PATRICK D. ROBBINS (CABN 152288)
Attorney for the United States
Acting Under Authority Conferred by 28 U.S.C. § 515

MARTHA BOERSCH (CABN 126569)
Chief, Criminal Division

DONOVAN MIGUEL MCKENDRICK (CABN 284339)
Special Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7164
FAX: (415) 436-7234
Donovan.McKendrick@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. APPROXIMATELY $23,604,815.09 IN ASSORTED CRYPTOCURRENCIES Defendant.	NO. COMPLAINT FOR FORFEITURE

NATURE OF THE ACTION

1. This is a judicial forfeiture action, as authorized by 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C), 981(b), and 21 U.S.C. § 881(a)(6), involving the seizure of the following property - assorted cryptocurrencies with a total estimated value of approximately $23,604,815.09 U.S. Dollars (USD) [1]:

a. 0.1 BTC seized from OKX by law enforcement on June 7, 2024, with an approximate U.S. dollar value of $9,638.01;

[1] Estimated on February 13, 2025, using online resources.

b. 100 USDT seized from OKX by law enforcement on June 7, 2024, with an approximate U.S. dollar value of $100.00;

c. 51.67768 BTC seized from OKX by law enforcement on June 10, 2024, with an approximate U.S. dollar value of $4,980,701.51;

d. 20,437.74 USDT seized from OKX by law enforcement on June 10, 2024, with an approximate U.S. dollar value of $20,437.74;

e. 0.0002 BTC seized from Payward Interactive, Inc. (dba Kraken) by law enforcement on June 13, 2024, with an approximate U.S. dollar value of $19.27;

f. 24.8 XRP seized from Payward Interactive, Inc. (dba Kraken) by law enforcement on June 13, 2024, with an approximate U.S. dollar value of $61.85;

g. 11.12935511 BTC seized from Payward Interactive, Inc. (dba Kraken) by law enforcement on June 14, 2024, with an approximate U.S. dollar value of $1,072,648.69;

h. 528,490.8 XRP seized from Payward Interactive, Inc. (dba Kraken) by law enforcement on June 14, 2024, with an approximate U.S. dollar value of $1,318,056.05;

i. 100 XRP seized from WhiteBIT by law enforcement on August 9, 2024, with an approximate U.S. dollar value of $249.40;

j. 3,665,398.43 XRP seized from WhiteBIT by law enforcement on August 14, 2024, with an approximate U.S. dollar value of $9,141,503.68;

k. 20 USDT seized from AscendEX Technology SRL by law enforcement on December 26, 2024, with an approximate U.S. dollar value of $20.00;

l. 355,903.72 USDT seized from AscendEX Technology SRL by law enforcement on January 14, 2025, with an approximate U.S. dollar value of $355,903.72;

m. 2 XRP seized from Ftrader Ltd (dba FixedFloat) by law enforcement on January 9, 2025, with an approximate U.S. dollar value of $4.98;

n. 193,000 XRP seized from Ftrader Ltd (dba FixedFloat) by law enforcement on January 11, 2025, with an approximate U.S. dollar value of $481,342.00;

o. 193,998 XRP seized from Ftrader Ltd (dba FixedFloat) by law enforcement on January 11, 2025, with an approximate U.S. dollar value of $483,831.01;

p. 0.999982 XRP seized from SwapSpace LLC by law enforcement on January 30, 2025, with an approximate U.S. dollar value of $2.49;

q. 2,265,186.615965 XRP seized from SwapSpace LLC by law enforcement on January 31, 2025, with an approximate U.S. dollar value of $5,649,375.42;

r. 0.0001 BTC seized from Rabbit Finance LLC (dba CoinRabbit) by law enforcement on February 5, 2025, with an approximate U.S. dollar value of $9.64; and

s. 0.94324 BTC seized from Rabbit Finance LLC (dba CoinRabbit) by law enforcement on February 6, 2025, with an approximate U.S. dollar value of $90,909.59;

(hereinafter, collectively, the "Defendant Property"), as property constituting, or derived from, any proceeds of 18 U.S.C. §§ 2314 (Transportation of Stolen Goods), and 1030(a)(2)(C) (Computer hacking), and/or as an instrumentality of 18 U.S.C. § 1956(c)(7) (Money Laundering) and thereby forfeitable pursuant to 18 U.S.C. §§ 981(a)(l)(C) and 28 U.S.C. § 2461(c).

JURISDICTION AND VENUE

2. This Court has jurisdiction under 28 U.S.C. §§ 1345 and 1355(a), and 18 U.S.C. §§ 981(a)(l)(C). Venue is proper because the defendant currency was seized in the Northern District of California, per 28 U.S.C. §§ 1355(b) and 1395. Further, the victim, and criminal acts, were committed within the Northern District of California.

3. Intra-district venue is proper in the San Francisco Division within the Northern District of California.

PARTIES

4. The Plaintiff is the United States of America.

5. The Defendant Property is assorted cryptocurrencies with a total estimated value of approximately $23,604,815.09 U.S. Dollars ("USD"), as follows:

a. 0.1 BTC seized from OKX by law enforcement on June 7, 2024, with an approximate U.S. dollar value of $9,638.01;

b. 100 USDT seized from OKX by law enforcement on June 7, 2024, with an approximate U.S. dollar value of $100.00;

c. 51.67768 BTC seized from OKX by law enforcement on June 10, 2024, with an approximate

U.S. dollar value of $4,980,701.51;

d. 20,437.74 USDT seized from OKX by law enforcement on June 10, 2024, with an approximate U.S. dollar value of $20,437.74;

e. 0.0002 BTC seized from Payward Interactive, Inc. (dba Kraken) by law enforcement on June 13, 2024, with an approximate U.S. dollar value of $19.27;

f. 24.8 XRP seized from Payward Interactive, Inc. (dba Kraken) by law enforcement on June 13, 2024, with an approximate U.S. dollar value of $61.85;

g. 11.12935511 BTC seized from Payward Interactive, Inc. (dba Kraken) by law enforcement on June 14, 2024, with an approximate U.S. dollar value of $1,072,648.69;

h. 528,490.8 XRP seized from Payward Interactive, Inc. (dba Kraken) by law enforcement on June 14, 2024, with an approximate U.S. dollar value of $1,318,056.05;

i. 100 XRP seized from WhiteBIT by law enforcement on August 9, 2024, with an approximate U.S. dollar value of $249.40;

j. 3,665,398.43 XRP seized from WhiteBIT by law enforcement on August 14, 2024, with an approximate U.S. dollar value of $9,141,503.68;

k. 20 USDT seized from AscendEX Technology SRL by law enforcement on December 26, 2024, with an approximate U.S. dollar value of $20.00;

l. 355,903.72 USDT seized from AscendEX Technology SRL by law enforcement on January 14, 2025, with an approximate U.S. dollar value of $355,903.72;

m. 2 XRP seized from Ftrader Ltd (dba FixedFloat) by law enforcement on January 9, 2025, with an approximate U.S. dollar value of $4.98;

n. 193,000 XRP seized from Ftrader Ltd (dba FixedFloat) by law enforcement on January 11, 2025, with an approximate U.S. dollar value of $481,342.00;

o. 193,998 XRP seized from Ftrader Ltd (dba FixedFloat) by law enforcement on January 11, 2025, with an approximate U.S. dollar value of $483,831.01;

p. 0.999982 XRP seized from SwapSpace LLC by law enforcement on January 30, 2025, with an approximate U.S. dollar value of $2.49;

q. 2,265,186.615965 XRP seized from SwapSpace LLC by law enforcement on January 31,

2025, with an approximate U.S. dollar value of $5,649,375.42;

r. 0.0001 BTC seized from Rabbit Finance LLC (dba CoinRabbit) by law enforcement on February 5, 2025, with an approximate U.S. dollar value of $9.64; and

s. 0.94324 BTC seized from Rabbit Finance LLC (dba CoinRabbit) by law enforcement on February 6, 2025, with an approximate U.S. dollar value of $90,909.59;

all of which was seized by law enforcement agents, pursuant to multiple federal seizure warrants.

