represented herself as a young attractive woman from Beijing who had lived in the states for the past seven years and who had recently moved from Miami, Florida to Irvine, California.

During their conversations, SUSPECT #3 brought up cryptocurrency. D.C. had no knowledge on how to invest in cryptocurrency, and therefore had to rely on what he was being told and instructed by SUSPECT #3. In April and May of 2022, D.C. was convinced by SUSPECT #3 to cash out his 401k valued at $130,000, to take out a $35,000 bank loan, and cash out the rest of his savings account and invest it all into cryptocurrency. D.C. estimated he lost $300,000 in the scam; the investigation was able to document approximately $250,000 in transactions.

27. SUSPECT #3 directed D.C. to websites https://www.cbot.com and https://www.comexant.com and instructed D.C. step-by-step on how to transfer his money into cryptocurrency and eventually into a cryptocurrency wallet address controlled by cbot.com. When D.C. attempted to withdraw his funds from the two websites, he was told he was unable to complete the withdrawal without first paying a tax on his earnings. D.C. made the following deposits at the direction of SUSPECT #3:

Date Wire Sent to Exchange	Dollar Amount of Wire Sent to Exchange	Name of Bank/Institution Wire Originated	Name of Exchange Wire Deposited Into
April 29, 2022	$ 49,990.00	Chase Bank	Coinbase
May 10, 2022	$200,080.00	Chase Bank	Coinbase

28. On October 3, 2022, the FBI TRA interviewed D.M. via, telephone, as D.M. currently resides in Roswell, Georgia. D.M. was referred to an investment opportunity by his friend who had a contact (SUSPECT #4) that was an "expert" in cryptocurrency trading and could predict future trends by analyzing the current market trades. D.M. communicated with SUSPECT #4 via WhatsApp and was instructed to download an app called Phemex and

Coinbase. D.M. did not know anything about cryptocurrency trading and relied entirely upon what SUSPECT #4 was telling and instructing him to do. Because D.M. did not know much about trading, he initially only invested $10,000. Soon after this deposit, D.M. made a profit on his trades and was even able to withdraw $6,500 of his funds and transfer them back into his Coinbase account. After the withdrawal, D.M. made two more deposits that totaled approximately $45,000. D.M. was instructed by SUSPECT #4 to make all his cryptocurrency deposits into specific wallet addresses. D.M. felt "forced" into making more investments and was told "the more you invest the more you are able to trade." D.M. decided he was done with trading and tried to withdraw his funds from the website. When D.M. attempted to withdraw his funds, he was told he was not eligible because he did not trade enough, and despite making more trades, he was still unable to withdraw his funds. D.M.'s friend who introduced him to SUSPECT #4, was also a victim to this scam, but not listed in this affidavit. D.M. made the following deposits:

Date Wire Sent to Exchange	Dollar Amount of Wire Sent to Exchange	Name of Bank/Institution Wire Originated	Name of Exchange Wire Deposited Into
April 20, 2022	$ 9,990.00	USAA Federal Savings Bank	Coinbase
April 28, 2022	$ 39,990.00	USAA Federal Savings Bank	Coinbase

29. On September 08, 2022, the FBI TRA interviewed B.F. via telephone as B.F. currently resides in San Clemente, California. B.F. was introduced to an Asian woman who went by the name of "Ann" (SUSPECT #5), by his uncle who met SUSPECT #5 over the social media platform, LinkedIn. B.F. communicated with SUSPECT #5 via WhatsApp.

SUSPECT #5 told B.F., his uncle, and his father, who are all victims of this scam, that she had an uncle by the name of "Yi Chen Zhang," who was able to buy blockchain data to analyze and use that data to help predict future trends in the market. B.F., his father, and uncle all were directed by SUSPECT #5 to websites Phenexibn.com and Minedigital.com and he was told to makes deposits to Coinbase and then into wallets given to them by SUSPECT #5. B.F. made profits from his trades under the guidance of SUSPECT #5 and her uncle. When B.F. tried to withdraw his funds, he was given many excuses such as he needed to pay a tax and he did not meet the eligibility because the number of his trades were too low. B.F. invested and estimated his loss of approximately $300,000 of his savings and money. Through the investigation it was documented B.F. made the following deposits:

Date Wire Sent to Exchange	Dollar Amount of Wire Sent to Exchange	Name of Bank/Institution Wire Originated	Name of Exchange Wire Deposited Into
April 21, 2022	$ 9,990.00	USAA Federal Savings Bank	Coinbase
April 28, 2022	$ 45,000.00	USAA Federal Savings Bank	Coinbase
May 24, 2022	$ 20,000.00	USAA Federal Savings Bank	Coinbase
May 27, 2022	$180,000.00	USAA Federal Savings Bank	Coinbase
August 12, 2022	$ 25,990.00	PNC Bank	Coinbase

30. On September 27, 2022, the FBI TRA interviewed J.P., who is an elderly victim of 74 years old, via telephone as he currently resides in Claremont, California. J.P. was approached by a woman who went by the name of "Sophia" (SUSPECT #6) on WhatsApp. SUSPECT #6 introduced J.P. to cryptocurrency trading and directed him to the trading website

https://www.cbot.com and https://www.webull.com. J.P. was instructed to download the applications Bitstamp, Crypto, and Coinbase, along with creating an account with cbot.com and webull.com. J.P. was shown how and when to make his trades on the websites. After J.P. made many trades and earned a big profit, he tried to make a withdrawal, but was told he was unable until he paid a tax on his earnings. The website also stated he needed to boost his account credit score in order to make any withdrawals, and in order to do that he needed to invest more money. J.P. made the following deposits:

Date Wire Sent to Exchange	Dollar Amount of Wire Sent to Exchange	Name of Bank/Institution Wire Originated	Name of Exchange Wire Deposited Into
April 27, 2022	$ 149,990.00	Comerica Bank	Coinbase
May 3, 2022	$ 264,990.00	Comerica Bank	Coinbase
May 4, 2022	$ 164,990.00	Comerica Bank	Coinbase

31. A portion of J.P., D.C., D.M., and B.F. stolen funds went into deposit address 0xc4a3…0a16 for the Target Binance Account according to blockchain analysis as shown below.

