UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF GEORGIA
SAVANNAH DIVISION

UNITED STATES OF AMERICA	)	
	)	
v.	)	**Civil Case No.**
	)	
CRYPTOCURRENCY DESCRIBED BELOW IN PARAGRAPH THREE	)	

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

COMES NOW the United States of America (the "United States" or the "Government"), by and through Jill E. Steinberg, United States Attorney for the Southern District of Georgia, and J. Bishop Ravenel, Assistant United States Attorney, and brings this Verified Complaint for Civil Forfeiture *In Rem*, with the following allegations:

NATURE OF THE ACTION

1. *In Rem* civil forfeiture is permissible under Rule G of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions.

2. The Defendants *In Rem* are subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) and (C) on the grounds that the Defendant Property, as defined later herein, is proceeds traceable to and/or derived from wire fraud in violation of 18 U.S.C. § 1343 and wire fraud attempt and conspiracy in violation of 18 U.S.C. § 1349, as well as property involved in, or traceable to such property involved in, money laundering and conspiracy to commit money laundering in violation of 18 U.S.C. §§ 1956 and 1957.

THE DEFENDANTS *IN REM*

3. The Defendants *In Rem* (hereinafter, the **"Defendant Property"**) represent the following assets:

a. All funds and other items of value held by Binance[1] user ID #161885085, particularly including 46.7900 USDT (Tether) received by the Government on or about September 5, 2023, and 29,348.653413 USDT (Tether) received by the Government on or about November 6, 2023 ("**Subject Account A**"); and

b. All funds and other items of value held by Binance user ID #547453271, particularly including 0.00013 BTC (Bitcoin) received by the Government on or about September 5, 2023, and 9.9036518 BTC (Bitcoin) received by the Government on or about September 11, 2023 ("**Subject Account B**").

The **Defendant Property** was seized on or about November 6, 2023[2], from Binance via electronic transfers as the result of a federal seizure warrant authorized in the Southern District of Georgia on May 17, 2023.

JURISDICTION AND VENUE

4. The United States brings this action *In Rem* in its own right to forfeit the **Defendant Property**.

5. This Court has jurisdiction over an action commenced by the United States pursuant to 28 U.S.C. § 1345.

6. The Court has jurisdiction over an action for forfeiture pursuant to 28 U.S.C. § 1355(a).

---

[1] BAM Trading Services Inc. d/b/a Binance.US is referred to herein as "Binance," the common name under which it operates.

[2] Binance provided the **Defendant Property** through a series of electronic transfers to the United States Secret Service beginning on or about September 5, 2023, and culminating on or about November 6, 2023, in response to a federal seizure warrant served shortly after its authorization in May 2023.

7. The Court has *In Rem* jurisdiction over the **Defendant Property** pursuant to 28 U.S.C. § 1355(b).

8. Venue is proper in this district pursuant to 28 U.S.C. § 1355(b)(1) because acts and/or omissions giving rise to the forfeiture of the **Defendant Property** occurred in this district.

9. Particularly, wires in furtherance of this fraud scheme began, continued, and/or completed in the Southern District of Georgia; acts in furtherance of a violation of 18 U.S.C. § 1349 (conspiracy to commit wire fraud in violation of 18 U.S.C. § 1343) occurred in the Southern District of Georgia; and attempts to commit violations of 18 U.S.C. § 1343 (in violation of 18 U.S.C. § 1349) occurred in the Southern District of Georgia.

10. Additionally, acts in furtherance of violations of 18 U.S.C. §§ 1956, 1956(h), and 1957 occurred in the Southern District of Georgia; violations of the underlying specified unlawful activities, as described in the previous paragraph, occurred in the Southern District of Georgia; and attempts to commit 18 U.S.C. §§ 1956 and 1957 occurred in the Southern District of Georgia.

11. The **Defendant Property** is currently in the possession of the United States Secret Service ("USSS") and was seized from Binance, a cryptocurrency company operating in the United States including but not limited to in Georgia.