BACKGROUND ON VIRTUAL CURRENCY

6. Virtual currencies, alternately commonly known as cryptocurrencies, are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Virtual currencies are not issued by any government or bank like traditional fiat currencies such as the U.S. dollar but are generated and controlled through computer software. Bitcoin is currently the most well-known virtual currency in use.

7. Virtual currency addresses are the particular virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of alphanumeric characters.

8. Each virtual currency address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

9. A virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

10. Many virtual currencies publicly record all their transactions on what was a "blockchain." The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour and record every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

FACTS

11. The Federal investigation underlying the above-described seizures was initiated from a report received by the U.S. Secret Service ("USSS') San Francisco Field Office. On or about January 30, 2024, "Victim 1," a resident of San Francisco, reported to the USSS that approximately $150,000,000 worth of cryptocurrency was transferred out of Victim 1's accounts by an unauthorized actor. As described in further detail below, an unauthorized party gained access to several of Victim 1's personal cryptocurrency wallets, or wallets controlled by Victim 1. Before Victim 1 could alert the relevant authorities and company, the movement of approximately 283,326,127 XRP - which at the time was valued at approximately $149,954,121 U.S. dollar Equivalent ("USDE") [2] - in unauthorized transactions had occurred. From there, the unknown actors transferred the XRP to multiple addresses.

12. Law enforcement knew that individuals who steal cryptocurrency often rapidly move that cryptocurrency across several addresses and often exchange it for other forms of cryptocurrency in an effort to obfuscate the source and final destination of the criminal proceeds, and to evade detection by law enforcement.

13. After notification by Victim 1 of the theft, law enforcement agents then began to trace and seize the stolen funds.

A. Victim 1 XRP Wallet Exploitation

14. On January 31, 2024, agents and analysts from the USSS San Francisco Field Office interviewed Victim 1 and Victim 1's colleague, "Victim 2." Victim 1 stated that the stolen XRP was managed by Victim 1's colleague Victim 2, and that Victim 1 had no knowledge of how the cryptocurrency had been stolen.

15. A subsequent interview with Victim 2 revealed that Victim 2 had opened and managed XRP wallets as directed by Victim 1. Victim 2 stated that Victim 2 would receive the private keys[3] from Victim 1 in written form, after the cryptocurrency wallet was created, then save the private keys in a "secure note" within a commercially available online password manager, a password manager that

[2] USDE value is based on XRP's approximate value at the time of each transaction.

[3] Ownership of cryptocurrency is established through the record of transfers between public addresses on a blockchain, and private keys are used to control the transfer of assets from those addresses.

generates and securely stores passwords and notes. Law enforcement agents knew from their training and experience that password managers such as the online password manager were software programs and/or websites that individuals used to securely manage login credentials for multiple websites and applications, credit card information, and other sensitive information.

16. Victim 2 stated that after inputting the private keys into the online password manager's password vault, which can store data such as passwords, secure notes, banking information, etc., Victim 2 would immediately destroy whatever the private key was written on. Victim 2 stated that Victim 2 had a long, unique password for the online password manager and that once logged in, a device was able to access the online password manager and any secure notes for thirty days. Four devices belonging to Victim 2 had access to the online password manager account which contained the private keys; Victim 2 stated that Victim 2 was aware of only Victim 2's family possessed the knowledge of the passcode of any number of these devices. According to Victim 2, nobody beyond Victim 2's partner knew that Victim 2 managed cryptocurrency wallets for Victim 1.

17. In December 2022, the above-described commercial online password manager suffered two major data breaches – one in August 2022 and one in November 2022 – in which the attackers stole encrypted passwords and the online password manager vault data. The Federal Bureau of Investigation ("FBI") has been investigating these data breaches, and law enforcement agents investigating the instant case have spoken with FBI agents about their investigation. From those conversations, law enforcement agents in this case learned that the stolen data and passwords that were stored in several victims' online password manager accounts were used to illegally, and without authorization, access the victims' electronic accounts and steal information, cryptocurrency, and other data.

18. Law enforcement agents investigating this case are also aware of public reporting of multiple incidents where victims reported the theft of cryptocurrency, specifically, where the only possible means of compromise was the decryption of the stolen online password manager data. According to the FBI, in these other incidents, there were no indicators of compromise on the victim's devices or their personal online password manager accounts. Based on their training and experience, the absence of these indicators of compromise, combined with the fact of the online password manager breaches, strongly suggested to the investigating law enforcement agents that the perpetrators obtained

access to the victims' cryptocurrency by obtaining private keys or other credentials through the online password manager accounts that were compromised because of the breaches.

19. In Victim 1's case, preliminary analysis of the devices that had access to the online password manager account have, similarly, not revealed any indicators of compromise on the devices themselves. Based on their training and experience, as well as that of other agents and analysts involved in this investigation, law enforcement agents knew that the absence of compromise indicators and similar theft typology is an indicator that Victim 1's theft occurred as a result of the 2022 the online password manager breach.

20. Based on their training and experience, law enforcement agents knew the theft of Victim 1's cryptocurrency required the coordinated and rapid movement of a very large amount of cryptocurrency - 283,326,127 XRP (worth over $149 million USDE) - which was then subsequently transferred, exchanged, and dissipated in a short period of time. The scale of a theft and rapid dissipation of funds would have required the efforts of multiple malicious actors, and was consistent with the online password manager breaches and attack on other victims whose cryptocurrency was stolen.

21. For these reasons, law enforcement agents believe the cryptocurrency stolen from Victim 1 was committed by the same attackers who conducted the attack on the online password manager, and cryptocurrency thefts from other similarly situated victims.

B. Law Enforcement's Tracing of the Stolen Cryptocurrency

22. After the theft of cryptocurrency from Victim 1, law enforcement agents reviewed the cryptocurrency transactions, which had siphoned Victim 1's money out of Victim 1's wallet, and the subsequent transfers on the public blockchain. As detailed below, the victim's cryptocurrency (*i.e.*, the criminal proceeds) was rapidly transferred to multiple different addresses, utilizing intermediary transactions.

23. Based upon their training and experience, the rapidity of the above transactions, and the use of multiple accounts controlled by multiple actors, law enforcement agents have concluded that the purpose of these transactions was to frustrate law enforcement's ability to trace and seize the criminal proceeds. In law enforcement's training and experience, these types of cryptocurrency movements, transactions, and chain-hopping activity are often used to complicate and confuse those attempting to

trace transactions using the public blockchain records.

24. Despite the criminal actors' efforts, between June 2024 and February 2025 law enforcement agents were able to trace the stolen cryptocurrency to the following cryptocurrency exchanges: OKX, Payward Interactive, Inc. (dba Kraken), WhiteBIT, AscendEX Technology SRL, Ftrader Ltd (dba FixedFloat), SwapSpace LLC, and Rabbit Finance LLC (dba CoinRabbit). Law enforcement agents then submitted seizure warrants in the Northern District of California to seize the stolen funds, *i.e.*, the Defendant Property.

