

UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Seizure of

(Briefly describe the property to be seized)

ALL VIRTUAL CURRENCY STORED WITHIN, OR
ASSOCIATED WITH, VIRTUAL CURRENCY ADDRESSES
AND ACCOUNTS IN THE CUSTODY OF TWO VIRTUAL
ASSET SERVICE PROVIDERS

)
)
)
)
)

Case No. 25-SZ-42

APPLICATION FOR A WARRANT
TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the jurisdiction of the District of Columbia is subject to forfeiture to the United States of America under 18 U.S.C. § § 981, 982, and 28 U.S.C § 2461

(describe the property):

SEE ATTACHMENTS A-1 and A-2, HEREBY INCORPORATED BY REFERENCE

The application is based on these facts:

SEE ATTACHED AFFIDAVIT, HEREBY INCORPORATED BY REFERENCE.

☒ Continued on the attached sheet.

Applicant's signature

Special Agent

Printed name and title

Attested to by the applicant in according with the requirements of Fed. R. Crim. P. 41 by telephone.

Date: 10/10/2025

City and state: District of Columbia

Moxila A. Upadhyaya, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT

for the
District of Columbia

In the Matter of the Seizure of
(Briefly describe the property to be seized)

ALL VIRTUAL CURRENCY STORED
WITHIN, OR ASSOCIATED WITH, VIRTUAL
CURRENCY ADDRESSES AND ACCOUNTS
IN THE CUSTODY OF TWO VIRTUAL ASSET
SERVICE PROVIDERS

)
)
)
)
)

Case No. 25-sz- 42

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the _____ Jurisdiction of the _____ District of _____ Columbia _____ be seized as being subject to forfeiture to the United States of America. The property is described as follows:

See Attachments A-1 and A-2, hereby incorporated by reference.

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property on or before 10/24/2025

(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to

Moxila A. Upadhyaya

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 10/10/2025



Judge's signature

City and state: Washington, D.C.

Moxila A. Upadhyaya, United States Magistrate Judge

Printed name and title

Return

Case No.: 25-sz- 42	Date and time warrant executed:	Copy of warrant and inventory left with:
------------------------	---------------------------------	--

Inventory made in the presence of:

Inventory of the property taken:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEIZURE OF
ALL VIRTUAL CURRENCY STORED
WITHIN, OR ASSOCIATED WITH,
VIRTUAL CURRENCY ADDRESSES
AND ACCOUNTS IN THE CUSTODY OF
TWO VIRTUAL ASSET SERVICE
PROVIDERS

SZ No. 25-sz-42

Filed Under Seal

Reference: USAO Ref. # 2025R00808;

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEIZURE WARRANTS

I, [REDACTED] being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a seizure warrant for all of the virtual currency stored within, or associated with, the following five virtual currency addresses, which are in the custody of or controlled by Tether Limited ("Tether"):

TGjgiiXSft9X3Q2894S1hLBxRx9icfKv74	("Target Property 40")
TE3RXGtd6YJZkDtv9CWDzLFbRbd8WHWUBB	("Target Property 41")
TXvK7Bikg9To8G78DtM6JK8jWwNTAxJkGT	("Target Property 42")
TR4U6oY95e2wQLYe9izoCt9hsAHVqiuFWs	("Target Property 43")
TVyENJr9iRdV4sqrbquoXX5StjYvXYhK9t	("Target Property 44")

This application is also made to support seizure of the following two Binance accounts, identified by their User Identification numbers, which are in the custody of or controlled by Nest Services Limited ("Binance"):

193278016	("Target Property 45")
1057117034	("Target Property 46")

Collectively these are referred to as the "Target Properties." The "Target Properties" are described in the following paragraphs and in Attachment A-1. The subject matter of this warrant is related to two other seizures, 25-sz-20, which was approved by Judge Matthew J. Sharbaugh of

this Court on March 25, 2025 (“25-sz-20 Seizure Warrant”) and 25-sz-34, which was approved by Judge Moxila A. Upadhyaya of this Court on June 25, 2025 (“25-sz-34 Seizure Warrant”).

2. I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(c), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a seizure warrant.

3. I am a Special Agent with the FBI and have been since September 2022. While employed by the FBI, I have investigated federal criminal violations related to high technology and cybercrime, including violations of 18 U.S.C. §§ 1030 (Fraud and Related Activities in Connection with Computers) and 1343 (Wire Fraud). I have gained experience through training and everyday work relating to conducting these types of investigations. Prior to becoming a Special Agent of the FBI, I earned a bachelor’s degree in history, a master’s degree in criminal justice, and served more than seven years as a communications officer in the United States Marine Corps. I have received training related to computer networking, virtual currency, and cyber security.

4. Specifically, I have completed the FBI’s Accelerated Cyber Training Program, which included ten virtual currency courses. I am one of only two agents in the FBI Albuquerque Field Office licensed to trace virtual currency via a Blockchain Analysis Software that has provided reliable information in the past and have attended in-person training and conferences focused on such. I have obtained a competency certification associated with Blockchain Analysis Software. I have seized both virtual currency and fiat currency in federal criminal investigations. I have obtained a Global Information Assurance Certification in Security Essentials and also a certification on using Open Source Intelligence investigative methods. In addition to my direct experience, I have also had conversations with cyber investigators across the FBI regarding dozens

of complex cases, including several involving virtual currency account and bank account seizures. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, analysts, witnesses, and agencies. This affidavit is intended to show that there is sufficient probable cause for the requested seizure warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

5. As further described below, this affidavit is made in support of an application for a seizure warrant for funds traceable to, and involved in, a scheme to solicit donations of virtual currency to Harakat al-Muqawamah al-Islamiyya, commonly known as HAMAS, a designated foreign terrorist organization, in violation of 18 U.S.C. § 2339B (Providing Material Support or Resources to Designated Foreign Terrorist Organizations), and to launder those donations on behalf of HAMAS. Thus, the **Target Properties** are subject to civil and criminal forfeiture: (1) under 18 U.S.C. § 981(a)(1)(G)(i) and 28 U.S.C. § 2461(c), because they constitute assets of a designated foreign terrorist organization, and property and assets that afford a person a source of influence over a designated foreign terrorist organization; (2) under 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 982(a)(1), because they constitute property involved in money laundering offenses intended to conceal or disguise the nature, the location, the source, the ownership, or the control of proceeds of a specified unlawful activity (to wit, 18 U.S.C. § 2339B), in violation of 18 U.S.C. § 1956(a)(1)(B)(i), and conspiracy to engage in concealment money laundering in violation of 18 U.S.C. § 1956(h); and (3) under 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), because they constitute or are derived from proceeds traceable to a violation of specified unlawful activity (to wit, 18 U.S.C. § 2339B).

6. Furthermore, virtual currencies are transferrable 24 hours a day, 365 days a year,

including on public holidays. As such, an order under 21 U.S.C. § 853(e) would not be sufficient to assure the availability of the property for forfeiture, as criminal actors can dissipate virtual currencies at any time.

