ISMAIL J. RAMSEY (CABN 189820)
United States Attorney

THOMAS A. COLTHURST (CABN 99493)
Chief, Criminal Division

GALEN A. PHILLIPS (CABN 307644)
CHRIS KALTSAS (NYBN 5460902)
Assistant United States Attorneys

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7200
Facsimile: (415) 436-7234
Email: galen.phillips@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 110607.71 TETHER (USDT), Defendant.	CASE NO. **VERIFIED COMPLAINT FOR CIVIL FORFEITURE *IN REM***

The United States of America, by its attorneys, Ismail J. Ramsey, United States Attorney, and Galen A. Phillips and Chris Kaltsas, Assistant United States Attorneys for the Northern District of California, brings this complaint and alleges as follows:

NATURE OF THE ACTION

1. This is a judicial forfeiture action *in rem*, as authorized by Title 18, United States Code, Sections 981 and 983.

2. This Court has jurisdiction under Title 18, United States Code, Section 981; and Title 28, United States Code, Sections 1345 and 1355, as the defendant property constitutes or is derived from

proceeds obtained, directly or indirectly, from, or property "involved in," violations of Title 18, United States Code, Sections 1343 and 1956.

3. This action is timely filed in accordance with Title 18, United States Code, Section 983.

4. Venue is proper because the defendant property represents the proceeds of a crime that may be prosecuted in the Northern District of California. 28 U.S.C. §§ 1355, 1395.

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

PARTIES

6. Plaintiff is the United States of America.

7. The Defendant Property includes approximately 110607.71 Tether[1] (USDT) (the "Defendant Property") held in a Binance account (the "Subject Account") associated with a deposit address 0xdddb12c230a3c51c0d17e50ec2abf7474a3f500b (the "0xdd Address").

FACTS

8. As detailed below, this case concerns the forfeiture of 110607.71 USDT seized from a cryptocurrency account used to launder fraud proceeds. Law enforcement discovered the account after tracing a portion of an elderly victim's funds across the blockchain to the 0xdd Address. An investigation of the account revealed that it is part of an ecosystem of fraud that has impacted numerous victims with established losses in aggregate of $1 million. Within eight months of the Subject Account's opening in September 2022, the account had received nearly $18 million in cryptocurrency deposits, though the accountholder has never deposited or withdrawn fiat money from the account.

A. <u>The XTRA Investment Scam</u>

9. In early February 2023, RB,[2] a 68-year-old resident of Santa Clara, California, connected with an individual identifying themselves as "Janey Lee" (LEE) over text message. At the time, RB was recently divorced and facing financial troubles.

10. LEE texted RB first. And, after a few messages, LEE claimed to have the wrong number. Still, her conversation with RB persisted, though it moved to WhatsApp and later to Telegram.

[1] Tether is a stablecoin. Its value is pegged to the value of the U.S. dollar.

[2] Victim names have been anonymized for their privacy.

11. RB and LEE discussed personal information: their backgrounds, relationship statuses, businesses, and finances. Within weeks, this budding relationship became romantic in nature, with LEE repeatedly messaging RB about their future together.

12. LEE's passion was not limited to RB, however. LEE also peppered their conversations with apparent non sequiturs concerning cryptocurrency futures. LEE claimed to work in Houston, Texas at a clothing design company. LEE had apparently also become successful as a cryptocurrency trader. LEE sent RB screenshots of her purported earnings. LEE also offered to help RB invest in cryptocurrency.

13. In March 2023, LEE introduced RB to a company called "XTRA," an alleged cryptocurrency trading platform. LEE directed RB to create an XTRA account on its website "xrahp.cc."

14. XTRA had the hallmarks of a legitimate cryptocurrency trading platform. Its website featured account numbers, cryptocurrency-wallet addresses, investment amounts and gains, and apparent deposit and withdrawal functions. Its graphics and layouts were consistent with most extant smartphone currency trading websites.

