CRAIG H. MISSAKIAN (CABN 125202)
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

THOMAS HARLESS
Law Clerk

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. 782,219.16107 TETHER WITH A TOTAL ESTIMATED VALUE OF $782,372.48 U.S. DOLLARS (USD) 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 28 U.S.C. § 2461(c) involving the seizure of the following property:

a. 782,219.16107 Tether ("USDT") with a total estimated value of $782,372.48 U.S. Dollars (USD)[1]

(hereinafter, collectively, the "Defendant Property"), as property constituting, or derived from,

[1] Estimated with online public sources on May 22, 2025.

any proceeds of Title 18 U.S.C. §§ 1343 (wire fraud), as well as 1956 and 1957 (money laundering) (hereafter the "Subject Offenses"), 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 was located, and the 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 782,219.16107 USDT with a total estimated value of $782,372.48 USD, which was seized from two separate Tether wallet addresses by law enforcement agents, pursuant to a federal seizure warrant: 259,012.134673 USDT seized from the cryptocurrency address 0x709e7f7f612a99FEBd9b1243E6D61d4EB9257D26 (hereinafter, "Target Address 1"), and 523,207.026397 USDT seized from the cryptocurrency address 0x619148e5753072907bECa86c932172ffbcBBD3fa (hereinafter, "Target Address 2").

BACKGROUND ON VIRTUAL CURRENCY

6. Virtual assets, also known as cryptocurrency, are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual assets 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 asset addresses are the particular virtual locations to which such currencies are sent and received. A virtual asset address is analogous to a bank account number and is represented as a string of alphanumeric characters.

8. Each virtual asset address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Users can operate multiple

addresses at any given time, with the possibility of using a unique address for every transaction. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address. 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.

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

10. Many virtual assets 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 asset address that ever received that virtual asset. It also maintains records of every transaction and all the known balances for each virtual asset address. There are different blockchains for different types of virtual assets. Some virtual assets are permissible across multiple blockchains.

11. Stablecoins are a type of virtual asset whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual asset. For example, USDC is a stablecoin pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

12. Tether ("USDT") is a type of stablecoin issued by Tether Limited. Tether Limited ("Tether") is a company that manages the smart contracts and the treasury (i.e., the funds held in reserve) for USDT tokens. USD Coin ("USDC") is another type of cryptocurrency known as a stablecoin. USDC is issued by Circle, a company based in Boston, Massachusetts.

BACKGROUND ON "PIG BUTCHERING" AND ROMANCE FRAUD SCAMS

13. "Pig Butchering" is a complex form of financial fraud, which combines elements of online "romance scams" with sophisticated software applications that imitate online investment platforms. In a romance scam the perpetrator contacts the victim via telephone or an online messaging platform and,

while using a fraudulent identity, develops a romantic relationship with the victim to build trust. Once a romantic connection is established, the perpetrator then leverages the victim's affection and sense of trust to manipulate and/or defraud the victim. Most often these frauds involve cryptocurrency rather than traditional forms of fiat currency.

14. Pig Butchering schemes often begin with a scammer sending a victim a social media/dating website connection, or through a seemingly misdialed text, sometimes via WeChat or WhatsApp. From there, the scammer establishes a more personal relationship with the victim using manipulative tactics similar to those used in online romance scams to gain the victim's affection and trust. Pig Butchering schemes frequently originate in various locations throughout Southeast Asia, including, but not limited to, Hong Kong, Myanmar, Cambodia, Malaysia, Thailand, and Singapore.

15. Soon after establishing the romantic connection, the scammer concocts a reason why the victim should send them cryptocurrency. In many cases the scammer suggests to the victim that they should invest in cryptocurrency by touting their own, or an associate's, success in the field.