LEGAL AUTHORITIES RELATING TO SEIZURE AND FORFEITURE

7. Pursuant to 18 U.S.C. § 981(a)(1)(G)(i), “[a]ll assets, foreign or domestic . . . of any individual, entity, or organization engaged in planning or perpetrating any Federal crime of terrorism (as defined in 18 U.S.C. § 2332b(g)(5)) against the United States, citizens or residents of the United States, or their property, and all assets, foreign or domestic, affording any person a source of influence over any such entity or organization” are subject to forfeiture to the United States. Violations of 18 U.S.C. § 2339B are included in the definition of a Federal crime of terrorism. Section 981(a)(1)(G)(i) thus covers two categories of property: (1) all assets, foreign or domestic, of individuals, entities, or organizations engaged in planning or perpetrating federal crimes of terrorism; and (2) all assets, foreign or domestic, that afford any person a source of influence over an entity or organization engaged in planning or perpetrating any federal crime of terrorism. *See, e.g., United States v. All Petroleum-Product Cargo Aboard the Bella with Int’l Mar. Org. No. 9208124*, Civil Action No. 20-1791 (JEB), 2021 U.S. Dist. LEXIS 189395, at *12–13 (D.D.C. Oct. 1, 2021) (“The Court concludes, as a result, that Defendant Properties likely afforded Madanipour and Mobin a source of influence over the IRGC because those properties were critical to furthering the affairs of the terrorist group’s enterprise. The Government thus properly brought this action for forfeiture under 18 U.S.C. § 981(a)(1)(G)(i).”) (citations omitted).

8. Among the government’s forfeiture authorities, the terrorism forfeiture provision applies to the broadest range of property. Specifically, Section 981(a)(1)(G)(i) provides for the

forfeiture of *all* property, foreign or domestic, of a terrorist organization or that affords a source of influence to any entity or organization over a terrorist organization, irrespective of whether the property has any nexus to a crime or to the United States. *See, e.g., United States v. One Gold Ring with Carved Gemstone*, Civil Action No. 16-CV-02442 (TFH), 2019 U.S. Dist. LEXIS 195423, at *1–2 (D.D.C. Nov. 7, 2019) (“§ 981(a)(1)(G)(i) covers all property ‘foreign or domestic.’ That is, the statute empowers the government to seek the forfeiture of property outside the United States, which may have never touched the United States. The broad expanse of this language is for forfeiture actions to reach all property of terrorist organizations.”).

9. Property that is involved in a money laundering offense (or conspiracy to commit a money laundering offense) is subject to forfeiture under both civil and criminal authorities. Pursuant to 18 U.S.C. § 981(a)(1)(A) and (a)(1)(C), “[a]ny property, real or 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,” and “[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to” a specified unlawful activity, such as a violation of 18 U.S.C. § 2339B, is subject to forfeiture to the United States. Similarly, 18 U.S.C. § 982(a)(1) provides that the “[t]he court, in imposing a sentence on a person convicted of an offense in violation of section 1956, 1957, or 1960 of this title, shall order that the person forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property.”

10. Property “involved in” a money laundering offense “includes the money or other property being laundered (the corpus), any commissions or fees paid to the launderer, and any property used to facilitate the laundering offense.” *United States v. Puche*, 350 F.3d 1137, 1153

(11th Cir. 2003) (internal quotation omitted). “The statute sweeps broadly because ‘money laundering largely depends upon the use of legitimate monies to advance or facilitate the scheme.’” *United States v. Bikundi*, 926 F.3d 761, 793 (D.C. Cir. 2019) (quoting *Puche*, 350 F.3d at 1153). Forfeitures can include untainted funds that are comingled with tainted funds derived from illicit sources. *See United States v. Casey*, 444 F.3d 1071, 1073 (9th Cir. 2006) (“It is . . . clear that Congress intended criminal forfeiture provisions to eliminate profit from certain criminal activities, including money laundering”); *United States v. Kivanc*, 714 F.3d 782, 794-95 (4th Cir. 2013) (“Consequently, when legitimate funds are comingled with property involved in money laundering or purchased with criminally derived proceeds, the entire property, including the legitimate funds, is subject to forfeiture.”); *United States v. Lazarenko*, 564 F.3d 1026, 1035 (9th Cir. 2009) (“[I]n a money laundering charge, the comingling of tainted money with clean money taints the entire account. The money transferred from a comingled account does not need to be traceable to fraud, theft, or any wrongdoing at all. It is enough that the money, even if innocently obtained, was comingled in an account with money that was obtained illegally.”) (internal citations omitted). When the laundering transaction is a purchase, sale, exchange, or disbursement, the property that is bought, sold, exchanged, or otherwise the subject of the transaction is deemed to be “involved in” the offense. *See, e.g., United States v. Real Prop. Identified As: Parcel 03179-005R*, 311 F. Supp. 2d 126, 130 (D.D.C. 2004) (“[T]he Court concludes that the government has demonstrated that the aircraft was involved in a monetary transaction [a payment of specific unlawful activity proceeds to release a lien on the aircraft] involving the proceeds of specified unlawful activity. Clearly, this involvement renders the aircraft subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).”)

11. Title 18, United States Code, Section 981(a)(1)(C) subjects to civil forfeiture “[a]ny property, real or personal, which constitutes or is derived from proceeds” of any “specified unlawful activity.” The term “specified unlawful activity” is defined in 18 U.S.C. § 1956(c)(7) and 1961(1) and it includes, among other crimes, Providing Material Support to a Foreign Terrorist Organization, in violation of 18 U.S.C. § 2339B.

12. In addition, 28 U.S.C. § 2461(c) provides that, “[i]f a person is charged in a criminal case with a violation of an Act of Congress for which the civil or criminal forfeiture of property is authorized,” then the government can obtain forfeiture of property “as part of the sentence in the criminal case.”

13. This application seeks a seizure warrant under both civil and criminal authorities because the Target Properties consist of a transferrable, virtual currency that can easily be placed beyond process if not seized by a warrant.

14. Pursuant to 18 U.S.C. § 981(b), property subject to forfeiture under § 981 may be seized via a civil seizure warrant issued by a judicial officer “in any district in which a forfeiture action against the property may be filed,” if there is probable cause to believe the property is subject to forfeiture. Section 982(b)(1) incorporates the procedures in 21 U.S.C. § 853 (other than subsection (d)) for criminal forfeiture proceedings. Section 853(f) of Title 21 permits the government to request the issuance of a seizure warrant for property subject to criminal forfeiture.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1355(a), which provides that [t]he district courts shall have original jurisdiction . . . of any action or proceeding for the recovery or enforcement of any fine, penalty, or forfeiture, pecuniary or

otherwise, incurred under any Act of Congress” This Court also has subject matter jurisdiction pursuant to 28 U.S.C. § 1345, which provides that “the district courts shall have original jurisdiction of all civil actions, suits or proceedings commenced by the United States.”

16. This Court has *in rem* jurisdiction over the **Target Properties** and venue lies in this Court pursuant to 18 U.S.C. § 981(b)(3) and 28 U.S.C. § 1355(b)(2), which provides that “[w]hen- ever property subject to forfeiture under the laws of the United States is located in a foreign coun- try, or has been detained or seized pursuant to legal process or competent authority of a foreign government, an action or proceeding for forfeiture may be brought . . . in the United States District Court for the District of Columbia.” *See, e.g., One Gold Ring with Carved Gemstone*, 2019 U.S. Dist. LEXIS 195423, at *2 (“This court is the sole jurisdiction where such litigation is properly lodged. 28 U.S.C. § 1355(b)(2).”). Specifically, Tether Limited, the issuer of Target Properties 40- 44, is domiciled in El Salvador. In addition, the Binance accounts constituting Target Properties 45-46 all belonged to users with foreign identification documents and addresses.