a. Both J.P. and D.C. had funds in BTC that were transferred to 33Y61L...eMSz:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
1227af9143e40f3fca6d43c3344f51ea56b28e4efd56a04b6cdc6ce5a5e10ca6	04/27/2022 10:01:00 PM	3.79729165	33Y61L...eMSz	J.P.
b522c3730cd217cc44804ae65c1a3a374dd9054ce3ffdae53787d081009819d9	04/27/2022 11:18:00 PM	(3.79729)	3JMjHD...k8UG	
a2e07423bfeebe7fd94d040fb32f4d608eddb55cf6e8fe23216ba149f501b23e	05/02/2022 8:56:00 PM	0.68255788	33Y61L...eMSz	J.P.
d215923f7c6e1325cb7f485e136dba66009959e240f86be6d0d8c0dea96b4df4	05/02/2022 8:56:00 PM	1.26255379	33Y61L...eMSz	D.C
933b1bb82de3752b8a284cf3599294fa3adacca010d8175ab5aa620df284d5a2	05/02/2022 9:21:00 PM	(1.94509295)	3JMjHD...k8UG	
faf35650ae3a4095a67804b3a46c3d3cf92f6a8d344f97d486cbd15d068c0a4b	05/03/2022 7:26:00 PM	6.87905472	33Y61L...eMSz	J.P.
b633163d32e98d1595c4239374d60dc96afce888696c63c0b246fd9581dcb6f6	05/03/2022 7:32:00 PM	(6.87904632)	3JMjHD...k8UG	
c1d0ed0b4d998566b4a525f928e660876e65b03afdc44dacc4dd8225689498c6	05/04/2022 8:34:00 PM	3.94840367	33Y61L...eMSz	J.P.
cf78ffd27385467d25f7a981a00136a1afd5a1e1e5fbb21f702056cd2ab51be3	05/05/2022 7:52:00 AM	(3.94838967)	3JMjHD...k8UG	

b. J.P.'s and D.C.'s funds were then swapped for WBTC using imToken as shown below:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0xc3c972f4fdfd30b8a6bb3baa78e17b187a4da5ad08793f7d629b7c24a96c4a13	04/27/2022 11:38:59 PM	3.78894127	0xd39a...09bB	J.P.
0x28858828b828fac1c65812adbe491fdfe2c11a2afd859444f669103ff128784b	04/27/2022 11:40:55 PM	(3.7889)	0x8D90...13c6	
0xfefb680e2f82cc60f9132163d01e91d1b36d095d53db97699222b5a912f7e4a6	05/02/2022 10:05:29 PM	1.93868114	0xd39a...09bB	J.P. & D.C
0xe1edef6398d6fe3d4d19c776c67611e222d9f480775ed5ff4dfbf71ee42c77e0	05/02/2022 10:15:33 PM	(1.9386)	0x8D90...13c6	
0x6d1a810c531db2eac0cc7826cd081d57b38576f13987413bd02ff6968e39ef8a	05/03/2022 8:01:27 PM	6.86392204	0xd39a...09bB	J.P.
0x64cfed7145d6945279539f78bc8e16be205542b79ef6e2e9ac287973958eb9af	05/03/2022 8:06:02 PM	(6.8639)	0x8D90...13c6	
0x75e32fd48236c4d48757fdde4fab424b013058f6cf07641933a86b106c800ed4	05/05/2022 8:22:19 AM	3.93970873	0xd39a...09bB	J.P.
0x8f062c0a350c432e3dd708ed79a72b018f13f0a65597227eff021dc83da5234b	05/05/2022 1:09:47 PM	(4.796)	0x4a14...650d	

c. J.P.'s and D.C.'s funds were then swapped for USDT by using Tokenlon as shown below:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x28858828b828fac1c65812adbe491fdfe2c11a2afd859444f669103ff128784b	04/27/2022 11:40:55 PM	147,998.581706	0xd39a...09bB	J.P.
0x9a55494038f56a4a42a9f51aa24725bf5897a0646824c08913e7e501217d1ea6	04/28/2022 12:02:33 AM	(147,998.581706)	0x034B...AEeF	
0xe1edef6398d6fe3d4d19c776c67611e222d9f480775ed5ff4dfbf71ee42c77e0	05/02/2022 10:15:33 PM	75,066.464264	0xd39a...09bB	J.P. & D.C
0xc5d24b74bfa3056b368c9d3699595e27de37d654ae3494cb0a85f5ab34224816	05/03/2022 12:12:40 AM	(75,066.4642)	0x034B...AEeF	
0x64cfed7145d6945279539f78bc8e16be205542b79ef6e2e9ac287973958eb9af	05/03/2022 8:06:02 PM	257,602.067108	0xd39a...09bB	J.P.
0xd53b22377939c2df593c0715386c3912639fa15d943b89f4a561a83726a5345c	05/03/2022 8:12:45 PM	(257,602.0671)	0x034B...AEeF	
0x8f062c0a350c432e3dd708ed79a72b018f13f0a65597227eff021dc83da5234b	05/05/2022 1:09:47 PM	188,468.304097	0xd39a...09bB	J.P.
0xcc461c78c83d50e75eb56a90714ec1e61e9d562657d6a29316051c282ae6a7a4	05/05/2022 3:29:30 PM	(188,468.3039)	0x034B...AEeF	

d. Both D.M. and B.F. had funds in BTC that were transferred to 39Es4h...yZyg):

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
90a17411d2c03eaf928c2e66440c00ae920581040f779024db5baf46ffa1013c	04/28/2022 8:30:32 PM	0.97839784	39Es4h...yZyg	D.M.
411e0f9345a14a8a06fa17cede35dda7092e3f8870267b1faf9de0e5cffe28bd	04/28/2022 8:42:26 PM	1.12146669	39Es4h...yZyg	B.F.
811bbc3bd27a84c6ac4f20ad39db2199885330eec10eb74a4b9a7665f32c8a02	04/28/2022 11:00:21 PM	(2.09984789)	3JMjHD...k8UG	

e. D.M.'s and B.F.'s funds were then swapped for WBTC using imToken as shown below:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0xb1fc9a36bb0d31265de0967ef3c59a5060e417a3d0217f678a2eed2f04829fed	04/28/2022 11:47:30 PM	2.09481202	0xe86d...5d0f	D.M. & B.F.
0x846b2b3a3bd62d4c375d9dce6101d0ebab74e1faacc825705d766cc6bd52fd5b	04/29/2022 12:38:26 AM	(2.0948)	0x4a14...650d	

f. D.M.'s and B.F.'s funds were then swapped for USDT by using Tokenlon as shown below:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x846b2b3a3bd62d4c375d9dce6101d0eba b74e1faacc825705d766cc6bd52fd5b	04/29/2022 12:38:26 AM	80,989.17	0xe86d...5d0f	D.M. & B.F.
0xf76aafcafb9e9532335b2809c02bca2f97a 68c73bed26c79b8f78fdd85d92f7f	04/29/2022 12:57:02 AM	(80,989.17)	0x034B...AEeF	