16. In the investment scam method, often the scammer directs a victim to a fake investment platform hosted on a website. These websites and the associated investment platforms are created by scammers to mimic legitimate platforms. The scammer may assist the victim with opening a cryptocurrency account on a reputable exchange, such as Coinbase, Kraken, Binance, OKX, and others, and will instruct the victim on how to transfer money from their bank account to that new account. Next, the victim will receive instructions on how to convert their money into cryptocurrency and transfer the cryptocurrency to the fake investment platform. On its surface, the platform portrays lucrative returns on the victim's investment, encouraging further investment; underneath, all deposited funds are routed to a wallet address controlled by the scammers. Some victims are even allowed to withdraw a small amount of their apparent profits to establish the "legitimacy" of the fraudulent cryptocurrency platforms and encourage them to invest larger amounts of funds.

17. When victims attempt to withdraw the majority of their funds, they are unable to do so and are provided various excuses as to why. For example, scammers will often levy a fake "tax" requirement, stating taxes must be paid on the proceeds generated from the platform before those proceeds may be withdrawn. This is often an eleventh-hour effort by subjects to elicit more money from victims. Ultimately,

victims are locked out of their accounts and lose all their funds in this manner.

FACTS

Overview

18. This investigation involves an individual referred to as VICTIM #1 (hereafter, the "victim"), whom law enforcement agents have interviewed. VICTIM #1 is a 59-year-old retiree that resided in Sausalito, California when the fraud described herein occurred.

19. Beginning in approximately July 2023 and ending on or about January 8, 2024, the victim was defrauded by a burgeoning fraud scheme known as "Pig Butchering", which resulted in a total loss of approximately $931,000 to the victim. As described above, Pig Butchering is a type of romance scam, or confidence scam, that convinces victims to send money to what they believe to be legitimate romantic partners. Romance scams target persons looking for romantic partners or friendships on dating websites and other social media platforms. As was the case here, the scammers typically 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 on behalf of the scammers. In this case and as explained in further detail below, efforts to defraud the victim became evident after the victim was convinced to send USDT (or "Tether") cryptocurrency from the cryptocurrency exchange Coinbase[2] to the Unknown Actor(s).

Description of the Wire Fraud Scheme by "HAUGHN"

20. In mid-2023 the victim met one or more individuals that purported to be "DAVID OSCAR LEWIS HAUGHN" (hereafter "HAUGHN") on the online dating website Match.com. HAUGHN initially presented himself as a real estate investor/developer residing in Sherman Oaks, California. Over the course of many months, HAUGHN led the victim to believe that he (HAUGHN) was a very wealthy individual from the United Kingdom, who was purportedly working as a diplomat

[2] Coinbase is a financial institution that is registered with FinCEN as a Money Services Business, and is required to comply with the Bank Secrecy Act. *See* Coinbase Help, *Coinbase Money Transmission and e-Money Regulatory Compliance*, https://help.coinbase.com/en/coinbase/privacy-and-security/other/coinbase-regulatory-compliance (last accessed June 4, 2025).

for the government of Sweden as a security operative. HAUGHN later gave the victim the impression that he was a spy.

21. HAUGHN and the victim communicated electronically via methods such as text message, the WhatsApp[3] messaging application, FaceTime[4], email, and on the Match.com dating website.

22. Figure 1 below shows a screenshot provided by the victim of HAUGHN's WhatsApp profile. A photo of HAUGHN is visible on the profile. Figure 2 is an image of HAUGHN that was provided by HAUGHN to the victim during the course of their relationship.