17. The property may also be seized pursuant to 18 U.S.C. § 981(b)(3), 28 U.S.C. §§ 1355(b)(1)(B) and 1395(a), and 18 U.S.C. § 3238, because the criminal offenses under investigation were begun or committed upon the high seas, or elsewhere out of the jurisdiction of any particular State or district, and no offender is known to have, or have had, residence within any United States district.

SUBSTANTIVE CRIMINAL OFFENSES

18. Providing Material Support or Resources to Designated Foreign Terrorist Organizations. This investigation relates to the provision of material support to a foreign terrorist organization, in violation of 18 U.S.C. § 2339B.

19. 18 U.S.C. § 2339B(a)(1) provides, “Whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 20 years, or both.” “[M]aterial support or resources” is defined as

any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials.

18 U.S.C. §§ 2339A(b)(1), 2339B(g)(4).

20. 18 U.S.C. § 2339B(d) identifies several bases for jurisdiction over an offense under Section 2339B(a)(1), including when “the offense occurs in or affects interstate or foreign commerce.” 18 U.S.C. § 2339B(d)(1)(E).

21. Money Laundering. 18 U.S.C. § 1956(a)(1)(B)(i) makes it a crime to conduct or attempt to conduct a financial transaction, knowing that the property involved in the transaction represents the proceeds of some form of unlawful activity, and which in fact involves the proceeds of specified unlawful activity, knowing that the transaction is designed in whole or in part to conceal the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity. This activity is commonly referred to as concealment money laundering.

22. The money laundering statute, 18 U.S.C. § 1956, also makes it a crime to conspire to engage in money laundering: “Any person who conspires to commit any offense defined in [section 1956] or section 1957 shall be subject to the same penalties as those prescribed for the

offense the commission of which was the object of the conspiracy.” 18 U.S.C. § 1956(h).

DEFINITIONS AND BACKGROUND

Background Related to Virtual Currency

23. **Virtual Currency**: Virtual currencies are digital tokens of value circulated over the Internet. Virtual currencies are typically not issued by any government or bank like traditional fiat currencies, such as the U.S. dollar, but rather are generated and controlled through computer software. Different virtual currencies operate on different blockchains, and there are many different, widely used virtual currencies currently in circulation. Bitcoin (or BTC) and ether (ETH) are currently the most well-known virtual currencies in use. BTC exists on the Bitcoin blockchain and ETH exists on the Ethereum network. Typically, a virtual currency that is “native” to a particular blockchain cannot be used on a different blockchain. Thus, absent technological solutions those native assets are siloed within a specific blockchain. For instance, ETH (the native token on the Ethereum network) cannot be used on other networks unless it is “wrapped” by smart contract code. This wrapping process results in what is called Wrapped ETH or WETH.

24. **Stablecoins**: Stablecoins are a type of virtual currency 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 currency. Stablecoins achieve their price stability via collateralizations (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

25. **Tether (USDT)**: Tether (“USDT”) is a virtual currency that resides on multiple blockchains. The value of USDT is tied to the value of the U.S. dollar; therefore, one unit of USDT is represented to be backed by one U.S. dollar in Tether Limited’s reserves, making it what is known as a “stablecoin.” USDT is hosted on the Ethereum and Tron blockchains, among others.

USDT is issued by Tether Limited, a company that controls the smart contracts and treasury for USDT, which, based on Tether's website, is domiciled in El Salvador. Because Tether manages the smart contracts for USDT, it can freeze addresses containing USDT. For example, as is relevant to this application, Tether can freeze addresses on the Ethereum network, rendering the USDT in the addresses inaccessible to whomever controls the private keys to the frozen addresses. In the instant case, at the request of law enforcement, Tether acted to freeze the USDT associated with the Target Addresses and has indicated that they will continue to do so until March 26, 2025, or it receives the instant warrant.

26. **Tron (TRX)**: Tron is a blockchain network built to host decentralized applications with high speed, scalability and low fees. TRX is the native token used to power the network. TRC20 is a network protocol used for smart contracts, often enabling USDT transfers via the Tron blockchain.

27. **Virtual Currency Address**: 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 letters and numbers.

28. **Private Key**: Each virtual currency address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password, which is 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.

29. **Virtual Currency Wallet**: There are various types of virtual currency wallets, including software wallets, hardware wallets, and paper wallets. The virtual currency wallets at issue for the purposes of this affidavit are software wallets (*i.e.*, 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 allows users to store, send, and receive virtual currencies. A virtual currency wallet can hold many virtual currency addresses at the same time.

30. Wallets that are hosted by third parties are referred to as "hosted wallets" because the third party retains a customer's funds until the customer is ready to transact with those funds. Conversely, wallets that allow users to exercise total, independent control over their funds are often called "unhosted" wallets.

31. **Blockchain**: 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 the decentralized network of computers, 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 has ever received that virtual currency and 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.

32. **Blockchain Explorer**: These explorers are online tools that operate as a blockchain search engine allowing users the ability to search for and review transactional data for any addresses on a particular blockchain. A blockchain explorer is software that uses API¹ and blockchain nodes to draw data from a blockchain and uses a database to arrange and present the data to a user in a searchable format.

¹ API is an initialism for "application programming interface," which is a set of definitions and protocols for building and integrating application software.

33. **Smart Contracts**: Smart contracts are computer programs stored on a blockchain that run when predetermined conditions are met. Typically, they are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement. The Ethereum network is designed and functions based on smart contracts.

34. **Virtual Currency Bridge**: A blockchain bridge, otherwise known as a cross-chain bridge, connects two blockchains and allows users to send virtual currency from one chain to the other.

35. **Virtual Currency Exchanges (VCEs)**: VCEs are trading and/or storage platforms for virtual currencies, such as BTC and ETH. There are generally two types of VCEs: centralized exchanges and decentralized exchanges, which are also known as "DEXs." Many VCEs also store their customers' virtual currency in virtual currency wallets. As previously stated, these wallets can hold multiple virtual currency addresses associated with a user on a VCE's network. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers (i.e., KYC checks) and to have anti-money laundering programs in place (to the extent they operate and service customers in the United States).

36. **Blockchain Analysis**: As previously stated, while the identity of a virtual currency address owner is generally anonymous, law enforcement can identify the owner of a particular virtual currency address by analyzing the blockchain (e.g., the Bitcoin blockchain). The analysis can also reveal additional addresses controlled by the same individual or entity. "For example, when an organization creates multiple [BTC] addresses, it will often combine its [BTC] addresses into a separate, central [BTC] address (i.e., a "cluster"). It is possible to identify a 'cluster' of [BTC]

addresses held by one organization by analyzing the [BTC] blockchain's transaction history. Open source tools and private software products can be used to analyze a transaction." *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020).

37. In addition to using publicly-available blockchain explorers, law enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions. Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

38. **Decentralized Finance (DeFi)**: Decentralized Finance, or DeFi, is an umbrella term for financial services on public blockchains, primarily the Ethereum network. The Ethereum network's native virtual currency is ETH. Ethereum was the first blockchain that offered various decentralized services within its network. To make these services possible, the Ethereum network allows other tokens besides ETH to run within the network. These tokens are known as ERC-20 tokens.