25. Below is a summary of the tracing for the different transactions, which funneled Victim 1's funds out of Victim 1's cryptocurrency wallet. All dates are on or about the date specified. All amounts are approximate.

C. Tracing From Victim 1's Cryptocurrency Wallet into Different Cryptocurrency Exchanges

a. April 2024 Tracing for Seizures from OKX

26. OKX is a Virtual Asset Service Provider ("VASP") headquartered in the Seychelles with offices and personnel throughout the U.S. OKX operates an exchange that allows customers to trade cryptocurrency for other digital currencies or fiat money. As an exchange, OKX facilitates transactions between users. OKX charges users a trading fee for conducting some categories of transactions on the platform. OKX is owned by OK Group, which also operates a U.S.-based VASP, OK Coin.

27. In April 2024 the Honorable U.S. Magistrate Alex G. Tse signed a seizure warrant in the Northern District of California for the seizure of the following from OKX:

a. Up to 12.0809200059057 bitcoin ("BTC") held in an OKX account identified by User ID: 537320874584945775, herein referred to as "**OKX Subject Account A**";

b. Up to 0.028912099241920002 BTC held in an OKX account identified by User ID: 336438580509590252, herein referred to as "**OKX Subject Account B**";

c. Up to 1.87386576888082 BTC and 20,545.386109146 ("USDT") held in an OKX account identified by User ID: 503216426199425330, herein referred to as "**OKX Subject Account C**"; and

d. Up to 37.8043030402 BTC held in an OKX account identified by User ID:

526009521433359391, herein referred to as "**OKX Subject Account D**."

28. Below is the tracing for these seizures:

Tracing for OKX Subject Account A

29. OKX Subject Account A was purportedly owned by a 24-year-old female from Latvia. The account was created on January 27, 2024, and only ever received funds linked to Victim 1's theft.

30. On January 30, 2024, 18,142,313 XRP, approximately $9,684,182 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rLtfq6. One minute later, 6,000,000 XRP was transferred from rLtfq6 to an address beginning with rLpnam. Less than an hour later, 1,000,000 XRP was transferred from rLpnam to an address beginning with rKMjf4. Finally, less than fifteen minutes later, 319,989.99991 XRP was transferred from rKMjf4 to an address belonging to OKX, which ultimately credited OKX Subject Account A.

31. Additionally, addresses rLtfq6 and rLpnam sent XRP directly to OKX Subject Account A in multiple transfers, including four transfers totaling 3,400,000 XRP from rLtfq6 and 1,050,000 XRP from rLpnam. The entirety of these funds, which total approximately 4,769,990 XRP, was directly traceable to Victim 1's stolen funds. A review of OKX Subject Account A's records revealed that the stolen XRP was promptly exchanged for BTC and then transferred out of the OKX exchange into an address on the Bitcoin blockchain. A portion of those funds, however, were frozen in the account and seized as the proceeds of a specified unlawful activity.

Tracing for OKX Subject Account B

32. OKX Subject Account B was purportedly owned by a 20-year-old female from Russia. The account was created on July 22, 2022.

33. On January 30, 2024, three transfers totaling 663,300 XRP were sent directly from Victim 1's wallet to an address beginning with rs1S85. Additionally, 11,366,068 XRP was sent from Victim 1's wallet to address rs1S85 through several "hops".[4] Afterwards, funds were sent, within hours, in 29 separate transfers totaling 12,013,930.89 XRP from rs1S85 to an address belonging to OKX,

[4] A series of transfers between cryptocurrency addresses.

which ultimately credited OKX Subject Account B. Approximately 11,968,795 XRP was directly traceable to Victim 1's stolen funds.

34. A review of account records revealed that some of the XRP was promptly exchanged for BTC and then transferred out of the OKX exchange into an address on the Bitcoin blockchain, and some of the XRP was exchanged for Tether (USDT) and transferred out of the OKX exchange to an address on the Tron blockchain. A portion of those funds, however, were frozen in the OKX account and seized as the proceeds of a specified unlawful activity.

Tracing for OKX Subject Account C

35. OKX Subject Account C was purportedly owned by a 26-year-old male from Russia. The account was created on October 25, 2023.

36. On January 30, 2024, seven transfers totaling 55,962,941.48 XRP, approximately $29,872,448.00 USDE, were sent from Victim 1's wallet to several XRP addresses. Of the 55,962,941.48 XRP sent, 4,040,000 XRP was sent to address beginning with rsH2j8 through several hops. Lastly, these funds were then sent, within hours, in 29 transfers totaling 4,039,999.99 XRP from rsH2j8 to an address belonging to OKX, which ultimately credited OKX Subject Account C.

37. The entirety of these funds, which total approximately 4,039,999.99 XRP, was directly traceable to Victim 1's stolen funds. A review of account records revealed that some of the funds were promptly converted from XRP to BTC and transferred out of the OKX exchange to an address on the Bitcoin blockchain. Some of the funds were converted into USDT and transferred out of the OKX exchange into an address on the Tron blockchain. A portion of those funds, however, were frozen in the OKX account and seized as the proceeds of a specified unlawful activity.

Tracing for OKX Subject Account D

38. OKX Subject Account D was purportedly owned by a 34-year-old female from Latvia. The account was created on December 27, 2023, and only received three small deposits of BTC just days prior to receiving funds linked to Victim 1's theft.

39. On January 30, 2024, 11,313,133 XRP, approximately $6,038,835 USDE was transferred from Victim 1's wallet to an XRP address beginning with r3kfyj. Less than 20 minutes later, 382,122 XRP was sent from r3kfyj to an address belonging to OKX.

40. On January 30,2024, 4,392,933 XRP was sent from r3kfyj to an XRP address beginning with r32KeW. Within one minute, 564,770 XRP was sent from r32KeW to an address belonging to OKX. Additionally, less than an hour later, 3,300,000 XRP was sent from r32KeW to an XRP address beginning with rhrrpK. Within two minutes, 3,200,000 XRP was sent from rhrrpK to an address belonging to OKX.

41. On January 30, 2024, 3,928,821 XRP was sent from r3kfyj to an XRP address beginning with rn6Y7B. Within four minutes, 490,000 XRP was sent from rn6Y7B to an address belonging to OKX. Additionally, within 12 minutes, 2,900,000 XRP was sent from rn6Y7B to an XRP address beginning with ruSMfG. Less than a minute later, 764,999 XRP was sent from ruSMfG to an address belonging to OKX. Lastly, these funds were ultimately credited to OKX Subject Account D.

42. The entirety of these funds, which total approximately 5,401,891 XRP, was directly traceable to Victim 1's stolen funds. A review of account records revealed that the funds were promptly exchanged for bitcoin (BTC) and transferred out of the OKX exchange onto an address on the Bitcoin blockchain. A portion of those funds, however, were frozen in the account and seized as the proceeds of a specified unlawful activity.

b. <u>May 2024 Tracing for Seizures from Payward Interactive, Inc. (dba Kraken)</u>

43. Kraken is a VASP headquartered in San Francisco, CA. Kraken refers collectively to Payward Ventures, Inc. and its subsidiaries. Kraken operates an exchange that allows customers to trade cryptocurrency for other digital currencies or fiat money. As an exchange, Kraken facilitates transactions between users. Kraken charges users a trading fee for conducting some categories of transactions on the platform., to which this seizure warrant is directed. Kraken's business address is Kraken c/o Payward Ventures, Inc., 237 Kearny Street #102, San Francisco, CA 94108 ("Kraken").