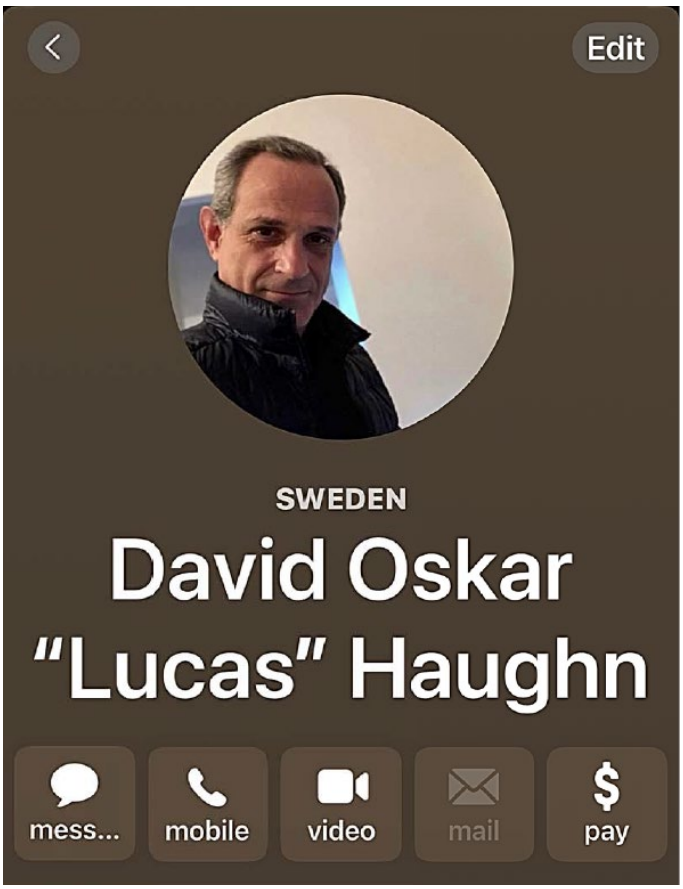

FIGURE 1: WHATSAPP PHOTO OF HAUGHN

[3] WhatsApp is an electronic messaging application for use on cellular phones that supports sending and receiving text, photos, videos, documents, locations, and voice calls.

[4] FaceTime is an application used to make video and audio calls from Apple iPhone and Apple iPad devices.

FIGURE 2: PHOTO OF HAUGHN PROVIDED TO THE VICTIM

23. Based on searches of the publicly available internet conducted by law enforcement, the individual portrayed in these photos did not appear to be HAUGHN, but rather Mr. Francesco Giro, an Italian politician. On September 10, 2024, law enforcement agents retrieved a photo from the Facebook profile for Francesco Giro[5], which appeared to be the exact same photograph of HAUGHN that HAUGHN had provided to the victim. Based on training and experience, law enforcement agents know that repurposing photos of a real person to make a fake online persona appear legitimate is a common technique used by perpetrators of romance scams. The investigating law enforcement agents therefore believed that photographs of Francesco Giro were taken from the open internet and used by the Unknown Actor(s) to develop a relationship with the victim as HAUGHN.

24. HAUGHN claimed to the victim that he worked at the Swedish Embassy in Los Angeles, California. The victim later learned that Sweden did not have an embassy in Los Angeles, but rather only a consulate. The victim further learned that the consulate was not fully functional and was mostly symbolic in nature. The victim thereafter contacted the Swedish consulate in Los Angeles, the Swedish

[5] Retrieved from Francesco Giro's Facebook profile (last accessed on September 10, 2024).

Embassy in Washington DC, and the Swedish government in Sweden, all of which claimed to not have any employees by the name "David Haughn". HAUGHN explained this to the victim by telling her that the Swedish government had to deny knowledge of him because he was a "security operative," and his position was "classified."

25. Between July 2023 and October 2023 HAUGHN continued to develop a relationship with the victim via messaging applications, phone calls, and video chats. By October of 2023 the victim believed that she was HAUGHN's fiancé. In October of 2023, HAUGHN further told the victim that he was selling his residence in Kensington, London with the intention of moving permanently to Sherman Oaks, California to be with the victim. HAUGHN also told the victim that he was going to sell a collection of jewels that he had amassed over his lifetime, valued at approximately £7 million. HAUGHN told the victim that he intended on having the jewels valued by an appraiser in the area of Frankfurt, Germany.