39. DeFi is a term used to describe a financial system that operates without the need for traditional, centralized intermediaries. Instead, DeFi platforms offer an alternative financial system that is open for anyone to use, and that allows centralized intermediaries to be replaced by decentralized applications (or dApps). With DeFi, one can do most of the things that banks support—earn interest, borrow, lend, buy insurance, trade derivatives, trade assets, etc.—but it is faster than using traditional banks and does not require paperwork or a third party. DeFi is global, peer-to-peer (*i.e.*, directly between two people rather than routed through a centralized system), pseudonymous, and open to the public.

Background of the Investigation

I. HAMAS and the al-Qassam Brigades

40. Harakat al-Muqawamah al-Islamiyya, commonly known as HAMAS, was founded in 1987 as an outgrowth of the Palestinian branch of the Muslim Brotherhood. From its inception, HAMAS's stated purpose has been to create an Islamic Palestinian state throughout Israel by eliminating the State of Israel through violent holy war, or jihad. HAMAS has not only directed its violence and terrorism against Israeli targets in furtherance of that goal; HAMAS's leaders have also assailed the United States and American citizens, in retaliation for and in an effort to weaken American support for Israel's right to exist and defense of that right. HAMAS has murdered and injured dozens of Americans as part of its campaign of violence and terror.

41. HAMAS carries out terrorist attacks and armed conflict through the Izz al-Din al-Qassam Brigades (the "al-Qassam Brigades"), its military wing. The al-Qassam Brigades conduct suicide bombings and other terrorist attacks within Israel, Gaza, and the West Bank, and have done so for decades. These attacks have included large-scale bombings against Israeli civilian targets, small-arms attacks, improvised roadside explosives, and rocket attacks.

42. On October 8, 1997, the United States Secretary of State designated HAMAS as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act. On October 31, 2001, the Secretary of State also designated HAMAS as a Specially Designated Global Terrorist under Executive Order 13224. The Secretary of State has also listed the following aliases for HAMAS: Islamic Resistance Movement, Harakat al-Muqawama al-Islamiya, Students of Ayyash, Students of the Engineer, Yahya Ayyash Units, Izz Al-Din Al-Qassim Brigades, Izz Al-Din Al-Qassim Forces, Izz Al-Din Al Qassim Battalions, Izz al-Din Al Qassam Brigades, Izz al-

Din Al Qassam Forces, and Izz al-Din Al Qassam Battalions. To date, HAMAS remains a designated FTO.

II. The October 7 HAMAS Massacres

43. On or about October 7, 2023, HAMAS and other terrorist groups, including the Palestinian Islamic Jihad (“PIJ”), another designated FTO,² launched a surprise assault into Israel (“the October 7 HAMAS Massacres”). HAMAS began by firing thousands of rockets, and then HAMAS militants crossed into Israel. The militants infiltrated Israeli towns and army bases and took civilian and soldier hostages, many of whom they brought back to Gaza. Israel formally declared war on HAMAS in response to the attack and began a ground invasion of the Gaza Strip on October 27, 2023. According to news reports, the HAMAS assault that began on or about October 7, 2023, killed approximately 1,200 people, including American citizens. HAMAS also took more than 250 people hostage, also including American citizens. HAMAS publicly took credit for the attacks.

44. In connection with the initiation of the October 7 HAMAS Massacres, on or about October 7, 2023, the supreme military commander of the al-Qassam Brigades, Mohammed al-Masri, a/k/a “Mohammed Deif,” a/k/a “al Khalid al-Deif,” issued a recorded message in which he “announce[d] the ‘Al-Aqsa Flood’ operation,” and identified himself as “commander-in-chief of

² On October 8, 1997, the United States Secretary of State designated Palestine Islamic Jihad – Shafaqi Faction as a Foreign Terrorist Organization under Section 219 of the Immigration and Nationality Act. On January 23, 1995, the Department of the Treasury also designated PIJ as a Specially Designated Terrorist under Executive Order 12947. The Secretary of State has also listed the following aliases for PIJ: PIJ-Shafaqi Faction, PIJ, Islamic Jihad in Palestine, Abu Ghunaym Squad of the Hizballah Bayt Al-Maqdis, Al-Quds Squads, Al-Quds Brigades, Saraya Al-Quds, Al-Awdah Brigades.

the Brigades of the martyr Ezeddine al-Qassam.”

45. Also on or about October 7, 2023, al-Masri stated in a message broadcast on al-Aqsa TV that the al-Qassam Brigades leadership had “decided to put an end to all the crimes of the occupation, and the time during which it was rampant without accountability has ended.” He stated that in the first minutes of the October 7 attacks, HAMAS launched 5,000 missiles and artillery shells, and asserted that the “Al-Aqsa Flood” operation was launched in response to what al-Masri described as “crimes committed by the Israeli occupation and colonial settlers,” and American and Western support for and international silence regarding the occupation. He also instructed:

Today, today, everyone who has a rifle, take it out, as now is the time. And whoever doesn’t have a rifle, take out your machete, your axe, your hatchet, your Molotov cocktail, your truck, your bulldozer, or your car.

46. On or about October 8, 2023, the day after the October 7 HAMAS Massacres had begun, Ali Baraka, HAMAS’s head of National Relations Abroad who is effectively responsible for HAMAS’s foreign relations,³ appeared in a video interview aired on a Russian television outlet. During the interview, Baraka conveyed that “[a] limited number of HAMAS leaders knew . . . about the attack and its timing.” Baraka stated that HAMAS’s social activities had actually been a

³ From 2011 to 2019, Baraka was HAMAS’s representative in Lebanon. Baraka is based principally in Lebanon. On or about December 13, 2023, the U.S. Department of the Treasury, Office of Foreign Assets Control (“OFAC”) designated Baraka as a Specially Designated Global Terrorist under Executive Order 13224. In announcing the designation, OFAC noted that, when he held the position of HAMAS’s representative to Lebanon, Baraka “met with international diplomats based in Lebanon on behalf of Hamas and spoke in support of violent campaigns” and that “[a]ccording to [] Baraka’s public statements, Hamas has long drawn on money and training from Iran and Iranian proxies like Hizballah while bolstering forces in Gaza.”

ruse, to “make them [*i.e.*, Israel and the international community] think that HAMAS was busy with governing Gaza, and that it wanted to focus on the 2.5 million Palestinians” living there, when “[a]ll the while, under the table, HAMAS was preparing for this big attack.” In fact, Baraka stated that HAMAS had “been preparing for this [*i.e.*, the October 7 HAMAS Massacres] for two years.” In response to a question about the hostages being held by HAMAS, Baraka stated, “There are also prisoners in the U.S. We want them. Of course. There are HAMAS members sentenced for life in the U.S. We want them too. Of course. We demand that the U.S. free our sons from prisons.”

47. The October 7 HAMAS attacks marked the beginning of what has become the Israel-HAMAS war. A ceasefire agreement between Israel and HAMAS was reached on or about January 15, 2025, and went into effect on or about January 19, 2025. On or about March 18, 2025, the Israeli Prime Minister’s Office released a statement indicating that he had authorized “the renewal of military action” against HAMAS.⁴

48. Between on or about October 7, 2023, and on or about May 1, 2025, numerous hostages taken by HAMAS have died in captivity or been released as part of a ceasefire deal with Israel.