g. Wallet address 0x034B...AEeF is the intermediary wallet address where the funds for all 4 victims above consolidated:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x9a55494038f56a4a42a9f51aa24725bf58 97a0646824c08913e7e501217d1ea6	04/28/2022 12:02:33 AM	147,998.581706	0x034B...AEeF	J.P.
0x5a56f2116032b70232e49b081cf7f0db5f4 692c1d36a12b0d94527ef845a4c7a	04/28/2022 5:47:20 AM	(179,034.00)	0x5E90...7aFD	
0xf76aafcafb9e9532335b2809c02bca2f97a 68c73bed26c79b8f78fdd85d92f7f	04/29/2022 12:57:02 AM	80,989.172837	0x034B...AEeF	D.M. & B.F.
0xa364712e585ac15b7d4e24b6a8f07239b bc08c94f729490ca1079c30acd55920	04/29/2022 6:15:21 AM	(100,744.00)	0x5E90...7aFD	
0xc5d24b74bfa3056b368c9d3699595e27d e37d654ae3494cb0a85f5ab34224816	05/03/2022 12:12:40 AM	75,066.4642	0x034B...AEeF	J.P. & D.C
0x94ff59c15575dc79ca9895b86390c0a643 6f6d294fd445eaa9b13c842b9c6bf6	05/03/2022 5:18:16 AM	(76,833.00)	0x5E90...7aFD	
0xd53b22377939c2df593c0715386c391263 9fa15d943b89f4a561a83726a5345c	05/03/2022 8:12:45 PM	257,602.0671	0x034B...AEeF	J.P.
0xc048670f3c55ca4f99d7ee703a94741433 39cb5e0e133779757dedfbdc2a654f	05/04/2022 6:03:08 AM	(287,910.00)	0x5E90...7aFD	
0xcc461c78c83d50e75eb56a90714ec1e61 e9d562657d6a29316051c282ae6a7a4	05/05/2022 3:29:30 PM	188,468.3039	0x034B...AEeF	J.P.
0x14957ee0676924e7359eac10d349f98c8 42fcc86087f29f3a1fc45808a1b5fda	05/05/2022 3:59:10 PM	(222,618.00)	0x29F9...0Cb9	

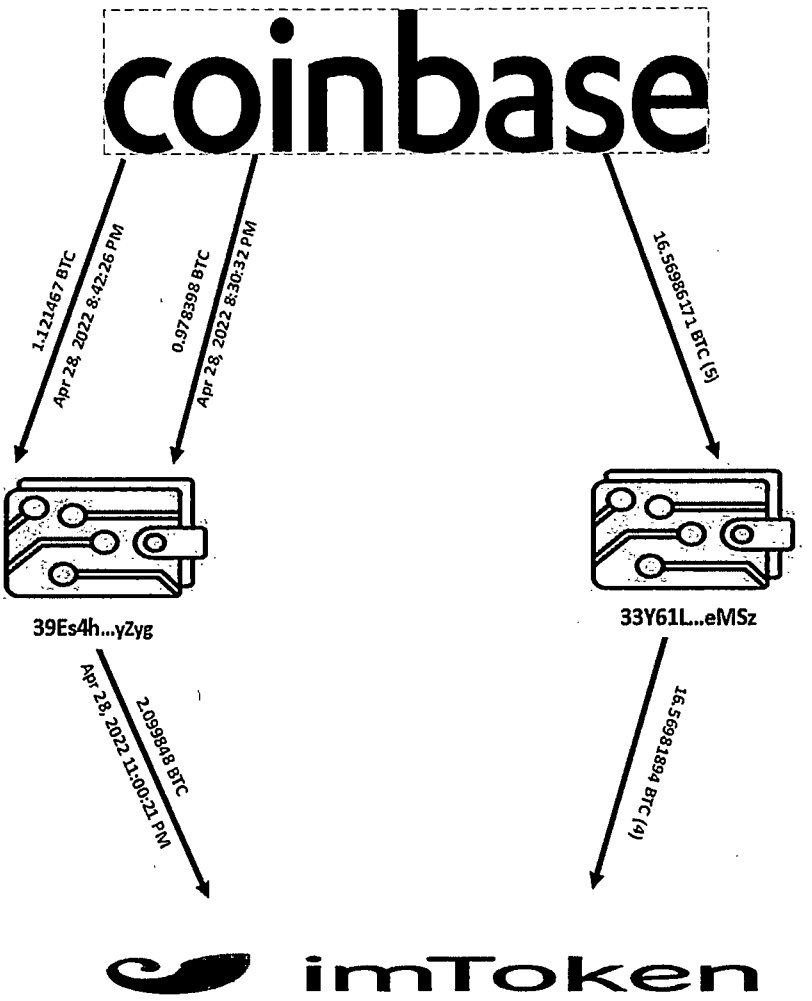
h. The victims' funds were then transferred to two wallet addresses, 0x5E90...7aFD and 0x29F9...0Cb9 before being consolidated again to deposit address 0xc4a3…0a16 for the Target Binance Account:

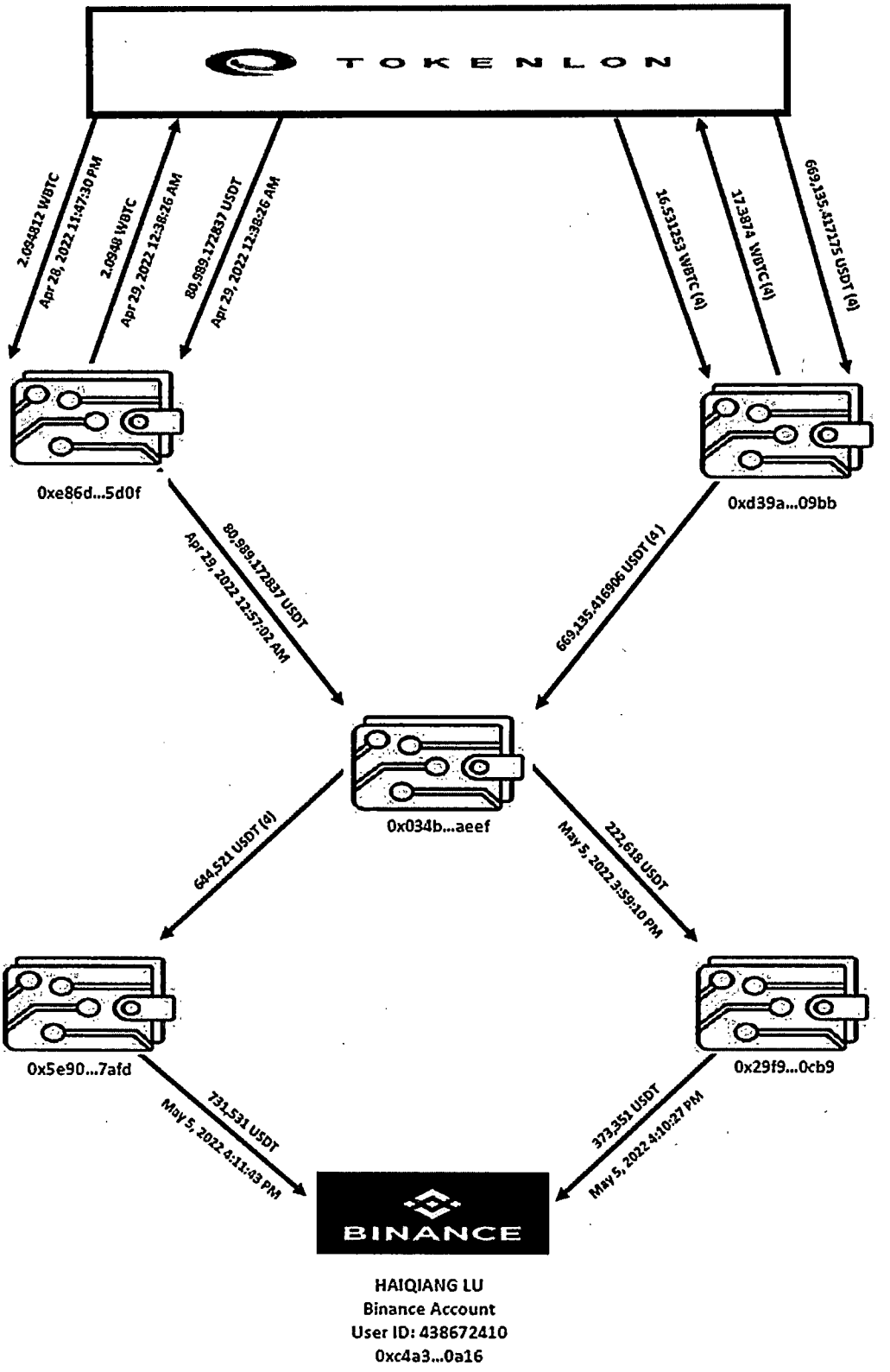
Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x5a56f2116032b70232e49b081cf7f0db5f4692c1d36a12b0d94527ef845a4c7a	04/28/2022 5:47:20 AM	179,034.00	0x5E90...7aFD	J.P.
0xa364712e585ac15b7d4e24b6a8f07239bbc08c94f729490ca1079c30acd55920	04/29/2022 6:15:21 AM	100,744.00	0x5E90...7aFD	D.M. & B.F.
0x94ff59c15575dc79ca9895b86390c0a6436f6d294fd445eaa9b13c842b9c6bf6	05/03/2022 5:18:16 AM	76,833.00	0x5E90...7aFD	J.P. & D.C
0xc048670f3c55ca4f99d7ee703a9474143339cb5e0e133779757dedfbdc2a654f	05/04/2022 6:03:08 AM	287,910.00	0x5E90...7aFD	J.P.
0x0ed43050f0144d1745cff47341457287baa2183ad42dd754e61cc8030d81fa90	05/05/2022 4:11:43 PM	(731,531.00)	0xc4A3...0A16	

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x14957ee0676924e7359eac10d349f98c842fcc86087f29f3a1fc45808a1b5fda	05/05/2022 3:59:10 PM	222,618.00	0x29F9...0Cb9	J.P.
0x582588774dee5bcf22b431c30e11c5edec33a707ae313ffa9fa674eb699375ca	05/05/2022 4:10:27 PM	(373,351.00)	0xc4A3...0A16	

i. The total amount of victims' funds from J.P., D.C., D.M., and B.F. into deposit address 0xc4a3…0a16 for the Target Binance Account was 1,104,882 USDT, or approximately $1.1 million U.S. dollars.

32. Figures showing the entire flow of the portion of all 4 of these victims' stolen funds (J.P., D.C., D.M., and B.F.) into deposit address 0xc4a3…0a16 for the Target Binance Account is below:


coinbase
1.121467 BTC
Apr 28, 2022 8:42:26 PM
0.978398 BTC
Apr 28, 2022 8:30:32 PM
16.56986171 BTC (5)
39Es4h...yZyg
33Y61L...eMSz
Apr 28, 2022 11:00:21 PM
2.099848 BTC
16.56981894 BTC (4)
imToken


TOKENLON
2.694812 WBTC
Apr 28, 2022 11:47:30 PM
2.6948 WBTC
Apr 29, 2022 12:38:26 AM
80,989.172837 USDT
Apr 29, 2022 12:38:26 AM
16.531253 WBTC (4)
17.3874 WBTC (4)
669,135.417175 USDT (4)
0xe86d...5d0f
0xd39a...09bb
80,989.172837 USDT
Apr 29, 2022 12:57:02 AM
669,135.416906 USDT (4)
0x034b...aeef
644.521 USDT (4)
222.618 USDT
May 5, 2022 3:59:10 PM
0x5e90...7afd
0x29f9...0cb9
731.531 USDT
May 5, 2022 4:11:43 PM
373.351 USDT
May 5, 2022 4:10:27 PM
BINANCE
HAIQIANG LU
Binance Account
User ID: 438672410
0xc4a3...0a16

7 Victims' Stolen Funds Transferred to Target Binance Account Wallet Address TPbxGy...d4CL

33. On August 17, 2022, the FBI TRA interviewed via telephone M.J. as she currently resides in University City, Missouri. In April of 2022, M.J. was approached by a male using the name of "Allen Chen" (SUSPECT #7), about his interest in renting a condo she had listed. They started to communicate using the communication application called Line. SUSPECT #7 represented himself as a family man who worked for Citibank in New York as a financial trader/analyst. SUSPECT #7 told M.J. he traded cryptocurrency and wanted to get her involved as he was very successful at it and wanted to help M.J. for helping him with the condo. SUSPECT #7 instructed M.J. on what applications to download such as BiKing and Coinbase, how to download them, and how to work them and makes trades using them. M.J. was directed to https://www.BiKing.com and told to create an account to make her trades. M.J. was also instructed to transfer her savings to Coinbase and eventually into the wallets provided to her by SUSPECT #7. M.J. was new to trading cryptocurrency and had to rely on SUSPECT #7's help and direction. After a few trades, M.J. started to make profits. SUSPECT #7 told M.J. the more money in her account the better the return. After seeing these profits and at the urging of SUSPECT #7, M.J. started to invest more of her savings into the scam and even got her family to invest as well. M.J. borrowed money from her family to invest more into the scam. In approximately 80 days, M.J. invested and lost what she claims to be approximately $965,000 of money she had in her savings to include her stocks and bonds, IRA accounts, and money she borrowed from family. When M.J. tried to withdraw her funds from the website,

she was told she needed to pay a 20% tax. The investigation was able to document the following deposits:

Date Wire Sent to Exchange	Dollar Amount of Wire Sent to Exchange	Name of Bank/Institution Wire Originated	Name of Exchange Wire Deposited Into
May 4, 2022	$ 28,000.00	US Bank	Coinbase
May 6, 2022	$320,000.00	Royal Banks of Missouri	Coinbase
May 13, 2022	$147,500.00	Royal Banks of Missouri	Coinbase
May 13, 2022	$ 20,000.00	US Bank	Coinbase
May 16, 2022	$ 50,000.00	Royal Banks of Missouri	Coinbase