15. LEE also directed RB to create a Crypto.com account to buy and send cryptocurrency to his XTRA account. Specifically, LEE instructed RB to purchase USDC[3] and ETH[4] from Crypto.com to invest in XTRA.

16. On March 7, 2023, RB made his initial investment into XTRA, with a transfer of approximately 300 USDC from RB's Crypto.com account to a purported XTRA deposit address. Following the initial investment, RB was able to view his fictitious "earnings" on the XTRA website, which reported a 20–30 percent gain against his initial investment.

17. RB's purported gains and LEE's continued encouragement were enough to convince RB to invest approximately $260,000.00 in USDC and ETH into the XTRA platform between March 2023 and April 2023, as detailed in the table on the following page.

//

//

[3] USDC is a stablecoin. Its value is pegged to the value of the U.S. dollar.

[4] ETH refers to ether, the cryptocurrency native to the Ethereum blockchain.

Date	Receiving Address	Amount	Asset
3/7/2023	0xe45D1C9d4C90fc451d09990df6052cb6676BaC45	290	USDC
3/20/2023	0xe45D1C9d4C90fc451d09990df6052cb6676BaC45	10,744.3	USDC
3/29/2023	0xb6660743f56C014C430d5efFe191f1b35E79D9cA	9,845	USDC
4/9/2023	0x0951F8fb9E89c1F1E1a1e928cCc9Bb34EB5d07DB	36,460	USDC
4/20/2023	0x0951F8fb9E89c1F1E1a1e928cCc9Bb34EB5d07DB	49,990	USDC
4/21/2023	0x0951F8fb9E89c1F1E1a1e928cCc9Bb34EB5d07DB	49,990	USDC
4/22/2023	0x0951F8fb9E89c1F1E1a1e928cCc9Bb34EB5d07DB	53.496	ETH
4/22/2023	0x0951F8fb9E89c1F1E1a1e928cCc9Bb34EB5d07DB	1,943.23	USDC
Total Value (USD)		**$259,538.64**	

18. By the end of April 2023, RB's XTRA account showed a value of approximately 487,327.775 USDC—representing a gain exceeding 80 percent of his investment in less than a month.

19. On or about April 25, 2023, RB tried to withdraw 100,743.23 USDC from his XTRA account. Instead of receiving his withdrawal, RB received a message from XTRA customer service saying that by May 2, 2023, in order to verify his account, RB needed to send his XTRA account an additional amount worth approximately 20 percent of his account balance.

20. At this point RB filed a complaint with IC3, a division of the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity.

B. Laundering RB's Funds to the Subject Account

21. RB's April 21, 2023, deposit passed through a series of transfers between cryptocurrency addresses, known as hops, to their arrival at the Subject Account.

22. In traveling to the Subject Account, RB's funds were swapped to USDT. Swaps of this sort are often conducted with no legitimate business purpose and are intended to obfuscate the nature, source, ownership, control, and/or sources of funds—that is, these swaps are often done to launder victim funds.

//

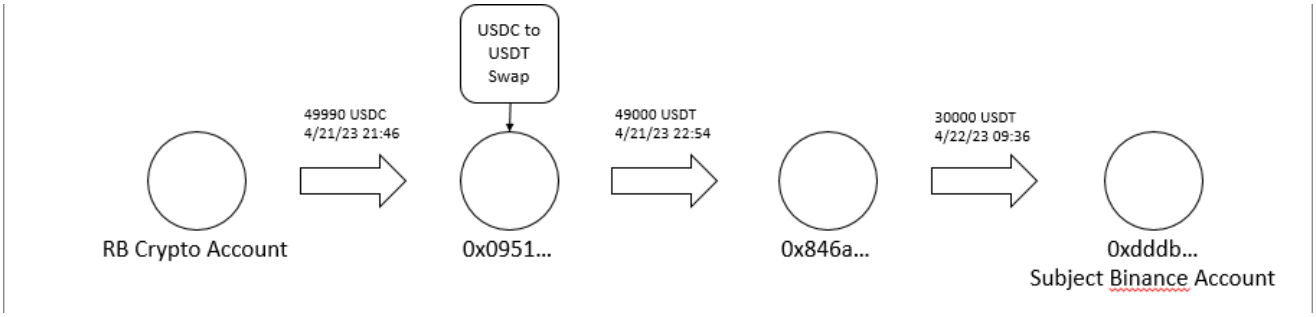
//

//

//

//

23. The cryptocurrency tracing of RB's April 21, 2023, deposit revealed the following transaction path leading to the Subject Account:



24. Using a "lowest intermediate balance" (LIBR) tracing methodology in which the stolen cryptocurrency is transferred from an address after all other untraceable cryptocurrency is spent, each of these transfers (meaning the initial transfer to the 0x0951 address; the subsequent transfer to the 0x846a address; and the final transfer to the Subject Account) contained funds traceable to RB's initial deposit of 49,990 USDC. Thus, based on LIBR, 30,000 USDT that was deposited into the Subject Account could be traced back to RB's original transaction, though that amount was ultimately withdrawn from the Subject Account before the government seized the Defendant Property.

25. Binance records show that, between September 16, 2022, and May 23, 2023, the Subject Account received nearly $18 million in cryptocurrency deposits. At no point in the Subject Account's history did the accountholder deposit or withdraw fiat currency, which is usually how users acquire cryptocurrency.

C. Additional Victims Are Linked to the XTRA Scam and Accounts in the Subject Account's Ecosystem

a. Multiple Victims Have Reported the XTRA Scam

26. Law enforcement has determined that three other victims collectively reported losses of approximately $550,000.00 from the XTRA scam. Those victims, whose losses are reported in the below table, each reported their dealings with XTRA in complaints they filed with IC3.

//

//

//

Affidavit Name	City/State/Country	Loss
Victim 1	El Paso, TX	$20,000
Victim 2	Plantation, FL	$30,000.00
Victim 3	Fort Worth, TX	$500,000.00
Total		**$550,000.00**

b. Victims of Other Scams Have Had Funds Laundered Through Addresses Connected to the Subject Account

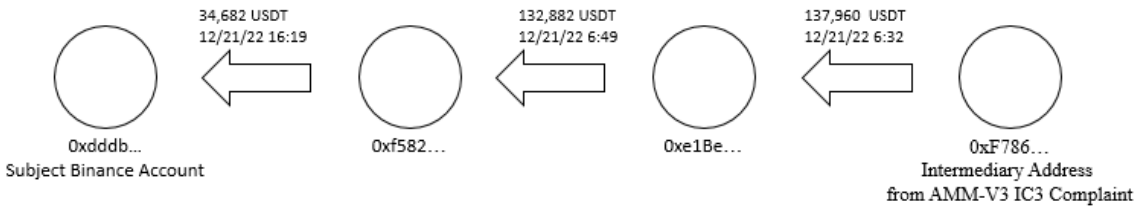
27. A victim of another Pig Butchering scam reported to IC3 lost $600,000 through a series of hops that passed through an address connected to the Subject Account. Indeed, some of this victim's funds passed through wallet address 0xF7862160e8BfAd48a39a6e7e37fb297D42D17fAc (0xF786). 0xF786 has exposure to the Subject Account.

28. The first significant deposit into the Subject Account from the Ethereum Blockchain occurred on December 21, 2022 and consisting of 34,682 USDT from wallet address 0xf5820Bf581A14CBD62Ee97d406Ee05F454f6d46f (0xf582). This deposit was the first withdrawal in 0xf582's transaction history.

29. The only transaction before this withdrawal in 0xf582's transaction history was a 132,882 USDT deposit from 0xe1Befb7cb6B17AEF4FbcF4f1f7ef887Ece2a8738 (0xe1Be), which was the first withdrawal in 0xe1Be's transaction history.