12. The **Defendant Property** is not tangible.

BACKGROUND INFORMATION

13. During the time period of the crimes alleged in this Verified Complaint, between in or about February 2023 and in or about April 2023, the following information in this section, titled "Background Information," was true and correct.

14. Virtual currencies, which include cryptocurrencies, are digital tokens of value circulated over the internet as substitutes for traditional fiat currency. 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 a well-known virtual currency.

15. 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.

16. 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.

17. 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.

18. Many virtual currencies publicly record all of their transactions on what is known as 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 records 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.

19. Tether, widely known as "USDT," is a blockchain based cryptocurrency whose tokens in circulation are backed by an equivalent amount of U.S. dollars, making it what is known as a "stablecoin." USDT is issued by Tether Ltd., a company headquartered in Hong Kong. Tether is connected to Bitfinex, a cryptocurrency exchange registered in the British Virgin Islands.

20. USDT is hosted on the Ethereum blockchain, among others. Ether ("ETH") is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a platform that uses "smart contract" technology. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track the movement of the ETH.

21. Smart contracts allow developers to create markets, store registries of debts, and move funds in accordance with the instructions provided in the contract's code, all while using the Ethereum blockchain protocol to maintain transparency. Smart contract technology is one of Ethereum's distinguishing characteristics and an important tool for companies or individuals executing trades on the Ethereum blockchain. When engaged, smart contracts automatically execute according to the

terms of the contract written into lines of code. A transaction contemplated by a smart contract occurs on the Ethereum blockchain and is both trackable and irreversible.

22. Like other virtual currencies, USDT is sent to and received from a USDT "address." An address is somewhat analogous to a bank account number and is represented as a 26 to 35 character long case-sensitive string of letters and numbers. Users can operate multiple addresses at any given time, with the possibility of using a unique address for every transaction.

23. Although the identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity.

24. Unlike bitcoin, USDT is "centralized," meaning that it is issued and controlled by a governing body. Most other cryptocurrencies are "decentralized" and have no such governing body.

25. Pig Butchering is a type of romance scam, or confidence scam, that convinces victims to invest in non-existent cryptocurrency trading platforms. Romance scams target persons looking for romantic partners or friendships on dating websites and other social media platforms. The scammers may create profiles using fictitious or fake names, locations, images, and personas, allowing the scammers to cultivate relationships with prospective romance scam victims. Romance scams aim

to use the fictitious relationship to obtain money or induce victims to conduct financial transaction(s) on behalf of the scammers. In one variation of the "Pig Butchering" scheme, scammers pose as potential home buyers with a budget of over a million dollars. The scammers cultivate the buyer/agent relationship before introducing a fake cryptocurrency platform along with fabricated successful returns on investments.

FACTS AND BASIS OF FORFEITURE

Wire Fraud and Wire Fraud Conspiracy Scheme

Victim 1 Online Scam

26. This investigation was initiated from a suspected fraud attempt report received by the USSS Savannah Resident Office from a real estate agent and a resident of Richmond Hill, Georgia ("VICTIM 1") located in the Southern District of Georgia.

27. On or about April 10, 2023, VICTIM 1 contacted the USSS Savannah Resident Office regarding communication with a person identifying himself[3] as "Jay," and VICTIM 1 provided the following information to the USSS regarding VICTIM 1's interaction with "Jay."

28. "Jay" stated "Jay" was a potential home buyer relocating from California, with a price range of $1 to $3 million for a five bedroom and five bath single family dwelling in a quiet neighborhood in Savannah, Georgia.

[3] Because this scheme involves an online scam and based on the investigation to date, the gender, true name, and identity of the perpetrators are not identified herein.

29. "Jay" contacted VICTIM 1 using WhatsApp, an application on a smart phone device in which communication is conducted through text messaging and phone calls via Voiceover IP ("VoIP").

30. VICTIM 1 provided the USSS with screenshots of the text messaging communications with "Jay."

31. "Jay's" phone number, (310) 935-0810, was displayed on the screenshots of "Jay's" WhatsApp text messages with VICTIM 1.

32. "Jay" also provided VICTIM 1 with the email address, zbud66888@gmail.com, so VICTIM 1 could send "Jay" real estate listings to review.