34. On October 04, 2022, the FBI TRA interviewed via telephone A.A. as he currently resides in Milpitas, California. A.A. had been contacted using the communication application called Line. A.A. was contacted by a young wealthy Chinese female who went by the name of "Lisa" (SUSPECT #8). SUSPECT #8 told A.A. her family was in the exporting and trading business and that she could help him with cryptocurrency trading so he could also be wealthy. SUSPECT #8 instructed A.A. to visit the website https://www.cbotcen.com and start investing. SUSPECT #8 directed A.A. on how to set up an account with cbotcen.com and with Coinbase. At first, A.A. invested and transferred $7,000 to Coinbase and eventually into wallet addresses given to him by SUSPECT #8. After making a quick profit, and after SUSPECT #8 told A.A. the profits would be much higher if he invested $200,000, A.A. sold his stock and bonds and invested $200,000. After the transfer, A.A. saw higher gains from his investments. With the pressure from SUSPECT #8, A.A. sold more of his stocks and bonds and invested another $250,000. A.A. was able to make a small withdraw of $500 from his

cbotcen.com account. After the withdrawal, A.A. sold his remaining stocks and bonds and invested another $70,000. After making more profits from his trades, A.A. attempted to withdraw $750,000 from his account but was unable due to the website stating he needed to complete advanced verification. A.A. uploaded a copy of his driver's license to the website. After weeks of verifying, A.A. was told his account credit score was down from 100 to 80 and it needed to be brought up for him to make any withdrawals. A.A. was advised he needed to pay $10,000 per point to bring his score back up to 100, which would cost him another $200,000. SUSPECT #8 told A.A. to quit his job so he could collect his 401k to pay the fee. A.A. invested and lost approximately $520,000 of his savings.

35. On September 15, 2022, the FBI Los Angeles Division interviewed F.J. via phone as she currently resides in Arcadia, California. F.J. first met "Ken Tang" (SUSPECT #9), on February 27, 2022, on the WeChat application, asking for a piano teacher in the Los Angeles area and presenting himself working in the metaverse and cryptocurrency. SUSPECT #9 introduced F.J. to cryptocurrency trading and directed her to BXMEX and Toptank and promised her investments in the crypto market with guaranteed 20-30% returns. SUSPECT #9 instructed F.J. step-by-step on how to download and use these applications. The Toptank and BXMEX applications were not found on the Apple application store. SUSPECT #9 sent her a link via WeChat to open and download the apps directly to her phone. F.J. also downloaded Coinbase and Crypto as per SUSPECT #9's instructions. SUSPECT #9 also told F.J. how and when to make her trades once the software and applications were installed. The website F.J. was directed to make her trades was https://www.toptankep.com. F.J. attempted to withdraw her funds from toptankep.com and was told she needed to pay fees and taxes on those funds

and when SUSPECT #9 was confronted, he cut off all communication with F.J. and she never heard back from him or from toptankep.com's customer service. F.J. was given the wallet address to transfer her cryptocurrency into and she made several deposits that equaled approximately $405,200, which she eventually lost in the scam.

36. Through blockchain tracing and obtaining records from Coinbase, the FBI has identified four more victims who have submitted complaints and filed reports through the FBI's Internet Crime Complaint Center (IC3). The FBI TRA has reviewed those IC3 reports filed by the following four victims and believe all their cases are similar to those victims that have already been interviewed.

37. On May 7, 2022, J.H., 63 years old, from Sterling Heights, Michigan submitted a report to IC3 stating she lost $156,000 in an online investment scam. J.H. was approached via LinkedIn, WeCchat, and WhatsApp by a Chinese male who went by the name of "Andy Wang" (SUSPECT #10). SUSPECT #10 introduced her to cryptocurrency trading and directed her to the websites https://www.toptank.com and sinsab.com/5#/ to make her trades. J.H. invested a small amount of $5,000 to start and was instructed by SUSPECT #10 to download Coinbase and he showed her how to transfer her savings into Coinbase and eventually into cryptocurrency wallets given to her by SUSPECT #10. SUSPECT #10 showed her how to transfer her funds back to her Coinbase account after making profits. After J.H. was able to transfer money back into her Coinbase, she started to trade even more money. After investing $156,000 of her savings, J.H. tried to withdraw her funds and transfer her money and profits back to her Coinbase account but was told she needed to pass advanced verification which

would require, one to thirty days of verification and then told her she needed to deposit another 30% into her account before any funds could be transferred.

38. On July 25, 2022, R.N., who is an elderly victim of 73 years old, from Littleton, Colorado submitted a report to IC3 and stating he lost approximately $2,000,000 of his savings in an online investment scam. R.N. reported he was approached by a friend of his girlfriend named "Anton Chen" (SUSPECT #11) about trading cryptocurrency. SUSPECT #11 stated he was part of a group that analyzes the blockchain and other macro-economic trends for cryptocurrency trading and the odds of gain were 90%. In April of 2022, SUSPECT #11 directed R.N. to the website https://www.Simexcen.com and coached him on how and when to make trades using this website. After R.N. made profits from his trades, he tried to withdraw his funds and, he was told he could only withdraw contents from his last trade and if the profit was greater than $500,000, he had to pay a 10% fee and taxes. R.N. was told he had to pay an additional $528,000 in taxes before he could make any withdrawals.

39. On June 30, 2022, R.T. from Tempe, Arizona submitted a report to IC3 stating he lost approximately $430,000 of his savings to an online investment scam. R.T. thought he was transferring his funds to a legitimate cryptocurrency trading platform and website called https://www.apexcryptobiz.com. When R.T. attempted to withdraw his funds and profits the website told him he owed a tax on his profits and was unable to withdraw any of his money.

40. On August 5, 2022, G.W. from Hayward, California submitted a report to IC3 stating he lost approximately $315,155.61 in an online investment scam. G.W. was approached by someone named "Tan" (SUSPECT #12) on Skype who helped him set up an account with Antrush Group and helped him trade Bitcoin cryptocurrency. Since April of 2022, G.W.

invested approximately $315,000 from his savings to wallets controlled by Antrush Group. When G.W. attempted to withdraw his funds and profits he was unable to login and was unable to withdraw any of his funds. The website he was directed to was https://www.antrush.com and https://www.antrushfx.com.