III. The History of HAMAS Virtual Currency Financing

49. Beginning in or about early 2019, HAMAS, through the al-Qassam Brigades, tested virtual currency fundraising by soliciting donations on its Telegram channel before shifting to direct fundraising through its official websites: alqassam.net, alqassam.ps, and qassam.ps.⁵

⁴ See <https://www.gov.il/en/pages/event-statement180325>.

⁵ I know these to be official websites for the al-Qassam Brigades based on a previous investigation and subsequent United States Department of Justice announcement. See

50. The al-Qassam Brigades boasted that bitcoin donations were untraceable and would be used for violent causes. Their websites offered video instruction on how to anonymously make donations, in part by using unique bitcoin addresses generated for each individual donor. However, such donations were pseudoanonymous. Through leveraging blockchain analysis, federal authorities seized virtual currency accounts, while also covertly seizing and operating the infrastructure behind alqassam.net.⁶



Above: Bitcoin donation advertisement on alqassam.net

51. In April 2023, HAMAS announced that it would stop receiving funds via bitcoin

<https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>.

⁶ Information obtained via the U.S. Department of Justice, available at <https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>

due to donor safety concerns. Statements on the website then called for donations to continue through other means.

PROBABLE CAUSE

Finding Donation Addresses

52. In February 2025, FBI Albuquerque identified a terrorist financing network soliciting donations to the al-Qassam Brigades via virtual currency. On February 6, 2025, an FBI Confidential Human Source (hereinafter referred to as “CHS-1”), who is located in the United States and has provided reliable information in the past, alerted me to a Telegram post asking supporters to send an email to an address associated with the al-Qassam Brigades, fund[[@](#)]alqassam.ps, in order to donate.



Above: Post from the al-Qassam Brigades asking for support

Fund[[@](mailto:fund@alqassam.ps)]alqassam.ps's email address is also posted at the bottom of the al-Qassam Brigades website, <https://alqassam.ps/arabic/>. I know this to be an official website for the al-Qassam Brigades

based on a previous investigation and subsequent United States Department of Justice announcement.⁷



Above: Contact information shown on [alqassam.ps/arabic/](mailto:info@alqassam.ps)

On February 10, 2025, CHS-1 emailed [fund\[@\]alqassam.ps](mailto:fund[@]alqassam.ps) asking how the CHS could donate to the al-Qassam Brigades. Several hours later, CHS-1 received a response from [fund\[@\]alqassam.ps](mailto:fund[@]alqassam.ps) in Arabic, machine translated to the following:

In the name of Allah, the Most Gracious, the Most Merciful

"Go forth, whether light or heavy, and strive with your wealth and your lives in the cause of Allah. That is better for you, if you only knew." [At-Tawbah: 41]

Dear sister/s: May Allah protect and care for you

Peace, mercy, and blessings of Allah be upon you,

May Allah reward you for your keenness to perform the duty of support and assistance to your mujahid brothers in Gaza; and we ask Allah Almighty to accept from you your efforts and giving. If you do not have experience in dealing with digital currencies, you can seek the help of a friend inside or outside your country, or go to a money transfer office or exchange in your country that has digital currencies, and show only the wallet information from this message; To transfer the support amount to it; it is necessary not to inform the party that will undertake the transfer on your behalf of our identity; to preserve your security.

⁷ Information obtained via the U.S. Department of Justice, available at <https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>

Attached is the address and data of our current digital currency wallet; which is received from all other platforms:

Current wallet address:

TSWL3euRjZWXiFJgzvV9tYAGiwShtPWkZK

Please make sure to copy only the letters without any spaces before and after the letters; and it is preferable to extract the address from the code below:

Network Type:

Trc20

Currency Type:

USDT

Important Notes:

1. You can notify us of the value of the support and donation amount upon completion of the transfer process; to follow up on the receipt, God willing.

2. The wallet address is changed periodically to preserve your safety; therefore, the address is only valid for one transfer and support process; therefore, it is necessary to communicate via this email for any other new transfer process.

3. It is preferable not to use the "BINANCE" platform to transfer support; and not to enter any data indicating our official name so that your wallet is not blocked and for your safety as well (entering any fictitious data as the recipient of the transfer); You can transfer through the application: trust wallet, RedotPay, OKX, Kast, BYBIT...

Note: "BINANCE" can be used to purchase currencies only, then use another application to complete the transfer process.

4. We hope to circulate the official email for support and donations to the Al-Qasam Brigades: fund[[@](mailto:fund@alqassam.ps)]alqassam.ps and published on the official website of the Brigades <https://alqassam.ps>; with the necessity of alerting our honorable audience that our response to their messages may reach them in the "junk" or "spam" mailbox and not in the Inbox; due to our access restriction policies.

May Allah write you the reward and reward you with all good,

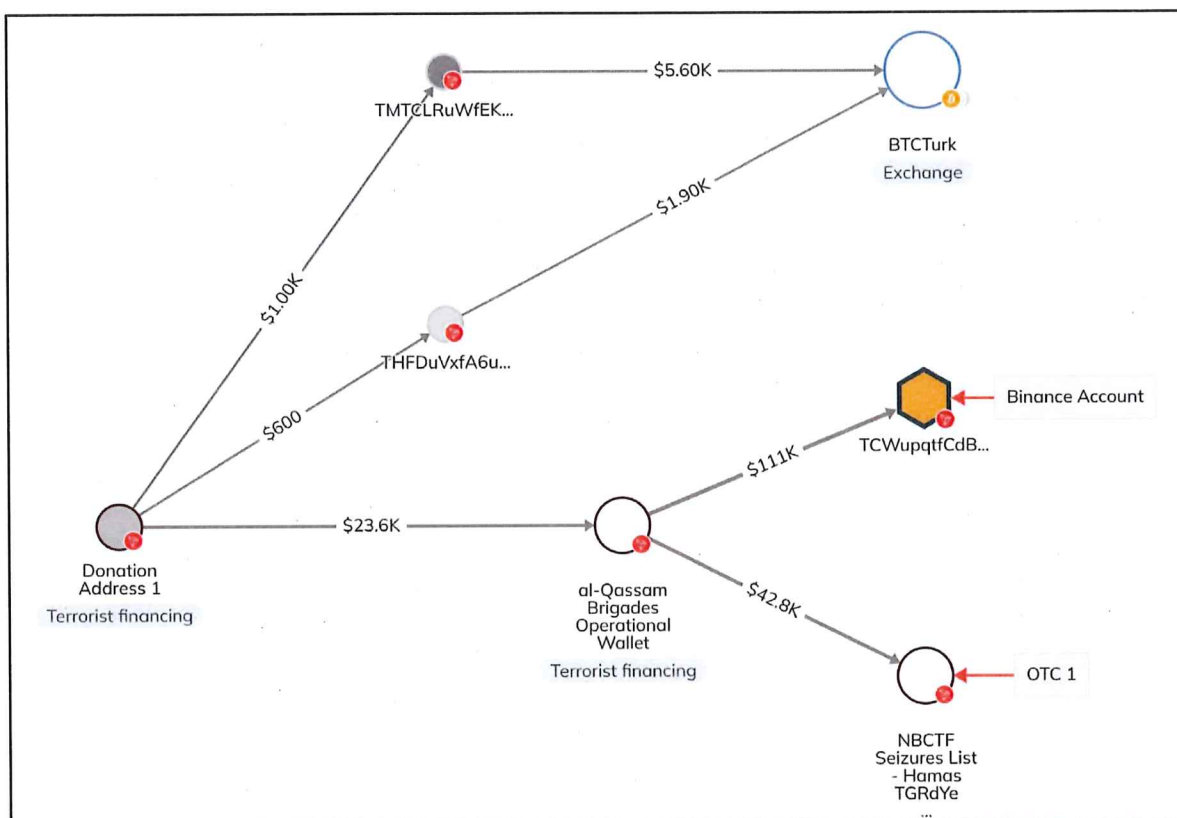
And we ask you to pray for your brothers in Gaza and Palestine