26. On October 4, 2023, HAUGHN called the victim and told her that while on the way to having the jewels valued in Germany he was detained by the German authorities. HAUGHN claimed to the victim that both the German and United States customs were demanding a percentage of the value of the jewels. Specifically, HAUGHN claimed to the victim that there was a fee of about $500,000, and that HAUGHN was able to retrieve only $100,000 from his own Barclays account. HAUGHN then told the victim that he needed her to send him $400,000 to cover the rest of the customs fees and taxes. Law enforcement agents know from their training and experience that United States customs would not be involved in Frankfurt for an individual traveling from the United Kingdom to Germany, and that this was likely a lie that HAUGHN told the victim as a part of HAUGHN's fraud scheme, to convince the victim to send HAUGHN money. Law enforcement agents also know from their training and experience that presenting a scenario where a loved one has been arrested or detained is a common tactic used by romance scam perpetrators to create a false sense of urgency and pressure for their victims.

27. HAUGHN then made a series of statements to the victim via wire that law enforcement agents believe were intended to defraud her of her funds. HAUGHN told the victim that discrepancies had arisen between the valuation of the jewels conducted by the German authorities and the value documented on his purported travel paperwork. HAUGHN further stated to the victim that the Germans were frustrated regarding this disparity and were irritated by HAUGHN's lack of awareness of customs duties. At one-point HAUGHN stated to the victim that the Germans were hostile towards him and abusive.

28. HAUGHN further told the victim that all his money was in a Chase bank account in the United States, and that he had attempted to transfer the required funds from this account, but that this action had triggered a fraud alert and a suspension of his account. HAUGHN told the victim that the only way for him to retrieve the funds was for him to walk into a Chase bank and wire the funds out, which he could not do because he was detained.

29. In response, the victim explained to HAUGHN that the only way that she could access the amount of money he purportedly needed would be to cash in her pension and retirement funds. It had taken the victim and her ex-husband over thirty years of work to accumulate these pensions and retirement funds. Included in the funds was money that her ex-husband had earned through military service, and money inherited from the victim's parents, who had also worked their entire lives to save these assets. The victim told HAUGHN that she did not want to access these funds because she was not yet 59 ½ years old, and therefore she would have to pay steep penalties and taxes if she were to withdraw these funds.

30. In response to this, HAUGHN told the victim that he felt that her cashing out her retirement funds was the only option they had. HAUGHN also claimed that his only family was his mother and his brother. HAUGHN stated to the victim that his mother had a heart condition and that his purported brother had borrowed approximately $500,000 from HAUGHN to open a restaurant, and that

the only thing he could do was to ask his brother to return whatever funds might remain from this endeavor. HAUGHN stated that he had about $100,000 in a Barclay's account in the United Kingdom, but that his money was supposed to be for his daughter's private school.

31. HAUGHN also attempted to induce the victim to send him money by telling her that if she were to send him the money it could be lucrative. HAUGHN told her that he had plenty of money and that he could pay her back with interest. HAUGHN told the victim that she could think of sending him money as an investment.

32. Approximately two weeks after HAUGHN initially stated that he was detained, the victim agreed to cash in her pension and send him the money that he needed to be released and come to the United States. To ease some of her concerns, the victim requested that HAUGHN secure a good law firm to put together a contract. HAUGHN stated to the victim that he had an individual from a top law firm in London by the name of KEITH BENNETT (hereafter "BENNETT") to put together a contract. The victim then received a call on the WhatsApp messaging application from an individual purporting to be BENNETT. BENNETT sent the victim a document that BENNETT said he would have HAUGHN sign to reflect the debt that would be owed to the victim by HAUGHN. BENNETT told the victim that he had set a figure of $1,130,000 to be owed to her by HAUGHN to reflect any fees that that she might have to pay for cashing in her retirement funds. This document was then sent to the victim with signatures purporting to be from both HAUGHN and BENNETT. However, there are no current practicing attorneys/barristers on the United Kingdom's Solicitor's Register by the name of "KEITH BENNETT", with the closest being a "Paul Keith Bennett". The victim stated to the investigating law enforcement agents that "Paul Keith Bennett" was not the individual that she had communicated with. The investigating law enforcement agents believe the victim's entire interaction with BENNETT was a ruse to lull her into a false sense of security that her funds would ultimately be returned to her.