41. Only a portion of M.J.'s, A.A.'s, F.J.'s, J.H.'s, R.N.'s, R.T.'s, and G.W.'s stolen funds were able to be traced into deposit address TPbxGy...d4CL for the Target Binance Account according to blockchain analysis as shown below.

a. R.N. had funds in USDC that were transferred to 0x569b...e244:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0xd6f47d2f379a1f80ad234ca807ab16f49106299c7093b27fc520a5fdb679b76c	05/04/2022 11:06:49 PM	119,000	0x569b...e244	R.N.
0x068276aa1daf908cffdd8ae5c9928023c8c9e481829654e8c0a3bfec7e281bdc	05/04/2022 11:23:51 PM	(119,000)	0x308f...859c	

b. The next hop with R.N.'s funds in USDC was:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x068276aa1daf908cffdd8ae5c9928023c8c9e481829654e8c0a3bfec7e281bdc	05/04/2022 11:23:51 PM	119,000	0x308f...859c	R.N.
0x43a28baf143ce47ad8693a91902f163a23c3292caa838d62212e5f0e7b095535	05/04/2022 11:28:51 PM	(150,780)	0x4a14...650d	

c. R.N.'s funds in USDC were then swapped for USDT by using Tokenlon in wallet address 0x308f...859c as shown below:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x43a28baf143ce47ad8693a91902f163a23c3292caa838d62212e5f0e7b095535	05/04/2022 11:28:51 PM	150,669.470937	0x308f...859c	R.N.
0x24b7efa5f36d548d37cfb7c3e93eab354cb5b480e29a608278d513f2f501a926	05/04/2022 11:50:25 PM	(150,669.46)	0xc0b1...1b2b	

d. M.J. had funds in USDC that were transferred to 0xf05b...44a7:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x886858df01a19ba5dad0d0fb012ccfba9bc567f0541502584ae98dafd38dc974	05/05/2022 3:23:34 AM	27,971.457514	0xf05b...44a7	M.J.
0x6ea56909e72fb4c6ba807de68ebaeecbccеb8f282cf30135301b21308cddd661	05/05/2022 4:52:39 AM	(27,971.457514)	0x0671...cc70	

e. The next hop with M.J.'s funds in USDC was:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x6ea56909e72fb4c6ba807de68ebaeecbccеb8f282cf30135301b21308cddd661	05/05/2022 4:52:39 AM	27,971.457514	0x0671...cc70	M.J.
0x6c8202582561b3b770f8f4bf962ad4dc60373f388c71cce5ec05fc6a9bd2b92b	05/05/2022 4:57:08 AM	(27,971.4575)	0xfD6C...B54F	

f. M.J.'s funds in USDC were then swapped for USDT by using Tokenlon in wallet address 0x0671...cc70 as shown below:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x6c8202582561b3b770f8f4bf962ad4dc60373f388c71cce5ec05fc6a9bd2b92b	05/05/2022 4:57:08 AM	27,931.831742	0x0671...cc70	M.J.
0x539d41aa35069c0d395bd9275854b4261e7cda4f65a8c4c33a9e4f9a3600001d	05/05/2022 5:03:11 AM	(27,931.831742)	0xc0b1...1b2b	

g. G.W. had funds in ETH that were transferred to 0x53c8...441c:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x71b95c7d5bdab3754f1ad16022b203bce86ee44265b1cced39943ece3d25bc4b	05/04/2022 8:40:01 PM	34.96260661	0x53c8...441c	G.W.
0x8b3639be63f11bf553854e4860faf246d8994c34de3a3ac078897ea12f2a921e	05/04/2022 9:50:12 PM	(34.96187496)	0x7535...fe97	

h. The next hop with G.W.'s funds in ETH was:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x8b3639be63f11bf553854e4860faf246d8994c34de3a3ac078897ea12f2a921e	05/04/2022 9:50:12 PM	34.96187496	0x7535...fe97	G.W.
0x14ccc93f9e8db39f2abb1cec973e9f3fdbf8ff54844fead645bb640f1cfd1a25	05/04/2022 10:22:16 PM	(35.9)	0x03f3...9659	

i. G.W.'s funds in ETH were then swapped for USDT by using Tokenlon in wallet address 0x7535...fe97 as shown below:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x14ccc93f9e8db39f2abb1cec973e9f3fdbf8ff54844fead645bb640f1cfd1a25	05/04/2022 10:22:16 PM	104,872.772201	0x7535...fe97	G.W.
0x0a9ed9fadd4b58e93d510be5671459ae21f740198ccd71c5ab123d744ac0ed47	05/05/2022 3:13:48 PM	(104,872.772201)	0xc0b1...1b2b	

j. R.T. had funds in ETH that were transferred to 0xc9d6...1e6b:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0xf9b1a1bbae77b026b8c409c54cb4d5e72e7e5aa5c2f7883968854aa9255265a5	05/05/2022 5:18:52 AM	18.9301738	0xc9d6...1e6b	R.T.
0xb715be657dda091e93a2b3065fef695fd408a0105320da8d8a8ef6776ce79eb8	05/05/2022 5:30:50 AM	(18.9285819)	0xC9aE...FC5F	

k. The next hop with R.T.'s funds in ETH was:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0xb715be657dda091e93a2b3065fef695fd408a0105320da8d8a8ef6776ce79eb8	05/05/2022 5:30:50 AM	18.9285819	0xC9aE...FC5F	R.T.
0x0b523bfb2ce32f3d2787007306637871588 4ef2f0ababcf6e5705ce4696b5440	05/05/2022 5:41:53 AM	(18.88)	0x03f3...9659	

l. R.T.'s funds in ETH were then swapped for USDT by using Tokenlon in wallet address 0xC9aE...FC5F as shown below:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x0b523bfb2ce32f3d2787007306637871588 4ef2f0ababcf6e5705ce4696b5440	05/05/2022 5:41:53 AM	55,213.804778	0xC9aE...FC5F	R.T.
0x4f28600fbfbf58b2e28fcf4441a9f3b25736f602bf556c0f8a9b6ab760c424be	05/05/2022 8:11:35 AM	(55,213.804778)	0xc0b1...1b2b	

m. J.H. had funds in USDC that were transferred to 0x4a79...d3d4:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x654e32692ba359ab5aba7bbd357c626a86410a4b3edf0ea5796a0854a7728376	05/04/2022 4:59:02 PM	100,000	0x4a79...d3d4	J.H.
0x3733a80d495e203d67465e759ee7ef58aa56e6249b51f3ffd0d5a7050f847cab	05/04/2022 6:06:24 PM	(100,000.005661)	0xb0e3...e55a	

n. F.J. had funds in USDC that were transferred to 0xb5a8...d623:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x0b53325082637e93df40077cc9f9692ba7465b207b3f6278161f8e558a0670d5	05/05/2022 2:43:27 AM	50,981.086298	0xb5a8...d623	F.J.
0x575c6f20e1e74c2b0b330f05417799d48d1d5ea869de016a7d404556765d3d4a	05/05/2022 3:02:26 AM	(50,981.086298)	0xb0e3...e55a	

o. J.H.'s and F.J.'s funds in USDC were consolidated in wallet address 0xb0e3…e55a:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x3733a80d495e203d67465e759ee7ef58aa56e6249b51f3ffd0d5a7050f847cab	05/04/2022 6:06:24 PM	100,000.005661	0xb0e3...e55a	J.H.
0x1351f77ec77d23e064cc77fcabca36f76814409d2ee86807d3d060f0d2f96bcd	05/04/2022 6:24:14 PM	(100,000.0056)	0x4a14...650d	
0x575c6f20e1e74c2b0b330f05417799d48d1d5ea869de016a7d404556765d3d4a	05/05/2022 3:02:26 AM	50,981.086298	0xb0e3...e55a	F.J.
0x17700991145a840737b54a354032bea911986abfdaab94208a0399f081332cc5	05/05/2022 3:13:00 AM	(50,981.0863)	0x4a14...650d	