33. VICTIM 1 stated it was not unusual to have international customers contact VICTIM 1 on WhatsApp.

34. However, VICTIM 1 stated VICTIM 1 did have a suspicion that something was not quite right.

35. VICTIM 1 based this suspicion on how the conversation was more about "Jay" coaching VICTIM 1 on cryptocurrency and using cryptocurrency (USDT) to make the property purchase than it was about the specifics of the property "Jay" was looking to purchase.

36. "Jay" also explained that "Jay" was a manager at Goldman Sachs 1MD for many years before resigning in 2015 and setting up "Jay's" own big data analysis team and trading options for nearly eight years.

37. VICTIM 1 also reported that "Jay" called VICTIM 1 using WhatsApp and described "Jay" as having an "Asian" accent.

38. VICTIM 1 indicated that VICTIM 1 received electronic communications from "Jay" in early 2023, including via WhatsApp, while VICTIM 1 was located in the Southern District of Georgia and concerning property in the Southern District of Georgia.

39. A database check for phone number (310) 935-0810 revealed the number was registered a VoIP service in which phone numbers can be changed often and can be used to cloak the identity of the caller.

Additional Victim Identified

40. A query of the Federal Bureau of Investigation's ("FBI") Internet Crime Complaint Center ("IC3"), a platform in which victims of fraud schemes can file complaints, revealed two complaints filed on or about April 8, 2023.

41. The search criteria used to find these complaints was the email address "Jay" provided to VICTIM 1, zbud66888@gmail.com.

42. Both IC3 complaints were filed by the same victim, a real estate agent located in North Carolina ("VICTIM 2").

43. In VICTIM 2's complaint, VICTIM 2 described losing $200,000 after VICTIM 2 was asked to trade cryptocurrency on a platform called Stormgain, and provided the following information regarding the scam.

44. When VICTIM 2 attempted to transfer VICTIM's funds from Stormgain back to VICTIM 2's Coinbase wallet, the company (Stormgain) kept giving VICTIM 2 excuses on why the Stormgain could not send it.

45. Stormgain said that if VICTIM 2 was a premier member, VICTIM 2 could get access to funds in 10 minutes, but it would cost another $50,000.

46. Stormgain also said to protect VICTIM 2's identity, Stormgain would need risk guarantee funds.

47. The description of the scam provided in the complaint is consistent with tactics used in "Pig Butchering" schemes, as described above.

48. Based on the information VICTIM 1 provided, USSS found other recent victims of "Pig Butchering" who filed complaints using the FBI's IC3.

49. On or about April 12, 2023, USSS investigators interviewed VICTIM 2 regarding the complaints VICTIM 2 filed on the FBI's IC3 system.

50. VICTIM 2 described similar interaction with a potential buyer identifying himself as "Fan YANG," who also was a potential home buyer with a price range of $3 million, and provided the following information about the scam.

51. VICTIM 2 was also contacted by "YANG" using Whatsapp, from phone number (626) 566-8010.

52. VICTIM 2 received both text and phone calls from "YANG" who VICTIM 2 described as having an "Asian" accent.

53. "YANG" also provided the email address of zbud66888@gmail.com for sending and receiving documents related to the purchase of real estate.

54. "YANG" coached VICTIM 2 on how to invest money through the use of a cryptocurrency trading platform called Stormgain.

55. "YANG" provided VICTIM 2 with a link to download the Stormgain application.

56. At the direction of "Yang," VICTIM 2 downloaded the application and subsequently linked VICTIM 2's Coinbase wallet to a smart contract.

57. USSS investigators believe this smart contract likely gave orchestrators of this scheme backdoor access to VICTIM 2's cryptocurrency account.

58. In order to deceive VICTIM 2 into investing, "YANG" provided a JP Morgan Chase Bank statement dated in November 2022 showing a balance in excess of $10 million and sent VICTIM 2 a United States Permanent Resident card and images of airline tickets for travel to North Carolina to see properties for the real estate purchase.