44. In May 2024 the Honorable U.S. Magistrate Judge Sally Kim signed a seizure warrant in the Northern District of California for the seizure of the following from Kraken:

a. Up to 11.1299551100 bitcoin ("BTC") held in a Kraken account identified by account number AA36 N84G 3DOI 2O5I, herein referred to as "Kraken **Subject Account A**";

b. Up to 392,255 Ripple ("XRP") held in a Kraken account identified by account number

AA85 N84G NFOO YGPY, herein referred to as "Kraken **Subject Account B**"; and

c. Up to 136,261 XRP held in a Kraken account identified by account number AA70 N84G VYQZ YFCQ, herein referred to as "Kraken **Subject Account C.**"

45. Below is the tracing for these seizures:

Tracing for Kraken Subject Account A

46. Kraken Subject Account A was purportedly owned by a 50-year-old female from Latvia. The account was created on May 1, 2023, and all XRP in the account was linked to Victim 1's theft. Additionally, the only other account activity in **Kraken Subject Account A** was a small USDT[5] deposit and withdrawal on June 15, 2023.

47. On January 30, 2024, 11,313,133 XRP, valued at approximately $6,038,835 USDE, was transferred from an address in Victim 1's wallet to an XRP address beginning with r3kfyj. Approximately an hour later, 3,928,821 XRP was transferred from r3kfyj to an address beginning with rn6Y7B. Approximately six minutes later, 378,000 XRP was transferred from rn6Y7B to an address belonging to Kraken, which ultimately credited Kraken Subject Account A.

48. Furthermore, on January 30, 2024, 7,151,611 XRP, valued at approximately $3,817,457 USDE, was transferred from another address in Victim 1's wallet to an XRP address beginning with rBY4Ae. Approximately 32 minutes later, 498,059 XRP was transferred from rBY4Ae to an address belonging to Kraken, which ultimately credited Kraken Subject Account A. Five minutes after, 4,830,002 XRP was transferred from rBY4Ae to an address beginning with rMos9D. Within nine minutes, 1,100,000 XRP was transferred from rMos9d to an address belonging to Kraken, which ultimately credited Kraken Subject Account A.

49. The entirety of these funds, which total approximately 1,976,059 XRP, was directly traceable to Victim 1's stolen funds. A review of Kraken Subject Account A's records revealed that the stolen XRP was promptly exchanged for BTC and then transferred out of the Kraken exchange into an address on the Bitcoin blockchain. A portion of those funds, however, were frozen in the account and seized as the proceeds of a specified unlawful activity.

[5] USDT or Tether is another type of cryptocurrency.

Tracing for Kraken Subject Account B

50. Kraken Subject Account B was purportedly owned by a 46-year-old male from Spain. The account was created on January 27, 2024, and only ever received funds linked to Victim 1's theft.

51. On January 30, 2024, 69,714,911 XRP, valued at approximately $37,213,109 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rGhR13. Approximately seven minutes later, 392,255 XRP was transferred from rGhR13 to an address belonging to Kraken, which ultimately credited Kraken Subject Account B. The entirety of these funds, which total approximately 392,255 XRP, was directly traceable to Victim 1's stolen funds.

Tracing for Kraken Subject Account C

52. Kraken Subject Account C was purportedly owned by a 37-year-old female from Spain. The account was created on October 17, 2023, and only ever received funds linked to Victim 1's theft.

53. On January 30, 2024, 69,714,911 XRP, valued at approximately $ 37,213,109 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rGhR13. Over an hour later 4,386,799.990217 XRP was transferred from rGhR13 to an address beginning with r36u4A. Less than an hour and a half later, 136,261 XRP was transferred from r36u4A to an address belonging to Kraken, which ultimately credited Kraken Subject Account C. The entirety of these funds, which total approximately 136,261 XRP, was directly traceable to Victim 1's stolen funds.

c. December 20, 2024, Tracing for Seizures from Ftrader Ltd (dba FixedFloat)

54. FixedFloat, which is run by Ftrader Ltd, is a non-custodial exchange offering fully automated service for exchanging cryptocurrencies. Some of the services FixedFloat offers to their customers is the option to buy and/or swap their cryptocurrency. As a trading platform, FixedFloat charges users a trading fee for conducting some categories of transaction on the platform. FixedFloat's address is House of Francis, Room 303, IleDu Port, Mahe, Seychelles.

55. In December 2024 the Honorable U.S. Magistrate Judge Sally Kim signed a seizure warrant in the Northern District of California for the seizure of the following from Ftrader Ltd (dba FixedFloat):

a. Up to 194,000 XRP held at FixedFloat and identified by transaction hash ABA38D19FF826BF4A3A0B08193997F6571C179AF0658A78EDFAA60DF9F60A37E and associated Order ID 9T47P2, herein referred to as **"FixedFloat Subject Account A"**; and

b. Up to 193,000 XRP held at FixedFloat and identified by transaction hash 4CA9E259D3C1E71067E60FFB4B4072EF81E9698A33941274D7FFA9CCE1315BE1 and associated Order ID QM8FDY, herein referred to as **"FixedFloat Subject Account B."**

56. Below is the tracing for these seizures:

Tracing for FixedFloat Accounts A and B

57. Based on FixedFloat records, a portion of Victim 1 victim's stolen XRP was deposited into FixedFloat. The majority of the stolen XRP was swapped for BTC. However, FixedFloat was able to block two orders and freeze the funds, under their own terms of service.

On January 30, 2024, 10,141,431 XRP, valued at approximately $5,413,392 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rLsUem. Over an hour later, 194,030 XRP was transferred from rLsUem to an address beginning with rMCWxC. Within five minutes, 194,000 XRP was transferred from address rMCWxC to an address belonging to FixedFloat, which was ultimately sent to (or credited) FixedFloat Subject Account A.

The entirety of these funds, which totals approximately 194,000 XRP, was directly traceable to Victim 1's stolen funds.

Additionally, on January 30, 2024, 2,143,331 XRP, valued at approximately $1,144,088 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rHxN46. Less than an hour later, 1,303,320.999946 XRP was transferred from address rHxN46 to an address beginning with rBu8Ni. Within seven minutes, 193,000 XRP was transferred from rBu8Ni to an address belonging to FixedFloat, which ultimately sent these funds to FixedFloat Subject Account B.

The entirety of these funds, which total approximately 193,000 XRP, was directly traceable to Victim 1's stolen funds, and was frozen under FixedFloat's terms of service.

///

d. December 20, 2024, Tracing for Seizures from Rabbit Finance LLC (dba CoinRabbit)

58. CoinRabbit, which is run by Rabbit Finance LLC, is a non-custodial cryptocurrency lending service and exchange. As a lending service, CoinRabbit lends customers assets to borrowers who pay interest on the loans they take. As an exchange platform, users can swap their cryptocurrencies. CoinRabbit's registered address is Richmond Hill Rd, Kingstown, St. Vincent and the Grenadines, VC01000.

59. In December 2024 the Honorable U.S. Magistrate Judge Sally Kim signed a seizure warrant in the Northern District of California for the seizure of the following from Ftrader Ltd (dba FixedFloat):

a. Up to 0.9432396564786945 Bitcoin ("BTC") held at CoinRabbit and identified by transaction hash 0491CFBB0A84152E2BDEA81F8E16C50636D75F7AD81F0309E3318E8C0DD2274, herein after referred to as **"CoinRabbit Subject Account A."**

60. Below is the tracing for these seizures:

Tracing for CoinRabbit Account A

61. Based on CoinRabbit records, a portion of Victim 1 victim's stolen XRP was deposited and swapped for BTC through CoinRabbit. Prior to the funds being withdrawn, CoinRabbit was able to cancel the withdrawal.