p. J.H.'s and F.J.'s funds in USDC were then swapped for USDT by using Tokenlon in wallet address 0xb0e3…e55a as shown below:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x1351f77ec77d23e064cc77fcabca36f76814409d2ee86807d3d060f0d2f96bcd	05/04/2022 6:24:14 PM	99,916.590485	0xb0e3...e55a	J.H.
0x60ed3e1f74d7238087595d999664315ec3f6d586e299b6dab4756a75595b3684	05/04/2022 6:52:17 PM	(149,044.552439)	0xc0b1...1b2b	
0x17700991145a840737b54a354032bea911986abfdaab94208a0399f081332cc5	05/05/2022 3:13:00 AM	50,826.497673	0xb0e3...e55a	F.J.
0xec1d4fe1eda97a0f63e3dcc25b23a2af23dd824d6247b885ca6bdbfc5389fecb	05/05/2022 3:20:52 AM	(50,826.497673)	0xc0b1...1b2b	

q. A.A. had funds in USDC that were transferred to 0x1c31...008f:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x520abd052e9e9a405ca2cf400fc80b96634430fc1e152c1f525536fce1561de7	05/04/2022 3:47:20 PM	70,000	0x1c31...008f	A.A
0x369f9271e4cd594660cc65da040fad2ec8a2a2a3e2a1f654652f2a85fd267cb2	05/04/2022 4:04:01 PM	(70,000)	0x63Fa...d221	

r. The next hop with A.A.'s funds in USDC was:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0x369f9271e4cd594660cc65da040fad2ec8a2a2a3e2a1f654652f2a85fd267cb2	05/04/2022 4:04:01 PM	70,000	0x63Fa...d221	A.A
0xaf48e557e3b7a81c4394902d381f3aac37b0651dd86449ecf31141babe3a7b35	05/04/2022 4:06:51 PM	(70,000)	0x4a14...650d	

s. A.A.'s funds in USDC were then swapped for USDT by using Tokenlon in wallet address 0x63Fa...d221 as shown below:

Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0xaf48e557e3b7a81c4394902d381f3aac37b0651dd86449ecf31141babe3a7b35	05/04/2022 4:06:51 PM	69,857.36769	0x63Fa...d221	A.A
0xaec72c8423083548b45834a710676ab378c6cb46bb6fc04d90ff91fc1767937f	05/04/2022 4:14:51 PM	(69,857.36769)	0xc0b1...1b2b	

t. Wallet address 0xc0b1...1b2b is the intermediary wallet address where the funds for all 7 victims above were consolidated and then were transferred to the two Malaysian Intermediary Accounts:

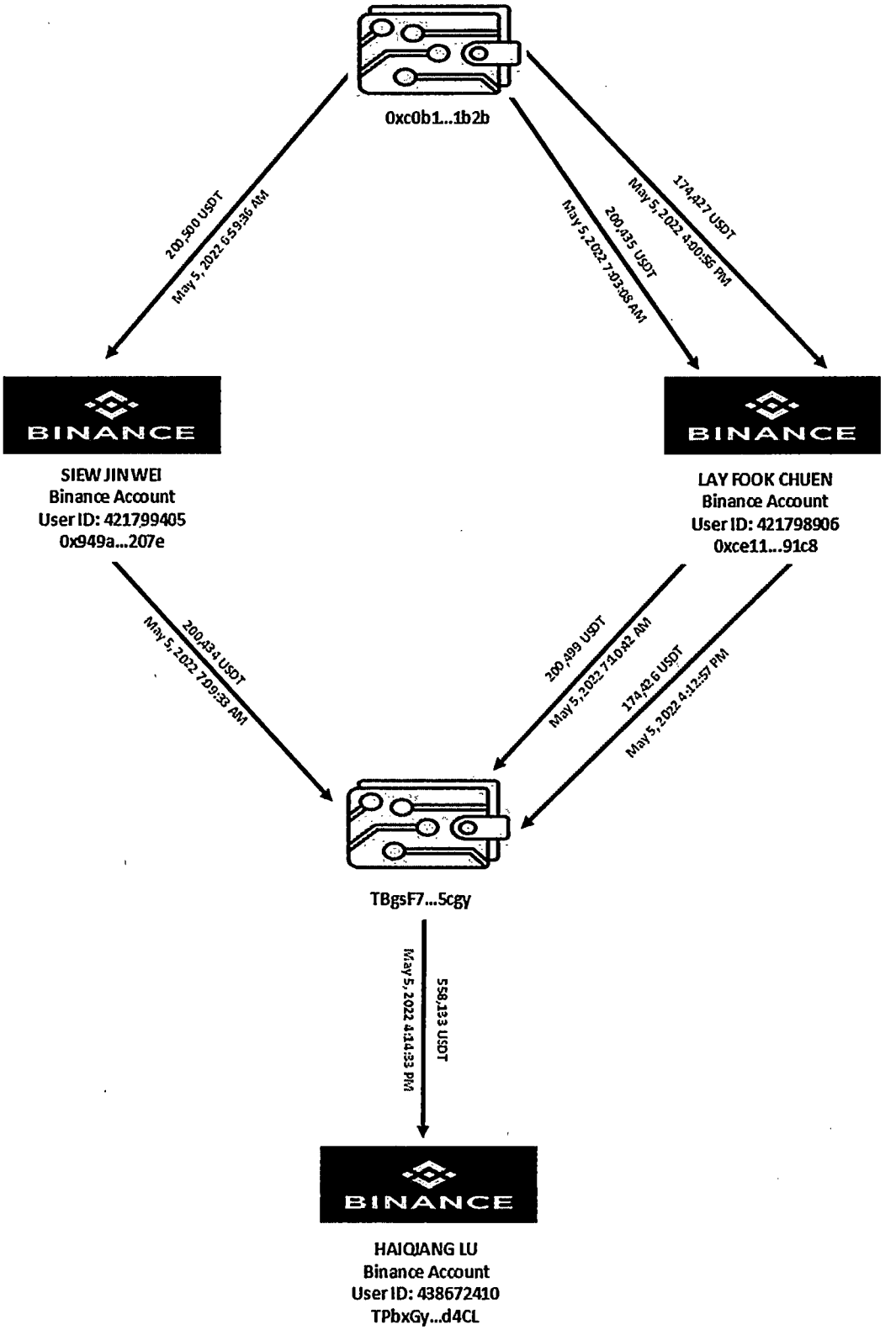
Transaction Hash	Timestamp	Amount	Wallet Address	Victim
0xaec72c8423083548b45834a710676ab378c6cb46bb6fc04d90ff91fc1767937f	05/04/2022 4:14:51 PM	69,857.36769	0xc0b1...1b2b	A.A
0x60ed3e1f74d7238087595d999664315ec3f6d586e299b6dab4756a75595b3684	05/04/2022 6:52:17 PM	149,044.552439	0xc0b1...1b2b	J.H.
0x24b7efa5f36d548d37cfb7c3e93eab354cb5b480e29a608278d513f2f501a926	05/04/2022 11:50:25 PM	150,669.46	0xc0b1...1b2b	R.N.
0xec1d4fe1eda97a0f63e3dcc25b23a2af23dd824d6247b885ca6bdbfc5389fecb	05/05/2022 3:20:52 AM	50,826.497673	0xc0b1...1b2b	F.J.
0x539d41aa35069c0d395bd9275854b4261e7cda4f65a8c4c33a9e4f9a3600001d	05/05/2022 5:03:11 AM	27,931.831742	0xc0b1...1b2b	M.J.
0x2f80da40d49cbc79a45cf0d9258cc29c5da7480b7531a4f27d1ebe01db851d46	05/05/2022 6:59:36 AM	(200,500)	0x949A...207e	
0xf733592627ed67aa2854d2d04994c1f1ebe32f3ae55395fbea9c4eeeeb8bd0a4	05/05/2022 7:03:08 AM	(200,435)	0xCE11...91C8	
0x4f28600fbfbf58b2e28fcf4441a9f3b25736f602bf556c0f8a9b6ab760c424be	05/05/2022 8:11:35 AM	55,213.804778	0xc0b1...1b2b	R.T.
0x0a9ed9fadd4b58e93d510be5671459ae21f740198ccd71c5ab123d744ac0ed47	05/05/2022 3:13:48 PM	104,872.772201	0xc0b1...1b2b	G.W.
0x30563c41ad29f7438e276f64d01428630c1577d2d2256ff5c49b985479670194	05/05/2022 4:00:56 PM	(174,427)	0xCE11...91C8	