59. VICTIM 2 stated that when "YANG" did not show up to meet regarding the real estate properties, VICTIM 2 contacted "YANG," who stated the reason was due to a sick family member.

60. VICTIM 2 suspected fraud and attempted to withdraw the funds from Stormgain, but was met with resistance and attempts from "administrators" to persuade VICTIM 2 to transfer more funds in the amount of approximately $50,000 in order to expediate the withdrawal.

61. At the conclusion of the interview, VICTIM 2 agreed to download VICTIM 2's cryptocurrency transactions and provided them to the USSS for tracing.

62. VICTIM 2 stated these communications and events occurred in early 2023.

63. On or about April 12, 2023, VICTIM 2 sent the downloaded transaction history to the USSS for investigative tracing.

64. Investigative tracing resulted in the discovery of five Binance deposit addresses of unknown account holders that received VICTIM 2's funds.

65. A review of the download revealed that on or about March 7, 2023 and continuing until approximately on or about April 8, 2023, VICTIM 2 conducted seven wire transfers from VICTIM 2's cryptocurrency account to the fake Stormgain cryptocurrency trading application representing an approximate total loss of $216,300.

66. On or about April 13, 2023, VICTIM 2 sent the downloaded text messaging history VICTIM 2 had with "YANG" along with screenshots from VICTIM 2's cellphone to the USSS.

67. The screenshots contain images of trades on the Stormgain application, a picture of a female Asian in a hospital bed, and a United States Permanent Resident identification card displaying the name Fan YANG with a country of birth as People's Republic of China, listing a date of birth.

68. A review of the text messaging history between "YANG" and VICTIM 2 reveal tactics used in "Pig Butchering" schemes.

69. "YANG" convinced VICTIM 2 to invest large sums of money into cryptocurrency (USDT) through the use of a downloaded trading platform named "Stormgain."

70. "YANG" made statements to VICTIM 2 about unrealistic gains and returns on the investments.

71. However, once VICTIM 2 became suspicious and attempted to withdraw funds, VICTIM 2's account on the Stormgain application was locked.

72. VICTIM 2 attempted to contact customer service via chat message through the Stormgain application.

73. VICTIM 2 was repeatedly requested by Stormgain to deposit more funds in order to "protect their identity and risk guarantee the funds."

74. VICTIM 2 continued text communications with "YANG" attempting to unlock the account and withdraw funds.

75. "YANG" continued to reassure VICTIM 2 and encourage VICTIM 2 to just follow the instructions from customer service and transfer additional funds into the Stormgain application.

76. The link to Stormgain VICTIM 2 received from "YANG" is identified as "stormgainali.com."

77. The authentic Stormgain application is located at website https://stormgain.com.

78. Investigative research of the spoofed Stormgain website (stormgainali.com) revealed it was created on February 26, 2023, and the register is PDR LTD (publicdomainregistry.com), registrant name is ali ali, and registrant country is Hong Kong, China.

79. The server that the spoofed domain is hosted on contains 31 other websites, and 13 of those sites are some variation of "stormgain.com."

80. As a result, investigators do not believe the legitimate Stormgain company was involved in this online scam, but rather that criminals impersonated this company in order to steal cryptocurrency from unsuspecting victims.

81. The USSS ran database checks on the information from the USA permanent resident card, which revealed there was no Fan YANG with the listed date of birth provided to VICTIM 2 through the identification document(s).

82. The U.S. Customs and Border Protection ("CBP") confirmed the USA permanent resident card provided to VICTIM 2 by "YANG" was counterfeit.

83. Information from JP Morgan Chase ("JPMC") bank confirmed that the JPMC bank statement "YANG" provided to VICTIM 2 was fraudulent.

Additional Stormgain Complaints

84. A query of the FBI's IC3 website using the search parameters of "Stormgain" revealed four additional complaints filed between on or about March 9, 2023 and on or about April 4, 2023.

85. Each of these complaints have similar commonalities in that all four complaints are real estate agents, who were contacted by purported real estate buyers in the market for multiple million dollar properties, and communication was via WhatsApp, which led to the introduction of "Stormgain" cryptocurrency trading platform.