30. The only transaction before this withdrawal in 0xe1Be's transaction history was a 137,960 USDT deposit from 0xF786.

31. In short, the Subject Account received funds from a totally separate account that is also linked to a separate report of a Pig Butchering scam. See the below graph for the flow of funds:



32. Finally, three additional victims who submitted complaints to IC3 identified in their complaints wallet addresses that also have exposure to the Subject Account. Indeed, the Subject Account received approximately 20,000 USDT from 0x2719c08abcad395b19d8465aec85243ff031e3b6 (0x2719). 0x2719 received funds from a victim who submitted an IC3 report in November 2022. And, in addition, 0x2719's first USDT deposit was received from 0x2733Bc02369586dA42f79B4766099CA7B926ae51 (0x2733), which is an address listed in an additional two IC3 complaints by victims.

COUNT ONE

Civil Forfeiture (Title 18, United States Code, Section 981(a)(1)(C)) for Wire Fraud (Title 18, United States Code, Section 1343)

33. Civil forfeiture of the proceeds of wire fraud is authorized by Title 18, United States Code, Section 981(a)(1)(C). Specifically, Section 981(a)(1)(C) authorizes forfeiture of "any property, real or personal, which constitutes or is derived from proceeds traceable to . . . any offense constituting 'specified unlawful activity' (as defined in section 1956(c)(7) of this title), or a conspiracy to commit such offense." Section 1956(c)(7)(A) defines the term "specified unlawful activity" as including "any act or activity constituting an offense listed in section 1961(1) of this title." And Title 18, United States Code, Section 1961(1), in turn, includes violations of Title 18, United States Code, Section 1343 in its definition of racketeering activity.

34. The Defendant Property constitutes, and is derived from, the proceeds of wire fraud, and is thus subject to forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C).

COUNT TWO

Civil Forfeiture (Title 18, United States Code, Section 981(a)(1)(A)) for Money Laundering (Title 18, United States Code, Section 1956(a)(1)(B)(i))

35. Civil forfeiture of property involved in a money laundering transaction, or property traceable to such property, is authorized by Title 18, United States Code, Section 981(a)(1)(A), which allows the United States to forfeit "any property, real or personal, involved in a transaction . . . in violation of section 1956 . . . of this title, or any property traceable to such property."

36. A violation of Title 18, United States Code, Section 1956(a)(1)(B)(i) occurs when a person conducts or attempts to conduct a financial transaction knowing that the transaction involves the proceeds of a specified unlawful activity when the transaction is designed in whole or part "to conceal or disguise the nature, the location, the source, the ownership or the control of the proceeds of the specified unlawful activity; or . . . to avoid a transaction reporting requirement under State or Federal law", or involves property "traceable to such property."

37. Wire fraud is a specified unlawful activity pursuant to Title 18, United States Code, Sections 1956(c)(7)(A) and 1961(1). Thus, the Defendant Property is subject to forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(A) because it was involved in, or is traceable to property involved in, money laundering transactions in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

PRAYER FOR RELIEF

38. The United States requests that due process issue to enforce the forfeiture of the above listed Defendant Property; that notice be given to all interested parties to appear and show cause why forfeiture should not be decreed; that the Court enter a judgment forfeiting the Defendant Property; and that the United States be awarded such other relief as may be proper and just.

DATED: November 13, 2023

Respectfully submitted,

ISMAIL J. RAMSEY
United States Attorney

/s/
GALEN A. PHILLIPS
CHRIS KALTSAS
Assistant United States Attorneys

VERIFICATION

I, Trevor Brady, state as follows:

1. I am a Special Agent with the United States Federal Bureau of Investigation. I am an agent assigned to this case. As such, I am familiar with the facts and the investigation leading to the filing of this Complaint.

2. I have read the Complaint and affirm that the allegations contained therein are true.

* * *

I declare under penalty of perjury that the foregoing is true and correct. Executed this 9th day of November, 2023.

Trevor Brady
Special Agent
United States Federal Bureau of Investigation