53. Based on my training and experience, I know that terrorists and cyber criminals often look for ways to obfuscate their online activity. Per the above message, the al-Qassam Brigades recommends donors avoid sending funds directly from Binance accounts. I have conducted in-depth virtual currency investigations and know Binance to be a commonly used exchange for users across the globe. However, I also know Binance maintains Know-Your-Customer (KYC) requirements to prevent fraudulent or illicit activity. Based on my training and experience, I also know other solutions listed, including Trust Wallet and Bybit, are commonly utilized to obfuscate the identity of the sender. By recommending these transfer solutions, the al-Qassam Brigades is seeking to receive funding while still attempting to protect the identities of their donors. Furthermore, I know USDT is a stablecoin that is widely used around the globe for different purposes, including, among other things, to finance criminal activities; and TRC20 is often chosen as a network because of its fast transaction speeds and low fees.

Finding the al-Qassam Brigades Operational Wallet

54. The FBI conducted virtual currency tracing and blockchain analysis on the USDT address that CHS-1 identified, TSWL3euRjZWXiFJgzuV9tYAGiwShtPWkZK, hereinafter referred to as "Donation Address 1". The FBI found that, despite al-Qassam's claims about operational security and each wallet being used to receive only one donation (cited above), Donation Address 1 received 34 deposits between on or about February 11, 2025, and February 21, 2025, totaling 25,211 USDT. The analysis indicated that Donation Address 1 completed six withdrawals on four separate occasions between February 12, 2025, and February 23, 2025. On each of the four occasions, Donation Address 1 was emptied. The highest balance Donation Address 1 reached

was 12,491.974213 USDT before it was emptied.



Above: A graphical representation of the flow of funds out of Donation Address 1

55. Of the 25,211 USDT received, 23,618 USDT was sent directly to another address, TA3aQxRwocYytqZBKqMPHPZT6pYvwGjLg1, hereinafter referred to as the “al-Qassam Brigades Operational Wallet.” Approximately 1,600 USDT of the 25,211 USDT was sent to a cluster of addresses on the public blockchain which, according to the Blockchain Analysis Software, is associated with an entity named BTCTurk, a virtual currency exchange operating out of Istanbul, Turkey. I have not requested records from BTCTurk due to concerns of the exchange notifying customers. However, through the course of numerous investigations, law enforcement has found

the attribution of clusters provided by this Blockchain Analysis Software to be reliable. Through the course of this investigation and many others, I have submitted hundreds of legal requests to virtual currency exchanges for records based on tracing and attribution via the same Blockchain Analysis Software, and in virtually every instance, the virtual currency exchange has been able to provide responsive records, or direct the FBI to a point of contact at the linked exchange, corresponding to the referenced transaction(s), thus confirming the Blockchain Analysis Software's attribution to the identified exchange. Your affiant is aware that in a few instances, subsidiaries of the listed exchanges themselves held records instead of the listed exchange. I submit probable cause exists to believe the Blockchain Analysis Software accurately identified the cluster of addresses displayed above as being owned by BTCTurk.

Identifying Exchange Accounts, Over the Counter Brokers, and Gas Wallet #1

56. Your affiant requested records from multiple exchanges (other than BTCTurk) and identified several donors who contributed to Donation Address 1. Additionally, investigators looked at all the virtual currency addresses that directly received donations for HAMAS and traced the flow of funds out of those accounts to exchanges. Based on records from those exchanges, the FBI learned of several individuals conducting book transfers of donation funds between accounts held at the same exchange. I know, based on my training and experience, that book transfers are difficult to trace because they are performed on an exchange's internal ledgers and not reflected on any public blockchain, and for this reason they are often used to obfuscate the flow of funds. As an example, Binance users can send USDT directly to other Binance users, without any blockchain record of the transactions. Investigators are unable to trace the flow of funds through trans-

actions like this with open-source tools, and are reliant on exchanges like Binance to provide records of the account-to-account transfers. Based on my training and experience, and the information learned from these exchange account records, I believe the al-Qassam Brigades has a robust network of financiers who conduct a series of transactions with donor funds to obfuscate the funds' ultimate destination.

57. Through blockchain analysis, I also observed the al-Qassam Brigades Operational Wallet send a portion of donated funds to an unattributed address, TGRdYen9qbfZGRDtpvGF7XGCYYWfpCPrQj, and "OTC 1."⁸ The al-Qassam Brigades Operational Wallet sent 42,800 USDT directly to OTC 1 via seven transactions occurring between February 11, 2025, and March 5, 2025. Based upon observations in this investigation, and my training and experience, HAMAS uses regional over-the-counter (OTC) money exchange businesses to transfer virtual currency. These regional OTCs can be used to obfuscate the flow of funds and swap virtual currency into government-issued fiat currency. Blockchain records of OTC 1 reveal numerous transfers to and from that account from many different sources over a brief period. In your affiant's training and experience, OTC addresses in a criminal enterprise such as OTC 1, have a similar pattern of transaction activity and are typically controlled by conspirators to prevent the conspirators' proceeds from being intercepted or stolen.

58. In addition, on February 16, 2025, I met with Person #1 via video conference. Person #1 is the Head of National Security Intelligence for the Virtual Currency Tracing Service that makes the Blockchain Analysis Software discussed above. Person #1 has been an industry expert

⁸ An unattributed address is a virtual currency address whose owner remains unknown at this time.