86. Each complainant received similar claims of investing opportunities with high yields.

87. However, upon attempted withdrawals, the "Stormgain" accounts became inaccessible, and complainants were given similar reasons and encouraged to make additional deposits to receive their funds sooner.

88. The combined total reported loss suffered by the four complaints was approximately $585,764.

89. Based on the different names and contact information used in the course of several similar deception schemes, and the complex and geographically distributed nature of the criminal activity, it is believed these criminal acts resulted from an organized conspiracy.

90. Additionally, WhatsApp, email, internet website, cryptocurrency, and mobile application communications and other transactions all caused interstate wires, particularly involving the Southern District of Georgia regarding VICTIM 1, who was located in the Southern District of Georgia at the time of the communications and resulting fraud.

91. For example, WhatsApp communications to and from Victim 1 in the Southern District of Georgia caused interstate wires between the state of Georgia and locations outside the state of Georgia.

Money Laundering and Money Laundering Conspiracy

92. For each of VICTIM 2's transactions, VICTIM 2's funds were traced on the publicly available blockchain through a series of transfers between addresses,

known as hops, prior to their arrival at **Subject Account A** and **Subject Account B**.

93. The USSS traced the flow of funds and identified numerous unique cryptocurrency addresses involved in the movement of VICTIM 2's funds following their transfer from VICTIM 2's cryptocurrency account.

94. While all victims' funds were withdrawn from VICTIM 2's cryptocurrency account as USDT, some of the criminal proceeds were converted to DAI (another cryptocurrency) and later back to USDT prior to reaching **Subject Account B**.

95. This type of behavior is a mechanism to evade law enforcement by "layering" the proceeds of criminal activity, all in an effort to conceal and disguise the nature, location, source, ownership, and/or control of those proceeds of the specified unlawful activity, in this case, wire fraud and wire fraud conspiracy.

96. The USSS reviewed records for three exchange accounts in receipt of VICTIM 2's funds and found that they were primarily established by individuals from east Asian or southeast Asian countries, which is consistent with Pig Butchering schemes.

97. Additional indications of these accounts' involvement in Pig Butchering schemes, or the laundering of funds from Pig Butchering and other schemes, included each account's unique behaviors and characteristics.

98. For instance, the accounts displayed a history of frequent, large dollar transactions, followed by a pattern of rapid movement of funds with large corresponding withdrawals.

99. Despite the short duration of their existence, **Subject Account A** received more than $108,000,000 worth of cryptocurrency in approximately six months, and **Subject Account B** received more than $9,500,000 worth of cryptocurrency in approximately three months.

100. The amount of cryptocurrency processed through **Subject Account A** and **Subject Account B** in less than six months of over $115 million, along with other facts set forth herein, is indicative of the use of these accounts for money laundering purposes.

101. During the course of the funds tracing and analysis, the USSS analyzed the USDT wallet addresses used in the various hops between the victim transactions to **Subject Account A** and **Subject Account B**, and observed an apparent pattern where individuals reported falling victim to Pig Butchering scams, among other scams.

102. In these instances, the USSS located approximately 48 victim complaints on either the FBI's IC3 or the Federal Trade Commission's ("FTC") Consumer Sentinel database, which databases log online scams reported by victims.

Subject Account A

103. On or about March 21, 2023, VICTIM 2 transferred approximately 24,463.49 USDT on the Ethereum blockchain to an Ethereum address as part of the investment scheme.

104. Between on or about March 21, 2023 and on or about March 22, 2023, the victim funds continued to be laundered through nine additional hops on the Ethereum blockchain before arriving at **Subject Account A**.

105. It should be noted that approximately six of these hops formed a circular flow of funds.

106. Money launderers often conduct otherwise unnecessary transactions in the transfer of funds to conceal and disguise the nature, location, source, ownership, and/or control of those criminal proceeds.

107. The number of hops in this transaction is a strong indication that the movement of funds was performed in a manner meant to conceal and disguise the nature, location, source, ownership, and/or control of those proceeds of a specified unlawful activity, to wit, wire fraud and wire fraud conspiracy.