62. On January 30, 2024, 7,151,611 XRP, valued at approximately $3,817,457 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rBY4Ae. Over two hours later, 87,000 XRP was transferred from address rBY4Ae to an address belonging to CoinRabbit, which was ultimately sent to (or credited) CoinRabbit Subject Account A.

63. The entirety of these funds, which total approximately 87,000 XRP, was directly traceable to Victim 1's stolen funds.

64. As previously noted, a review of the records provided by CoinRabbit revealed Victim 1 victim's stolen XRP was promptly exchanged for BTC. Prior to the withdrawal, those funds were frozen

in CoinRabbit Subject Account A and are subject to seizure as proceeds of specified unlawful activity. As of May 27, 2024[6], this amounts to 0.9432396564786945 BTC, or approximately $64,642 USDE[7].

e. December 20, 2024, Tracing for Seizures from SwapSpace LLC

65. SwapSpace, which is run by SWAPSPACE LLC, operates as a cryptocurrency exchange aggregator. As an aggregator, SwapSpace collects swap offers from major cryptocurrency exchanges and arranges deals based off the best rate. As a non-custodial platform, SwapSpace offers customers the option to buy, sell and swap their cryptocurrency. SwapSpace's registered address, and principal place of business, is First Floor, First St Vincent Bank Ltd Building, James Street, Kingstown, St. Vincent and the Grenadines.

66. SwapSpace is not a traditional cryptocurrency exchange that holds funds belonging to customers in traditional user accounts. Rather SwapSpace processes "swaps" or "trades" between cryptocurrencies on behalf of users, and temporarily provides users with "SwapSpace Order IDs." SwapSpace does not collect traditional Know Your Customer ("KYC")/subscriber information, as it is solely serving as a money transmitter/exchanger. In these cases, criminal proceeds transferred utilizing SwapSpace were identified solely by the transaction hashes and temporary SwapSpace Order IDs.

67. In December 2024 the Honorable U.S. Magistrate Judge Sally Kim signed a seizure warrant in the Northern District of California for the seizure of the following from SwapSpace LLC:

a. Up to 747,080 Ripple ("XRP") identified by SwapSpace Order ID zsDQ5dAkk and associated transaction hash B3ACA54E4DC060B19E371508FF65B5BB0EBB9AF0F34AFA820B43745E2F10F1E, herein referred to as "**SwapSpace Subject Account A**";

b. Up to 714,100 XRP identified by SwapSpace Order ID rtGlOZ3yRs and associated transaction hash 23662783F5DF42B37CB40E6008C045C5D7127DA706BC65D0D050186081F3E08B, herein referred to as "**SwapSpace Subject Account B**"; and

[6] CoinRabbit's confirmation date of the approximate total sum of frozen funds in the account.

[7] This BTC value was based on the asset's approximate opening value on 5/27/2024 per CoinMarketCap, a popular open-source website that tracks cryptocurrency values in real time.

c. Up to 804,009 XRP identified by SwapSpace Order ID FHlTZR5q4E and associated transaction hash B75770468058B19429E2B3F584B79485E50B7B85ADA9EE8B3427456977851A62, herein referred to as "**SwapSpace Subject Account C.**"

68. Below is the tracing for these seizures:

Tracing for SwapSpace Subject Account A

69. SwapSpace Subject Account A is identified by SwapSpace Order ID zsDQ5dAkk.

70. On January 30, 2024, 2,143,331 XRP, valued at approximately $1,144,088 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rHxN46. Approximately 30 minutes later, 1,303,320.999946 XRP was transferred from rHxN46 to an address beginning with rBu8Ni. Within nine minutes, 747,080 XRP was transferred from rBu8Ni to an address belonging to SwapSpace, which ultimately credited SwapSpace Subject Account A.

71. The entirety of these funds, which total approximately 747,080 XRP, was directly traceable[8] to Victim 1's stolen funds.

Tracing for SwapSpace Subject Account B

72. SwapSpace Subject Account B is identified by SwapSpace Order ID rtGlOZ3yRs.

73. On January 30, 2024, 1,714,114 XRP, valued at approximately $914,977 USDE, was transferred from Victim 1's wallet to an XRP address beginning with r3YWhN. Approximately 24 minutes later, 937,103.999964 XRP was transferred from r3YWhN to an address beginning with rwtM83. Within nine minutes, 714,100 XRP was transferred from rwtM83 to an address belonging to SwapSpace, which ultimately credited SwapSpace Subject Account B.

74. The entirety of these funds, which total approximately 714,100 XRP, was directly traceable to Victim 1's stolen funds.

Tracing for SwapSpace Subject Account C

75. SwapSpace Subject Account C is identified by SwapSpace Order ID FHlTZR5q4E.

[8] Using a "last in, first out" (or "LIFO") tracing methodology in which the cryptocurrencies from immediately preceding transfers are the first withdrawn in subsequent transfers before any other funds, each of these transfers contained all of the funds traceable to Victim 1's stolen funds.

76. On January 30, 2024, 5,186,526 XRP, valued at approximately $2,768,515 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rMgfrA. Over an hour later, 3,397,495.999946 XRP was transferred from rMgfrA to an address beginning with r4GR3G. Less than an hour later, 804,009 XRP was transferred from r4GR3G to an address belonging to SwapSpace, which ultimately credited SwapSpace Subject Account C.

77. The entirety of these funds, which total approximately 804,009 XRP, was directly traceable to Victim 1's stolen funds.

f. December 20, 2024, Tracing for Seizures from AscendEX Technology SRL

78. AscendEX is a cryptocurrency trading platform. AscendEX allows customers to trade cryptocurrency for other digital assets or fiat money. As a trading platform, AscendEX charges users a trading fee for conducting some categories of transaction on the platform. AscendEX Technology SRL is the operational entity for the exchange. AscendEX Technology SRL provided to law enforcement their business address as Bucuresti Sectorul 2, Strada Mihai Eminescu Nr. 105-107, O CAMERA, Etaj 5, Ap. 19. Per AscendEX's website at https://ascendex.com/en/risk last accessed on December 19, 2024, at 8:52 PM, the company is located in Romania.

79. In December 2024 the Honorable U.S. Magistrate Judge Sally Kim signed a seizure warrant in the Northern District of California for the seizure of the following from AscendEX Technology SRL:

80. Up to 355,923.72 Tether ("USDT") held in an AscendEX account identified by user UID U3001155122, herein referred to as "**AscendEX Subject Account A**."

81. Below is the tracing for these seizures:

Tracing for AscendEX Subject Account A

82. AscendEX Subject Account A was purportedly owned by a 20-year-old male from Ukraine. The account was created on October 4, 2023, and only received a small amount of BTC on January 27, 2024, before receiving funds linked to Victim 1's theft.

83. On January 30, 2024, 18,142,313 XRP, valued at approximately $9,684,182 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rLtfq6. Almost six hours later,

500,000 XRP was transferred from rLtfq6 to an address belonging to AscendEX, which ultimately credited AscendEX Subject Account A.

84. The entirety of these funds, which total approximately 500,000 XRP, was directly traceable to Victim 1's stolen funds.