33. When the victim first attempted to withdraw her funds from her retirement funds held at Fidelity Investments (hereafter, "Fidelity"), she openly told Fidelity that she was, "attempting to cash in her retirement to help her boyfriend who had been detained by customs in Frankfurt, Germany". Upon receiving this information Fidelity flagged the victim's account for fraud and told her that they were going to close her account. Fidelity would only allow the victim to transfer her funds out to another brokerage or financial retirement firm. The victim then sent her money to Charles Schwab (hereafter, "Schwab"), where she held the small retirement account that she had inherited from her deceased parents.

34. On October 23, 2023, the victim wired $500,000 from her Schwab account to an account that she held at Crypto.com[6]. When submitting the reason for moving the funds, the victim openly told Crypto.com the same thing that she told Fidelity. In response to this Crypto.com removed the victim from their platform and returned her funds, with $400,000 of the returned funds deposited to the victim's checking account at JP Morgan Chase.

Victim's Usage of Coinbase to Transfer her Funds to "HAUGHN"

35. The victim had previously opened an account with Coinbase in approximately 2020. Coinbase is a cryptocurrency exchange founded and with offices in San Francisco, California. As of October 2023, this account was still open with a balance of approximately $5.02. On November 3, 2023, the victim transferred a total of approximately $396,000.00 of her funds from her JP Morgan Chase account to her Coinbase account. Most of the funds transferred to Coinbase ultimately originated from the victim's Schwab account. After fees, this resulted in a total of approximately $395,980.00 being deposited to the victim's Coinbase account.

36. Per statements from the victim, corroborated by financial records law enforcement reviewed, on November 4, 2024, the victim gave HAUGHN access to her Coinbase account. While

[6] Crypto.com is a cryptocurrency exchange headquartered in Singapore.

speaking on the phone with HAUGHN, the victim provided to HAUGHN the two-factor authentication[7] code that was sent to her via text message from Coinbase. HAUGHN then used this to log in to the victim's Coinbase account and used the victim's US Dollars to purchase USDT cryptocurrency.

37. On November 10, 2023, HAUGHN provided **Target Address 1** to the victim verbally over the phone and coached the victim through transferring approximately 383,238.467333 USDT from the victim's Coinbase account to **Target Address 1.** This transaction occurred at approximately 1:02 AM UTC on November 11, 2023. After transaction fees, this resulted in approximately 383,235.034673 being stored at **Target Address 1**.

38. After this transfer, the victim was contacted by HAUGHN, who then told her that although he had settled what he owed to the German authorities, he would face additional fees to enter the United States. Since the victim had already sent what she believed to be a substantial amount of money to HAUGHN, she felt that she was already committed to him and did not have any other choice but to transfer HAUGHN the additional money that he was requesting.

39. On November 17, 2023, the victim transferred approximately $600,000.00 from her account at Schwab to her account at Coinbase. After fees, this resulted in approximately $599,990.00 deposited to her Coinbase account. That same day, the victim used these funds to purchase approximately 580,814.343842 USDT. Thereafter, on that same day, HAUGHN provided **Target Address 2** to the victim verbally over the phone and coached her through transferring the USDT from her Coinbase account to **Target Address 2**. This transaction occurred at approximately 6:32 PM UTC on November 17, 2023. After transaction fees, the transaction resulted in approximately 580,811.023397 USDT being stored at **Target Address 2.**

[7] Two-factor authentication is a method of electronic authentication in which a user must present two or more pieces of information in order to authenticate to a system. It is commonly implemented as a user needing to provide both a password and a code provided via text-message when logging in to a system.