108. As illustrated in the chart attached as Exhibit 1, which is incorporated by reference herein, VICTIM 2's funds were traced through approximately 10 hops before arriving at **Subject Account A**.

109. The USSS performed analyses on each of the hops identified in this movement of funds and repeatedly located reports of additional fraud in transactions involving the addresses through which VICTIM 2's funds hopped.

110. For example, a USDT address starting with 0x370d22d2 was found to have interacted with addresses where, between five and six hops earlier, 17 individuals reported being victims to the FBI's IC3 or the FTC's Consumer Sentinel system. A review of these complaints indicated that the victims were part of fraud schemes that ranged from Pig Butchering to likely Pig Butchering.[4]

111. An analysis of Binance information for **Subject Account A** revealed multiple indications of money laundering activity.

112. Records received from Binance indicate that **Subject Account A** was used for money movement service activities, that included sharing credentials or disguising geolocation to avoid compliance flags.

113. Records show that the account holder had a Thailand based registration phone number. However, logins showed that the account holder was logging in from different geographical locations, including Thailand, United States, and Singapore.

114. In several instances, it would be highly unlikely for the account holder to be in these different geographic locations within the given time frames.

115. This indicates that the subject is either engaging in account sharing or disguising their true IP address using virtual private network(s) (VPNs), both of which are consistent with money laundering activity.

[4] References to "likely pig butchering" refer to schemes that, as described by victims, have the hallmarks of a typical pig butchering scheme, but may not have been specifically labeled that way or included enough detail for investigators to definitively confirm the nature of the scheme. For example, some may not have indicated that they initially encountered their scammer via a dating website or other online platform, something which is known, based on USSS's training and experience, that victims are often embarrassed to disclose. All of the scams labeled "likely pig butchering" nevertheless involved the solicitation of fraudulent investments.

Subject Account B

116. On or about April 4, 2023, VICTIM 2 transferred approximately 41,212.23 USDT on the Ethereum blockchain to an Ethereum address as part of the investment scheme.

117. Between on or about April 4, 2023 and on or about April 11, 2023, the victim funds continued to be laundered through 12 additional hops on the Ethereum blockchain before arriving at **Subject Account B**.

118. The number of hops in this transaction is a strong indication that the movement of funds was performed in a manner meant to conceal and disguise the nature, location, source, ownership, and/or control of those proceeds of a specified unlawful activity, to wit, wire fraud and wire fraud conspiracy.

119. An analysis of the Binance information for **Subject Account B** revealed multiple indications of money laundering activity.

120. This activity includes numerous hops employed to layer proceeds of crime, and rapid suspicious transactions that make it difficult for law enforcement to capture the funds for asset forfeiture purposes.

121. Prior to the criminal proceeds reaching **Subject Account B**, the victim funds were swapped to a different type of cryptocurrency using decentralized exchanges on two separate occasions, likely as a method of confusing and evading law enforcement.

122. As illustrated in the chart attached as Exhibit 2, which is incorporated by reference herein, VICTIM 2's funds were traced through 13 hops before arriving at **Subject Account B**.

123. The USSS performed the same type of analyses on each of the hops as explained above.

124. The USSS located 31 reports of additional fraud in transactions involving the addresses through which VICTIM 2's funds hopped.

125. For example, the USDT address associated with **Subject Account B** was found to have interacted with addresses where, six hops earlier, 26 individuals reported being victims to the FBI's IC3 or the FTC's Consumer Sentinel system.

126. A review of these complaints indicated that the victims were part of fraud schemes that ranged from Pig Butchering to likely Pig Butchering.

Summary

127. As a result of the facts set forth herein, the **Defendant Property** constitutes proceeds of wire fraud and wire fraud conspiracy, as well as property involved in and traceable to property involved in money laundering and money laundering conspiracy, and is therefore subject to forfeiture.

128. Transactions and attempted transactions involving the **Defendant Property**, and property traceable to such property, included monetary transactions of over $10,000 in criminally derived property and which were derived from specified unlawful activity, to wit, wire fraud and wire fraud conspiracy.