42. As shown previously, the Withdrawal History report for the two Malaysian Intermediary Accounts revealed that both Binance accounts withdrew funds to an external

address TBgsF7...5cgy. The funds in TBgsF7...5cgy were then transferred to deposit address TPbxGy...d4CL for the Target Binance Account. The total amount of victims' funds from M.J., A.A., F.J., J.H., R.N., R.T., and G.W. into deposit address TPbxGy...d4CL for the Target Binance Account was 558,133 USDT, or approximately $558,000 in U.S. dollars.

43. Figures showing the entire flow of the portion of all 7 of these victims' stolen funds (M.J., A.A., F.J., J.H., R.N., R.T., and G.W.) into deposit address TPbxGy...d4CL for the Target Binance Account is below:

coinbase
0x569b...e244
0x308f...859c
119,000 USDC
May 4, 2022 11:23:51 PM
0xf05b...44a7
0x0671...cc70
27,971.457514 USDC
May 5, 2022 4:52:39 AM
0x53c8...441c
0x7535...fe97
34.961875 ETH
May 4, 2022 9:50:12 PM
0xc9d6...1e6b
0xc9ae...fc5f
18.928582 ETH
May 5, 2022 5:30:50 AM
0x4a79...d3d4
0xb0e3...e55a
0xb5a8...d623
0x1c31...008f
0x63fa...d221
0xc0b1...1b2b
119,000 USDC
May 4, 2022 11:36:49 PM
27,971.457514 USDC
May 5, 2022 3:23:34 AM
34.962607 ETH
May 4, 2022 8:40:01 PM
18.930174 ETH
May 5, 2022 5:18:52 AM
100,000 USDC
May 4, 2022 4:59:02 PM
100,000.005661 USDC
May 4, 2022 6:06:24 PM
50,981.086298 USDC
May 5, 2022 2:43:27 AM
50,981.086298 USDC
May 5, 2022 3:02:26 AM
70,000 USDC
May 4, 2022 3:47:20 PM
70,000 USDC
May 4, 2022 3:47:20 PM
199,871.050112 USDT (3)
69,557.367769 USDT
May 4, 2022 11:51:51 PM
350,969.46 USDT
May 4, 2022 11:50:25 PM
27,971.457514 USDT
May 5, 2022 5:03:11 AM
10,827.277201 USDT
May 5, 2022 3:13:48 PM
52,243.804778 USDT
May 5, 2022 8:11:35 AM


0xc0b1...1b2b
200,500 USDT
May 5, 2022 6:59:36 AM
200,435 USDT
May 5, 2022 7:03:08 AM
174,427 USDT
May 5, 2022 4:00:56 PM
BINANCE
SIEW JIN WEI
Binance Account
User ID: 421799405
0x949a...207e
BINANCE
LAY FOOK CHUEN
Binance Account
User ID: 421798906
0xce11...91c8
200,434 USDT
May 5, 2022 7:09:33 AM
200,499 USDT
May 5, 2022 7:10:42 AM
174,426 USDT
May 5, 2022 4:12:57 PM
TBgsF7...5cgy
558,133 USDT
May 5, 2022 4:14:33 PM
BINANCE
HAIQIANG LU
Binance Account
User ID: 438672410
TPbxGy...d4CL

CONTACT FROM PURPORTED OWNER OF TARGET BINANCE ACCOUNT

44. On October 21, 2022, I received an email from HAIQIANG LU at 999lhq@gmail.com that read, "FBI agent Nathan Wood, hello, my case number is 2022R05663. Please check for me when it can be solved." According to records from Binance, HAIQIANG LU is the owner of the Target Binance Account. I had previously provided the case number to Binance as part of the process of temporarily freezing the Target Binance Account.

45. On October 25, 2022, I received the identical email from the same email address.

46. As of the date of this affidavit, I have not responded to either email.

CONCLUSION

47. Based on the foregoing, I believe there is probable cause to believe the cryptocurrencies seized from the following Target Binance Account were involved transactions or attempted transactions in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) (Money Laundering) and 1956(h) (Conspiracy to Commit Money Laundering), and constitute or were derived from proceeds traceable to violations of 18 U.S.C. §§ 1343 (Wire Fraud), 1349 (Conspiracy to Commit Wire Fraud), 1956(a)(1)(B)(i) (Money Laundering), and 1956(h) (Conspiracy to Commit Money Laundering), and are therefore subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (a)(1)(C).

Seized from Binance User ID 438672410:

Currency Name	Currency Code	Balance
USDT	TetherUS	1,150,049.51316
ETC	Ethereum Classic	59,939.992

I swear, under penalty of perjury, that the foregoing is true and correct.

Nathan Wood
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 27th day of March, 2023.

KASSANDRA JUAREZ
Notary Public - State of Arizona
PIMA COUNTY
Commission # 576932
Expires December 31, 2023

Notary Public