40. After these transfers, HAUGHN told the victim that he had arrived in Los Angeles, but that he was under pressure with his work at the Swedish embassy. The victim explained to HAUGHN that she was desperate for money to pay her bills. The victim had to pay, among other things, medical bills that she had incurred.

41. After pleading with HAUGHN, on November 22, 2023, HAUGHN returned approximately 15,000 USDT from **Target Address 1** to the victim's Coinbase account. After continued pleading to HAUGHN, on January 7, 2024, HAUGHN made an additional transfer of approximately $50,000 USDT from **Target Address 1** to the victim's Coinbase account. Law enforcement agents know from the investigating law enforcement agents' training and experience that perpetrators of pig butchering schemes will often provide a small amount of funds to a victim to create a false sense of trust with the victim. Law enforcement agents believe that this was the purpose of these transactions.

42. The relationship between HAUGHN and the victim began to break down following the victim's repeated requests for repayment. HAUGHN eventually told the victim that his mother had become ill and that he needed to travel back to Sweden. On February 18, 2024, HAUGHN claimed to the victim that his mother had died. HAUGHN's communications with the victim then began to fade away, with HAUGHN eventually telling the victim that he was in the hospital and sedated. On approximately April 14, 2024, or April 15, 2024, the victim reached out to HAUGHN's purported doctor, who told the victim that HAUGHN was getting better and would call soon, but he never did. Shortly thereafter, the victim realized that she may have been a victim of fraud, eventually reporting the incident to law enforcement on or about April 24, 2024.

43. From the investigating law enforcement agents' training and experience, law enforcement agents know that perpetrators of pig butchering schemes will often string victims along as possible to provide their money laundering network with time to obtain and launder their criminal proceeds and reduce the likelihood of seizure by law enforcement.

44. Based on the totality of the above information, law enforcement agents believe that HAUGHN is a false persona which was created by the Unknown Actor(s). The investigating law enforcement agents further believe that this false persona was used to develop a romantic relationship with the victim with the purpose of defrauding her of her retirement funds.

Tracing The Target Funds

45. As described above, the perpetrators of the criminal scheme against VICTIM #1 provided her with **Target Address 1** and **Target Address 2** for deposits, which law enforcement investigators believe were both controlled by the criminal actors.

46. Based on blockchain analysis, the initial transfer of the victim's funds to **Target Address 1** on November 11, 2023, was the first and only time any USDT was sent to **Target Address 1.** Therefore, criminal investigators believe **Target Address 1** was specifically and solely used for the fraud scheme against the victim, and all USDT stored at **Target Address 1** were the proceeds of this fraud. As described herein, after the initial transfer of approximately 383,235.034673 USDT to **Target Address 1**, a total of approximately 65,000 USDT was returned to the victim in two transfers on November 22, 2023, and January 7, 2024. Law enforcement agents believe these transfers of the victim's own funds – having been obtained through fraud - back to the victim, utilizing Coinbase, were conducted to continue the fraud scheme, as is the case in other pig butchering schemes.

47. In addition to these two transfers returning funds to the victim, another 64 transfers of USDT moved approximately 59,229.9 USDT of the victim's funds out of **Target Address 1** to various other cryptocurrency addresses. From the investigating law enforcement agents' training and experience law enforcement agents know perpetrators of fraud schemes such as this will rapidly siphon their criminal proceeds out of recipient accounts through multiple transactions to make tracing by law enforcement more difficult.

48. Approximately 259,012.134673 USDT of the victim's funds remained at **Target Address 1** and were thereafter seized by law enforcement agents.

49. As with **Target Address 1**, per the law enforcement agents' analysis, the initial transfer of the victim's funds to **Target Address 2** on November 17, 2023, was the first transfer of any USDT to **Target Address 2**. Therefore, criminal investigators believe **Target Address 2** was specifically and solely used for the fraud scheme against the victim, and immediately following this transfer, all USDT stored at **Target Address 2** was also the victim's funds obtained by fraud. Between April 15, 2024, and May 22, 2024, fourteen transfers occurred which moved approximately 57,607 USDT out of **Target Address 2**, resulting in a total of approximately 523,204.023397 USDT of the victim's funds remaining at **Target Address 2**.