129. Cryptocurrency in **Subject Account A** and **Subject Account B**, including the **Defendant Property** and property traceable thereto, was used to conceal and disguise the nature, location, source, ownership, and/or control of those proceeds of the specified unlawful activity, in this case, wire fraud and wire fraud conspiracy.

130. This criminal scheme involved the use of interstate and foreign wires and impacted interstate and foreign commerce.

CLAIMS FOR RELIEF

First Claim for Relief
(Forfeiture Pursuant to 18 U.S.C. § 981(a)(1)(C))

131. The United States incorporates by reference the allegations contained in paragraphs 1 through 130 above as if set forth fully herein.

132. The **Defendant Property** is property that constitutes and/or is derived from proceeds traceable to one or more violation and/or attempted violation of 18 U.S.C. §§ 1343 and 1349.

133. The **Defendant Property** is therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

Second Claim for Relief
(Forfeiture Pursuant to 18 U.S.C. § 981(a)(1)(C))

134. The United States incorporates by reference the allegations contained in paragraphs 1 through 130 above as if set forth fully herein.

135. The **Defendant Property** is property that constitutes and/or is derived from proceeds traceable to one or more violation of 18 U.S.C. § 1349, which is a conspiracy to violate 18 U.S.C. § 1343.

136. The Defendant Property is therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

Third Claim for Relief
(Forfeiture Pursuant to 18 U.S.C. § 981(a)(1)(A))

137. The United States incorporates by reference the allegations contained in paragraphs 1 through 130 above as if set forth fully herein.

138. The **Defendant Property** is property that was involved in a transaction or attempted transaction, or is property traceable to such property, in violation of 18 U.S.C. §§ 1956 and/or 1957.

139. The Defendant Property is therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

Fourth Claim for Relief
(Forfeiture Pursuant to 18 U.S.C. § 981(a)(1)(A))

140. The United States incorporates by reference the allegations contained in paragraphs 1 through 130 above as if set forth fully herein.

141. The **Defendant Property** is property that was involved in, or traceable to such property, a conspiracy to commit a violation of 18 U.S.C. §§ 1956 and/or 1957, in violation of 18 U.S.C. § 1956(h).

142. The Defendant Property is therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

CONCLUSION

143. WHEREFORE, the United States of America prays that:

a. Process of a Warrant for Arrest and Notice *In Rem* be issued for the arrest of the **Defendant Property**;

b. The **Defendant Property** be forfeited and condemned to the use and benefit of the United States;

c. The United States be awarded its costs and disbursements in this action and for such other and further relief as this Court deems just and proper; and

d. That due notice be given to all parties to appear and show cause why the forfeiture of the **Defendant Property** should not be decreed.

Respectfully submitted,

JILL E. STEINBERG
UNITED STATES ATTORNEY

By: */s/ J. Bishop Ravenel*
J. Bishop Ravenel
Assistant United States Attorney
Virginia Bar Number 70250
P.O. Box 8970
Savannah, GA 31412
(912) 652-4422

VERIFICATION OF COMPLAINT FOR FORFEITURE *IN REM*

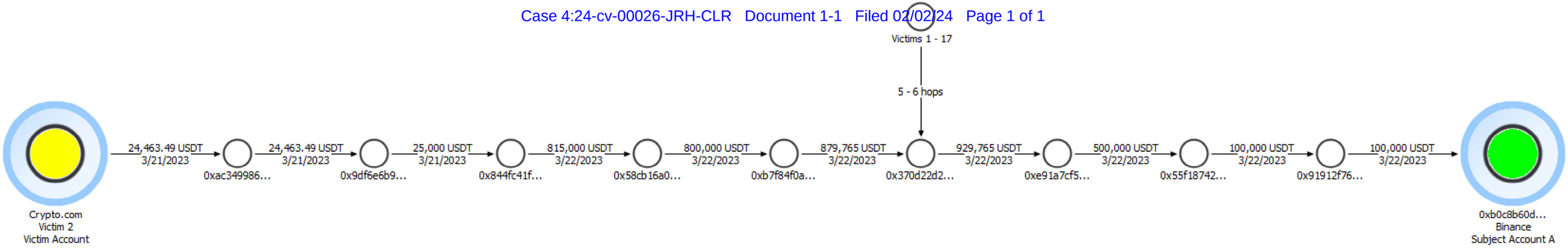
I, Special Agent J. Craig Reno, have read the foregoing Complaint for Forfeiture *In Rem* in this action and state that its contents are true and correct to the best of my knowledge and belief.