85. A review of AscendEX Subject Account A's records revealed that the 500,000 XRP was exchanged for approximately to 5.93823 BTC. The funds were frozen in the account and seized as the proceeds of a specified unlawful activity.

g. December 20, 2024, Tracing for Seizures from WhiteBIT

86. WhiteBIT.com is a regulated cryptocurrency exchange headquartered in Vilnius, Vilniaus Apskritis, Lithuania, and licensed in Spain, Lithuania, Poland, Czech Republic, and Bulgaria. WhiteBIT operates an exchange, among other services, that allows customers to trade cryptocurrency for other digital currencies or fiat money. As an exchange, WhiteBIT facilitates transactions between users. WhiteBIT charges users a trading fee for conducting some categories of transactions on the platform. Transactions can be executed by registered WhiteBIT users or exchange orders can be submitted by clients of various third-party exchange services who utilize WhiteBIT's application programming interface ("API") and transit gateway. In these cases, verification of these clients is carried out by the third-party exchange services outside of WhiteBIT's platform, and WhiteBIT will not receive this information.

87. In other words, regarding transactions by a third-party exchange service, which solely uses WhiteBIT's API and liquidity for money transmittance, WhiteBIT does not receive any of the traditional Know Your Customer ("KYC")/subscriber information, as it is solely serving as a money transmitter/exchanger on behalf of another cryptocurrency exchange. In these cases, criminal proceeds transferred utilizing WhiteBIT are identified by the transaction hash, and associated details (*e.g.*, time, and sending address).

88. In July 2024 the Honorable U.S. Magistrate Judge Hixson signed a seizure warrant in the Northern District of California for the seizure of the following from WhiteBIT.com:

a. Up to 650,000 Ripple ("XRP") held in a WhiteBIT account identified by user kannap@inbox.lv, herein referred to as "WhiteBIT Subject Account A";

b. Up to 451,105 XRP held in a WhiteBIT account identified by user whitebit0@inbox.lv, herein referred to as "WhiteBIT Subject Account B";

c. Up to 839,032 XRP held in a WhiteBIT account identified by user lacplesis1100@outlook.com, herein referred to as "WhiteBIT Subject Account C";

d. Up to 473,761 XRP associated with exchange order from email address k99pshfg@10mail.tk, herein referred to as "WhiteBIT Subject Account D";

e. Up to 460,000 XRP associated with exchange order from email address rbontdeid@laste.ml, herein referred to as "WhiteBIT Subject Account E";

f. Up to 62,000 XRP associated with exchange order from email address Arthju896@proton.me, herein referred to as "WhiteBIT Subject Account F";

g. Up to 61,030 XRP associated with exchange order from email address k9czgfy1@10mail.tk, herein referred to as "WhiteBIT Subject Account G";

h. Up to 75,400 XRP associated with exchange order from email address tonlodieg@emltmp.com, herein referred to as "WhiteBIT Subject Account H";

i. Up to 70,000 XRP associated with exchange order from email address wnaetdeid@laste.ml, herein referred to as "WhiteBIT Subject Account I";

j. Up to 42,451 XRP associated with exchange order from email address f17k91wg@spymail.one, herein referred to as "WhiteBIT Subject Account J";

k. Up to 94,009.70 XRP associated with exchange order from email address centrumxx@protonmail.com, herein referred to as "WhiteBIT Subject Account K",

l. Up to 74,930 XRP associated with exchange order from email address iahanama009@outlook.com, herein referred to as "WhiteBIT Subject Account L";

m. Up to 83,275.73 XRP associated with exchange order from email address pushpendra@inbox.lv, herein referred to as "WhiteBIT Subject Account M";

n. Up to 100,000 XRP associated with exchange order transaction hash F311746FB0075F44F1A2D9E8F4686E61EC0B2D7CCD52E00B5BB58204EAA06BA, herein referred to as "WhiteBIT Subject Account N";

o. Up to 58,504 XRP associated with exchange order transaction hash 4C0E24296D9F61044BD3FE3E8E87651CA128A9B9A6CAA2AEB4B018D32FDB9623, herein referred to as "WhiteBIT Subject Account O"; and

p. Up to 70,000 XRP associated with exchange order from email address kedbi4@gmail.com, herein referred to as "WhiteBIT Subject Account P."

89. Below is the tracing for these seizures:

Tracing for WhiteBIT Subject Account A

90. Based upon WhiteBIT user records, WhiteBIT Subject Account A was purportedly owned by a 32-year-old male from Latvia. The account was created on January 25, 2024, and only ever received funds linked to Victim 1's theft.

91. On January 30, 2024, 18,142,313 XRP, valued at approximately $9,684,182 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rLtfq6. Approximately one minute later, 6,000,000 XRP was transferred from rLtfq6 to an address beginning with rLpnam. Less than an hour later, two separate transfers totaling 650,000 XRP were transferred from rLpnam to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account A.

92. The entirety of these funds, which total approximately 650,000 XRP, was directly traceable[9] to Victim 1's stolen funds.

Tracing for WhiteBIT Subject Account B

93. Based upon WhiteBIT user records, WhiteBIT Subject Account B was purportedly owned by a 22-year-old female from Latvia. The account was created on April 17, 2023, and only ever received funds linked to Victim 1's theft.

94. On January 30, 2024, 69,714,911 XRP, valued at approximately $37,213,109 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rGhR13. Approximately five minutes later, 451,105 XRP was transferred from rGhR13 to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account B.

[9] Using a "last in, first out" (or "LIFO") tracing methodology in which the cryptocurrencies from immediately preceding transfers are the first withdrawn in subsequent transfers before any other funds, each of these transfers contained all of the funds traceable to Victim 1's stolen funds.

95. The entirety of these funds, which total approximately 451,105 XRP, was directly traceable to Victim 1's stolen funds.

Tracing for WhiteBIT Subject Account C

96. Based upon WhiteBIT user records, WhiteBIT Subject Account C was purportedly owned by a 27-year-old male from Latvia. The account was created on March 24, 2023, and all XRP currently in the account was linked to Victim 1's theft. Additionally, the only other account activity was a small bitcoin (BTC) deposit, swap from BTC to ether[10] (ETH), and ETH withdrawal on January 26, 2024.

97. On January 30, 2024, 7,151,611 XRP, valued at approximately $3,817,457 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rBY4Ae. Approximately three minutes later, 349,000 XRP was transferred from rBY4Ae to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account C. Additionally, approximately 33 minutes later, 4,830,002 XRP was transferred from rBY4Ae to an address beginning with rMos9d. Approximately a minute and a half later, 490,032 XRP was transferred from rMos9d to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account C.

98. The entirety of these funds, which total approximately 839,032 XRP, was directly traceable to Victim 1's stolen funds.

Tracing for WhiteBIT Subject Account D

99. WhiteBIT Subject Account D is not a registered WhiteBIT user. Instead, the exchange orders were submitted by a client of a third-party exchange service utilizing WhiteBIT's API and transit gateway. All eight exchange orders originated from email address k99pshfg@10mail.tk and are linked to Victim 1's theft.

100. On January 30, 2024, transfers totaling 473,761 XRP were sent from Victim 1's wallets, through several "hops"[11], to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account D.

[10] Ether is the native token on the Ethereum network.

[11] A series of transfers between cryptocurrency addresses.

101. A review of WhiteBIT Subject Account D's records revealed one of the transactions, transaction hash 82D011593F1BFB5A6FD9247ED3D6366ADCC74DE85C8BE6A82DA9DC522DBEC434 for 60,000 XRP, underwent immediate conversion from XRP to BTC after the funds were deposited to WhiteBIT. However, WhiteBIT's team executed the funds' block/suspension procedures and converted the BTC back to XRP. Due to the exchange rates and fees, this resulted in a slight deviation from the initially deposited amount of 60,000 XRP.