50. Per the law enforcement investigators, **Target Address 2** appeared to have been specifically set-up and used for criminal purposes, as an instrumentality of fraud, by the perpetrators of the criminal scheme against the victim. HAUGHN specifically provided to the victim **Target Address 2** during the scheme. Further, no other funds were transferred to Target Address 2 prior to the fraud. On May 25, 2024, three transactions occurred in which approximately 3,003 USDT total was transferred into **Target Address 2** from an unknown source. These new funds made up less than 0.001% of the total funds stored at **Target Address 2**; the vast majority of the USDT stored at **Target Address 2** was made up of the victim's funds and is the proceeds of fraud. Law enforcement agents further believe the purpose of these small transfers may have been as part of a money laundering effort – specifically to commingle these other funds and thereby conceal the purpose of the address.

51. Based on this investigation, along with all the evidence gathered to date in this investigation and the investigating law enforcement agents' training and experience, law enforcement agents had and do have probable cause to believe that the Target Funds were subject to seizure and forfeiture as the proceeds of wire fraud and as property involved in money laundering, pursuant to both

18 USC § 981(a)(1)(A) and 18 USC § 982(a)(1). Law enforcement agents further believed there was probable cause to believe **Target Address 1** and **Target Address 2** were subject to seizure as property involved in, or as an instrumentality of money laundering under 18 USC § 981(a)(1)(A) and 18 USC § 982(a)(1) (both civil and criminal forfeiture).

SEIZURE OF THE DEFENDANT PROPERTY

52. Based upon the foregoing investigation, law enforcement agents obtained seizure warrants in the Northern District of California, signed by the Honorable Peter H. Kang, on October 17, 2024 (*see* Case Number 3:24-mj-71512 PHK). Both warrants were executed soon after, and the funds held in **Target Address 1** and **Target Address 2** – *i.e.*, the Defendant Property - were seized by law enforcement. The Defendant Property is now in U.S. government control.

VIOLATIONS

53. The United States incorporates by reference the allegations in paragraphs one through 51 as though fully set forth.

54. **Title 18, United States Code, Section 1343 (Wire Fraud)** provides in relevant part: "Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both."

55. **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, Section 1343 is considered a specified unlawful activity.

56. **Title 18, United States Code, Section 1957 (Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity)** provides in relevant part: "Whoever, in any of the circumstances set forth in subsection (d), knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than $10,000 and is derived from specified unlawful activity, shall be punished as provided in subsection (b)."

57. **Title 18, United States Code, Section 981(a)(1)(A)** provides for civil and criminal forfeiture of "[a]ny property, real of personal, involved in a transaction or attempted transaction in violation of section 1956, 1957 or 1960 of this title, or any property traceable to such property."

58. **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 [. . .] any offense constituting 'specified unlawful activity' (as defined in section 1956(c)(7) of this title), or a conspiracy to commit such offense."

59. 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 1343 (wire fraud) 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)).

///

///

///

///

///

///

///

///

///

///

///

///

60. 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 wire fraud, and wire fraud conspiracy, in violation of 18 U.S.C. §§ 1343, 1956, and 1957. As such, the Defendant Property is forfeitable pursuant to 18 U.S.C. § 981(a)(1)(A) and 981(a)(1)(C).

61. 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: July 28, 2025

Respectfully submitted,

CRAIG H. MISSAKIAN
United States Attorney

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

DAVID COUNTRYMAN
Assistant United States Attorney

VERIFICATION

I, JESSE BUMANLAG, state as follows:

1. I am a Special Agent with the Internal Revenue Service-Criminal Investigation. 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. Law enforcement agents 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 28th day of July 2025 in Oakland, California.

/s/ Jesse Bumanlag
JESSE BUMANLAG
Special Agent
Internal Revenue Service-Criminal Investigation