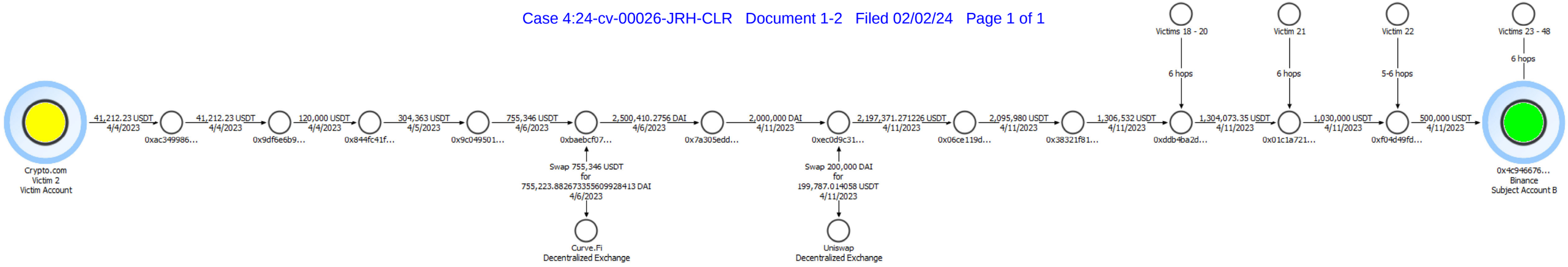
Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

This 1st day of February 2024.

J. Craig Reno

J. Craig Reno
Resident Agent in Charge
United States Secret Service


Victims 1 - 17
5 - 6 hops
Crypto.com
Victim 2
Victim Account
24,463.49 USDT
3/21/2023
0xac349986...
24,463.49 USDT
3/21/2023
0x9df6e6b9...
25,000 USDT
3/21/2023
0x844fc41f...
815,000 USDT
3/22/2023
0x58cb16a0...
800,000 USDT
3/22/2023
0xb7f84f0a...
879,765 USDT
3/22/2023
0x370d22d2...
929,765 USDT
3/22/2023
0xe91a7cf5...
500,000 USDT
3/22/2023
0x55f18742...
100,000 USDT
3/22/2023
0x91912f76...
100,000 USDT
3/22/2023
0xb0c8b60d...
Binance
Subject Account A


Crypto.com
Victim 2
Victim Account
41,212.23 USDT
4/4/2023
0xac349986...
41,212.23 USDT
4/4/2023
0x9df6e6b9...
120,000 USDT
4/4/2023
0x844fc41f...
304,363 USDT
4/5/2023
0x9c049501...
755,346 USDT
4/6/2023
0xbaebcf07...
Swap 755,346 USDT
for
755,223.88267335560928413 DAI
4/6/2023
Curve.Fi
Decentralized Exchange
2,500,410.2756 DAI
4/6/2023
0x7a305edd...
2,000,000 DAI
4/11/2023
0xec0d9c31...
Swap 200,000 DAI
for
199,787.014058 USDT
4/11/2023
Uniswap
Decentralized Exchange
2,197,371.271226 USDT
4/11/2023
0x06ce119d...
2,095,980 USDT
4/11/2023
0x38321f81...
1,306,532 USDT
4/11/2023
Victims 18 - 20
6 hops
0xddb4ba2d...
1,304,073.35 USDT
4/11/2023
Victim 21
6 hops
0x01c1a721...
1,030,000 USDT
4/11/2023
Victim 22
5-6 hops
0xf04d49fd...
500,000 USDT
4/11/2023
Victims 23 - 48
6 hops
0x4c946676...
Binance
Subject Account B