102. The entirety of these funds, which total approximately 473,761 XRP, was directly traceable to Victim 1's stolen funds.

Tracing for WhiteBIT Subject Account E

103. WhiteBIT Subject Account E is not a registered WhiteBIT user. Instead, the exchange orders were submitted by a client of a third-party exchange service utilizing WhiteBIT's API and transit gateway. All three exchange orders originated from email address rbontdeid@laste.ml and are linked to Victim 1's theft.

104. On January 30, 2024, transfers totaling 460,000 XRP were sent, within one hop, from Victim 1's wallets to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account D.

105. The entirety of these funds, which total approximately 460,000 XRP, was directly traceable to Victim 1's stolen funds.

Tracing for WhiteBIT Subject Account F

106. WhiteBIT Subject Account F is not a registered WhiteBIT user. Instead, the exchange order was submitted by a client of a third-party exchange service utilizing WhiteBIT's API and transit gateway. The exchange order originated from email address Arthju896@proton.me and was linked to Victim 1's theft.

107. On January 30, 2024, 11,313,133 XRP, valued at approximately $6,038,835 USDE, was transferred from Victim 1's wallet to an XRP address beginning with r3kfyj. Over an hour later, 3,928,821 XRP was transferred from r3kfyj to an XRP address beginning with rn6Y7B. Lastly, 62,000

XRP was transferred from rn6Y7B to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account F.

108. The entirety of these funds, which total approximately 60,000 XRP, was directly traceable to Victim 1's stolen funds.

Tracing for WhiteBIT Subject Account G

109. WhiteBIT Subject Account G is not a registered WhiteBIT user. Instead, the exchange order was submitted by a client of a third-party exchange service utilizing WhiteBIT's API and transit gateway. The exchange order originated from email address k9czgfy1@10mail.tk and was linked to Victim 1's theft.

110. On January 30, 2024, 1,623,255 XRP, valued at approximately $866,477 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rh7rd9. Approximately five minutes later, 61,030 XRP was transferred from rh7rd9 to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account G.

111. The entirety of these funds, which total approximately 61,030 XRP, was directly traceable to Victim 1's stolen funds.

Tracing for WhiteBIT Subject Account H

112. WhiteBIT Subject Account H is not a registered WhiteBIT user. Instead, the exchange order was submitted by a client of a third-party exchange service utilizing WhiteBIT's API and transit gateway. The exchange order originated from email address tonlodieg@emltmp.com and was linked to Victim 1's theft.

113. On January 30, 2024, 1,623,255 XRP, valued at approximately $866,477 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rh7rd9. Approximately six minutes later, 75,400 XRP was transferred from rh7rd9 to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account H.

114. The entirety of these funds, which total approximately 75,400 XRP, was directly traceable to Victim 1's stolen funds.

///

///

Tracing for WhiteBIT Subject Account I

115. WhiteBIT Subject Account I is not a registered WhiteBIT user. Instead, the exchange order was submitted by a client of a third-party exchange service utilizing WhiteBIT's API and transit gateway. The exchange order originated from email address wnaetdeid@laste.ml and was linked to Victim 1's theft.

116. On January 30, 2024, 22,124,313 XRP, valued at approximately $11,809,733 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rKPERa. Over an hour later, 70,000 XRP was transferred from rKPERa to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account I.

117. The entirety of these funds, which total approximately 70,000 XRP, was directly traceable to Victim 1's stolen funds.

Tracing for WhiteBIT Subject Account J

118. WhiteBIT Subject Account J is not a registered WhiteBIT user. Instead, the exchange order was submitted by a client of a third-party exchange service utilizing WhiteBIT's API and transit gateway. The exchange order originated from email address f17k91wg@spymail.one and was linked to Victim 1's theft.

119. On January 30, 2024, 69,714,911 XRP, valued at approximately $37,213,109 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rGhR13. Approximately 21 minutes later, 16,143,113 XRP was transferred from rGhR13 to an XRP address beginning with rntvnT. After several hours, 42,451 XRP was transferred from rntvnT to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account J.

120. The entirety of these funds, which total approximately 42,451 XRP, was directly traceable to Victim 1's stolen funds.

Tracing for WhiteBIT Subject Account K

121. WhiteBIT Subject Account K is not a registered WhiteBIT user. Instead, the exchange order was submitted by a client of a third-party exchange service utilizing WhiteBIT's API and transit gateway. The exchange order originated from email address centrumxx@protonmail.com and was linked to Victim 1's theft.

122. On January 30, 2024, 7,151,611 XRP, valued at approximately $3,817,457 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rBY4Ae. Approximately two and a half hours later, 94,039 XRP was transferred from rBY4Ae to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account K.

123. A review of Subject Account K's transaction, transaction hash C167B15FCB0BFE8001B16ABE28CC6B20813495A39AE10610D5951A6A10A5EDAD for 94,039 XRP, underwent immediate conversion from XRP to BTC after the funds were deposited to WhiteBIT. However, WhiteBIT's team executed the funds' block/suspension procedures and converted the BTC back to XRP. Due to the exchange rates and fees, this resulted in a slight deviation from the initially deposited amount of 94,039 XRP.

124. The entirety of these funds, which total approximately 94,009.70 XRP, was directly traceable to Victim 1's stolen funds.

Tracing for WhiteBIT Subject Account L

125. WhiteBIT Subject Account L is not a registered WhiteBIT user. Instead, the exchange order was submitted by a client of a third-party exchange service utilizing WhiteBIT's API and transit gateway. The exchange order originated from email address iahanama009@outlook.com and was linked to Victim 1's theft.

126. On January 30, 2024, 7,151,611 XRP, valued at approximately $3,817,457 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rBY4Ae. Over an hour later, 1,293,044 XRP was transferred from rBY4Ae to an XRP address beginning with rGQGWV. Approximately five minutes later, 74,930 XRP was transferred to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account L.

127. The entirety of these funds, which total approximately 74,930 XRP, was directly traceable to Victim 1's stolen funds.

Tracing for WhiteBIT Subject Account M

128. WhiteBIT Subject Account M is not a registered WhiteBIT user. Instead, the exchange order was submitted by a client of a third-party exchange service utilizing WhiteBIT's API and transit

gateway. The exchange order originated from email address pushpendra@inbox.lv and was linked to Victim 1's theft.

129. On January 30, 2024, 7,151,611 XRP, valued at approximately $3,817,457 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rBY4Ae. Approximately 30 minutes later, 1,830,002 XRP was transferred from rBY4Ae to an XRP address beginning with rMos9d. Over an hour later, 1,290,000 XRP was transferred from rMos9d to an address beginning with rHkQBT. Less than an hour later, 83,275.73 was transferred from rHkQBT to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account M.

130. The entirety of these funds, which total approximately 83,275.73 XRP, was directly traceable to Victim 1's stolen funds.

Tracing for WhiteBIT Subject Account N

131. WhiteBIT Subject Account N is not a registered WhiteBIT user. Instead, the exchange order was submitted by a client of a third-party exchange service utilizing WhiteBIT's API and transit gateway. The exchange order information did not provide an associated email address, but transaction hash F311746FB0075F44F1A2D9E8F4686E61EC0B2D7CCD52E00B5BB58204EAA06BA6 was linked to Victim 1's theft.

132. On January 30, 2024, 69,714,911 XRP, valued at approximately $37,213,109 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rGhR13. Approximately 21 minutes later, 16,143,113 XRP was transferred from rGhR13 to an XRP address beginning with rntvnT. Several hours later, 100,000 XRP was transferred from rntvnT to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account N.

133. The entirety of these funds, which total approximately 100,000 XRP, was directly traceable to Victim 1's stolen funds.

Tracing for WhiteBIT Subject Account O

134. WhiteBIT Subject Account O is not a registered WhiteBIT user. Instead, the exchange order was submitted by a client of a third-party exchange service utilizing WhiteBIT's API and transit gateway. The exchange order information did not provide an associated email address, but transaction

hash 4C0E24296D9F61044BD3FE3E8E87651CA128A9B9A6CAA2AEB4B018D32FDB9623 was linked to Victim 1's theft.

135. On January 30, 2024, 651,414 XRP, valued at approximately $347,718 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rHhjp1. Over three hours later, 59,132 XRP was transferred from rHhjp1to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account O.

136. A review of WhiteBIT Subject Account O's transaction, transaction hash 4C0E24296D9F61044BD3FE3E8E87651CA128A9B9A6CAA2AEB4B018D32FDB9623 for 59,132 XRP, underwent immediate conversion from XRP to BTC after the funds were deposited to WhiteBIT. However, WhiteBIT's team executed the funds' block/suspension procedures and converted the BTC back to XRP. Due to the exchange rates and fees, this resulted in a slight deviation from the initially deposited amount of 59,132 XRP.

137. The entirety of these funds, which total approximately 58,504 XRP, was directly traceable to Victim 1's stolen funds.

Tracing for WhiteBIT Subject Account P

138. WhiteBIT Subject Account P is not a registered WhiteBIT user. Instead, the exchange order was submitted by a client of a third-party exchange service utilizing WhiteBIT's API and transit gateway. The exchange order originated from email address kedbi4@gmail.com and was linked to Victim 1's theft.

139. On January 30, 2024, 22,124,313 XRP, valued at approximately $11,809,733 USDE, was transferred from Victim 1's wallet to an XRP address beginning with rKPERa. Less than an hour later, 70,000 XRP was transferred from rKPERa to an XRP address beginning with r3up8w. Within 15 minutes, 70,000 XRP was transferred from r3up8w to an address belonging to WhiteBIT, which ultimately credited WhiteBIT Subject Account P.

140. The entirety of these funds, which total approximately 70,000 XRP, was directly traceable to Victim 1's stolen funds.

///

///

CONCLUSION

141. Based on this investigation, law enforcement had probable cause to believe the same attackers behind the above-described commercial online password manager attack used a stolen password held in Victim 1's online password manager account and, without authorization, accessed his cryptocurrency wallet/account, which held Victim 1's XRP tokens, in violation of Title 18, United States Code, Section 1030 (Computer hacking). The attackers then stole and transferred these XRP tokens – worth more than $149 million USDE - quickly to other individuals/accounts for their own use, in violation of Title 18, United States Code, Section 2314 (Interstate Transportation of Stolen Property). In so doing, they moved the cryptocurrency across multiple addresses/wallets in an attempt to conceal/disguise their nature, location, source, ownership, or control in violation of Title 18, United States Code, Section 1956 (Money Laundering).

142. Based upon the rapidity of the above transactions, and use of multiple accounts controlled by multiple actors, law enforcement believed the attackers engaged in these transactions to specifically obfuscate the source of their criminal proceeds, obtained from the victim. In their training and experience, these types of movements, transactions, and chain-hopping activity are often used to complicate and confuse those attempting to trace transactions using the public blockchain records.

143. For the reasons set forth above, there is probable cause to conclude that the numerous Subject Accounts – at the above-described exchanges OKX, Payward Interactive, Inc. (dba Kraken), WhiteBIT, AscendEX Technology SRL, Ftrader Ltd (dba FixedFloat), SwapSpace LLC, and Rabbit Finance LLC (dba CoinRabbit) - contained the proceeds of the Target Offenses. Pursuant to federal seizure warrants signed by U.S. Magistrate Court judges in the Northern District of California, law enforcement seized the Defendant Property, which is now in government control, and should be forfeited to the U.S. government for proper disposition, pursuant to Title 18, United States Code, Sections 981.

VIOLATION

144. The United States incorporates by reference the allegations in paragraphs one through **143** as though fully set forth.

145. Title 18, United States Code, Section 2314 (**interstate transportation of stolen property**) makes it a crime to, among other things transport, knowingly transmit, or transfer in interstate

or foreign commerce any goods, wares, merchandise, securities, or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud.

146. Title 18, United States Code, Section 1030(a)(2)(C) (**computer hacking**) imposes criminal penalties on whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains – … (C) information from any protected computer." Title 18, United States Code, Section 1030(e)(2)(B) defines a "protected computer" to include any computer "which is used in or affecting interstate or foreign commerce or communication."

147. Title 18, United States Code, Section 1956 (**money laundering**) makes it unlawful to knowingly conduct a financial transaction involving the proceeds of a specified unlawful activity with the intent to promote the carrying on of that specified unlawful activity or to conceal or disguise the nature, location, source, ownership, or control of the proceeds of specified unlawful activity. Under Title 18, United States Code, Section 1956(c)(7), a violation of Title 18, United States Code, Sections 1030 and 2314 are both considered specified unlawful activities.

148. Title 18, United States Code, Section 981(a)(1)(C) provides for civil and criminal forfeiture of "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to a violation of section [. . .] 1030" (Computer hacking) or "any offense constituting 'specified unlawful activity' (as defined in section 1956(c)(7) of [Title 18]), or a conspiracy to commit such offense." Specified unlawful activities are enumerated therein, as well as at Title 18, United States Code, Sections 1956(c)(7) and 1961(1), which provide that Title 18, United States Code, Sections 2314 (Interstate Transportation of Stolen Property) is a specified unlawful activity. This section provides both civil forfeiture authority and criminal forfeiture authority (by virtue of Title 28, United States Code, Section 2461(c)).

149. In light of the foregoing, and considering the totality of the circumstances, there is probable cause to believe that the entirety of the Defendant Property represents proceeds traceable to computer hacking and the interstate transportation of stolen property, in violation of violation 18 U.S.C. §§ 2314 and 1030. As such, the Defendant Property is forfeitable pursuant to 18 U.S.C. § 981(a)(1)(C).

150. WHEREFORE, plaintiff United States of America requests that due process issue to enforce the forfeiture of the Defendant Property; that notice be given to all interested parties to appear

and show cause why forfeiture should not be decreed; that judgment of forfeiture be entered; that the Court enter judgment forfeiting the Defendant Property; and that the United States be awarded such other relief as may be proper and just.

DATED: 03/06/2025

Respectfully submitted,
PATRICK D. ROBBINS
Acting United States Attorney

/s/ Donovan McKendrick
DONOVAN M. MCKENDRICK
Special Assistant United States Attorney

DAVID COUNTRYMAN
Assistant United States Attorney

VERIFICATION

I, FRANK NGUYEN, state as follows:

1. I am a Special Agent with the U.S. Department of Homeland Security, United States Secret Service ("USSS"). I am a case agent assigned to this case. As such, I am familiar with the facts, and the investigation leading to the filing of this Complaint for Forfeiture.

2. I have read the Complaint and believe the allegations contained in it to be true.

* * * * *

I declare under penalty of perjury that the foregoing is true and correct. Executed this 5th day of March 2025 in Walnut Creek, California.

/s/ Frank Nguyen
FRANK NGUYEN
Special Agent
United States Secret Service