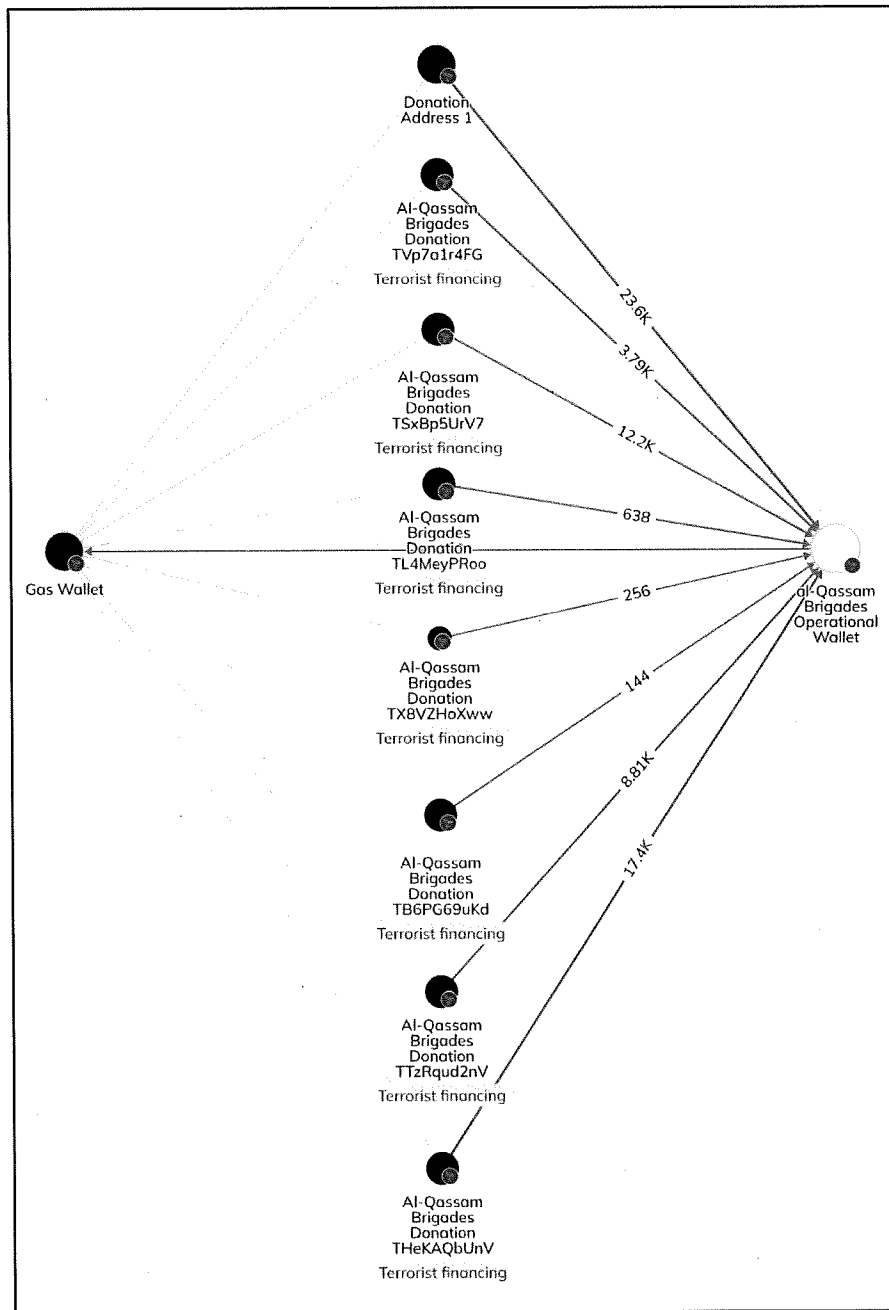
who has provided reliable information in the past and has at least three years of experience in virtual currency investigations. The FBI requested additional information from the Virtual Currency Tracing Service about Donation Address 1 and flows of digital currency from that address.

59. Person #1 indicated they had analyzed the donation network and found a recurring trend. Person #1 explained that the Virtual Currency Tracing Service identified what appeared to be many other donation addresses to the al-Qassam Brigades Operational Wallet. Each address received different amounts, but the vast majority of all transfers out of these donation addresses went to the al-Qassam Brigades Operational Wallet, similar to the pattern seen in the graph above illustrating transactions related to Donation Address 1. Furthermore, Person #1 showed me that most of the transfers out of the donation addresses were paid for via the same “Gas Wallet” (TMMF2wEzg3ywHSWrAeZttfdWpuBt1Az5TV, hereafter “Gas Wallet #1”). I confirmed what Person #1 showed me by reviewing publicly available information using the Blockchain Analysis Software.

60. A “gas wallet” is a virtual currency address that holds the funds necessary to pay virtual currency transaction fees, similar to how a car needs gas to run. I know, based on my training and experience, that addresses with outbound transactions paid for via the same gas wallet are almost always controlled by the same actor or group of actors, especially when the funds ultimately end in the same destination. Based on my training and experience, I know USDT transfers on TRC20 networks require funding, or “gas,” to transfer USDT between addresses. Gas fees on TRC20 are paid using TRX, the native token used to power the Tron network. I know new USDT addresses on TRC20 take only a matter of minutes to create, but sending funds in order to fund

transfers once donations are received requires organization and a consistent balance of TRX. Because of this, I also know that transfers paid for via the same gas funding address are almost always operated by the same actor or group of actors.

61. The graph below shows Donation Address #1 and seven other addresses which sent all the funds they collected to the al-Qassam Brigades Operational Wallet. Gas Wallet #1 paid the transaction fees to move the funds from Donation Address #1 and the seven other addresses to the al-Qassam Brigades Operational Wallet.



Above: A graphical representation showing the connection between the Gas Wallet #1 and multiple donation addresses, including Donation Address 1 and seven additional donation addresses identified as described below.

Finding Additional Donation Addresses

62. Following the findings that the Virtual Currency Tracing Service shared, your affiant conducted additional blockchain analysis and discovered more connections showing likely historical donations based upon the connection between the Gas Wallet #1 and the al-Qassam Brigades Operational Wallet. Blockchain data shows that the al-Qassam Brigades Operational Wallet had received approximately 1,574,719 USDT between October 28, 2024, and March 21, 2025. Furthermore, approximately 93% of outbound transfers from the al-Qassam Brigades Operational Wallet were funded via the previously mentioned Gas Wallet #1.

63. On February 17, 2025, another FBI Confidential Human Source based in the United States (hereinafter referred to as "CHS-2") alerted me to seven additional USDT donation addresses that CHS-2 received by emailing [fund\[.\]@alqassam.ps](mailto:fund[.]@alqassam.ps) in the same manner as CHS-1 had previously done. I reviewed the email responses from [fund\[.\]@alqassam.ps](mailto:fund[.]@alqassam.ps) to CHS-2 and found the email messages to be identical to the one that CHS-1 shared, except for the different donation addresses. The seven virtual currency addresses that CHS-2 received from the [fund\[.\]@alqassam.ps](mailto:fund[.]@alqassam.ps) accounts were embedded in emails with the same text as the one quoted above. These addresses were as follows:

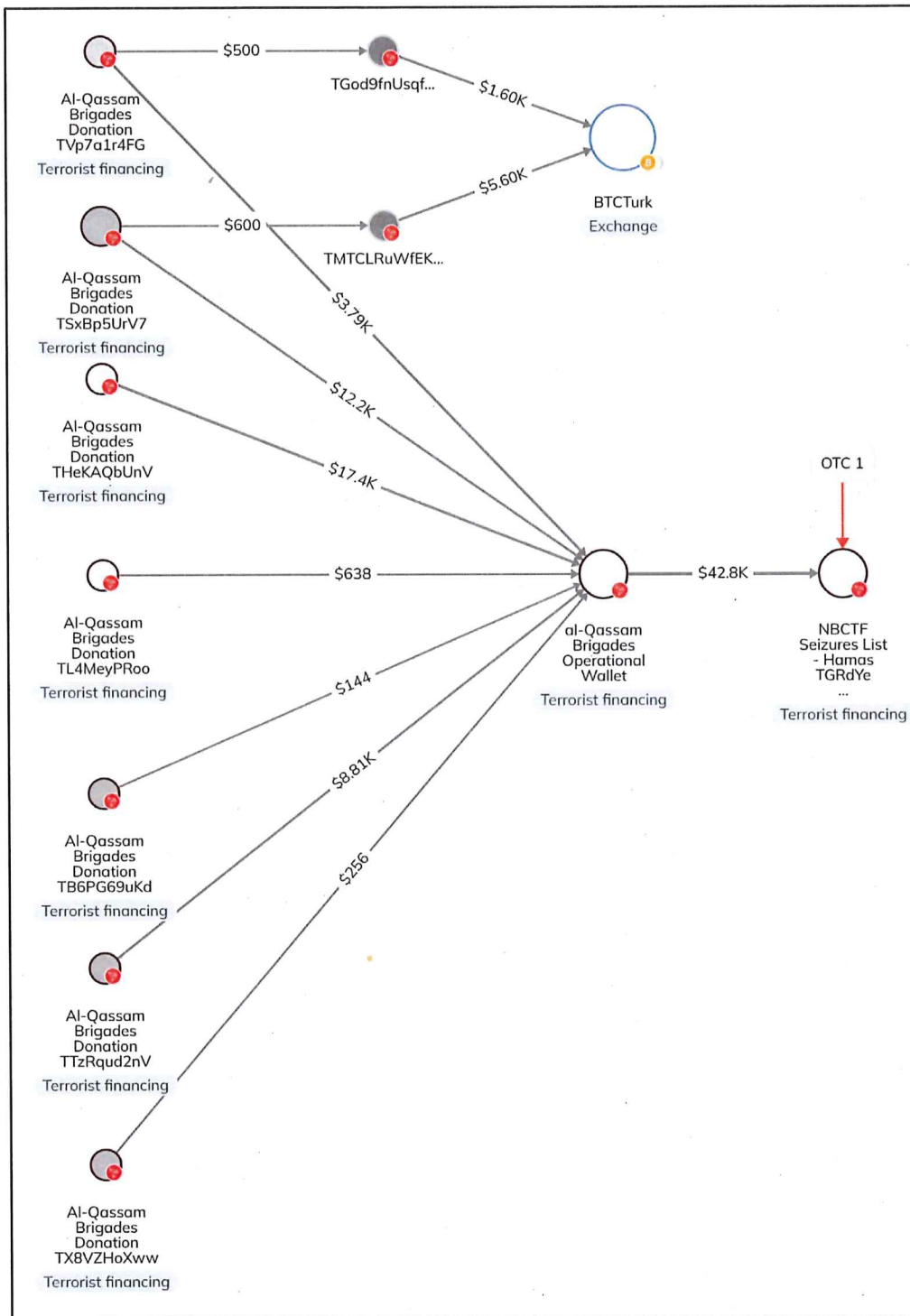
1. TVp7a1r4FGNgWE2ViskhcfVYxbyZRvpvmv
2. TB6PG69uKdN6NJirx8PnV7mJMVh4XRZvzp
3. THeKAQbUnV58Hnt8WxwwXaC4EjzTquoVes
4. TL4MeyPRooqL9UhCiqAHww7u2pNYs6guJS
5. TSxBp5UrV7HDp7Zu5EJc1ijDWGWhwsfBFK
6. TTzRqud2nVZJUSahxspmjqTHZKmfj3d9Uc

7. TX8VZHoXwwGDvL75m7cZee1gyipac3p5PQ

64. I conducted virtual currency tracing and blockchain analysis on all seven addresses obtained by CHS-2, finding the transaction pattern to be consistent with the pattern observed with Donation Address 1. In particular:

- All seven donation addresses received TRX to fund outbound transfers from the same previously identified Gas Wallet #1.
- The majority of all donations were subsequently transferred to the al-Qassam Brigades Operational Wallet.
- Based on additional records provided by a cryptocurrency exchange in response to requests for information, many of the funds sent out of the al-Qassam Brigades Operational Wallet went through a series of internal book transfers between different accounts at the same exchange, as with Donation Address 1.
- Some funds were transferred on the public blockchain to BTCTurk. As discussed above, Blockchain Analysis Software identified BTCTurk based on its own internal clustering and processes – which I have repeatedly found to be accurate in other investigations.
- The seven addresses appeared to be in use for only a few days at a time and were completely emptied when the user withdrew funds from them.

A graph depicting the above observations is reproduced below. Based on my training and experience, I know the transaction patterns discussed in the above bullets demonstrate that the virtual currency accounts are controlled by the same actor or group of actors.



Above: A graphical representation of donations through the seven addresses provided by CHS-2

65. The total amount received through the observation of the above seven donation addresses was approximately 45,948 USDT over a period of two weeks, between February 14, 2025, and February 28, 2025. Your affiant is aware that this is only a portion of the donation addresses used by the al-Qassam Brigades within this financing network during this period. During that same time the al-Qassam Brigades Operational Wallet received a total of 155,448 USDT from other addresses.

Further Investigation Identifies Additional Target Properties

66. Based on my training and experience, and the investigation described herein, all USDT addresses sent to potential donors by fund[[@alqassam.ps](#)] are used to as a means to provide material support to HAMAS. As discussed *infra*, your affiant's training and experience indicates that funds sent to the al-Qassam Brigades Operational Wallet were intended to fund HAMAS. Several other accounts and virtual currency addresses associated with the al-Qassam Brigades Operational Wallet (including several of the addresses discussed above) and Gas Wallet #1 were the subject of the 25-sz-20 Seizure Warrant (which was public) and the 25-sz-34 Seizure Warrant (which remains under seal).

67. As part of the investigation, additional funds held in accounts that were funded by the al-Qassam Brigades Operational Wallet were frozen by Tether on March 12, 2025. Based on blockchain transaction records, I observed donation addresses send funds to the al-Qassam Brigades Operational Wallet for several days after the freeze was placed. Beginning on or around March 17, 2025, your affiant observed what are, in your affiant's training and experience, new HAMAS donations traversing through other wallets, that were no longer consolidating through the same al-Qassam Brigades Operational Wallet. [REDACTED]

[REDACTED] Based on my training and experience, in conjunction with the patterns observed and described in this investigation, all addresses receiving direct TRX exposure from the Gas Wallet #1 are used to support this HAMAS financing network.

[REDACTED]

68. The Court seizure of funds from this network, including the affidavit in support of the seizure in 25-SZ-20, was unsealed or about March 27, 2025. Notably, that affidavit identified Gas Wallet #1 and its use in the criminal scheme. As discussed herein, and in your affiant's training and experience, the operators of the HAMAS donation network attempted to make changes to further obfuscate their ongoing criminal activity.

69. On or around April 21, 2025, [REDACTED]
[REDACTED]
[REDACTED] and provide TRX to the network in a very similar manner as previously seen. Transactions enabled [REDACTED] for approximately a week. Approximately 80 addresses were observed receiving what appeared to be consistent with donated funds. Once those funds were received, the 80 addresses consolidated those funds in another address. [REDACTED]

[REDACTED] These funds consolidated in a manner very similar to previous observations of the al-Qassam Brigades donation network. After consolidating, funds were distributed out to multiple different addresses that appeared to be OTCs or virtual currency exchange services. Approximately \$20,200 in USDT was sent to a Binance deposit address [REDACTED]

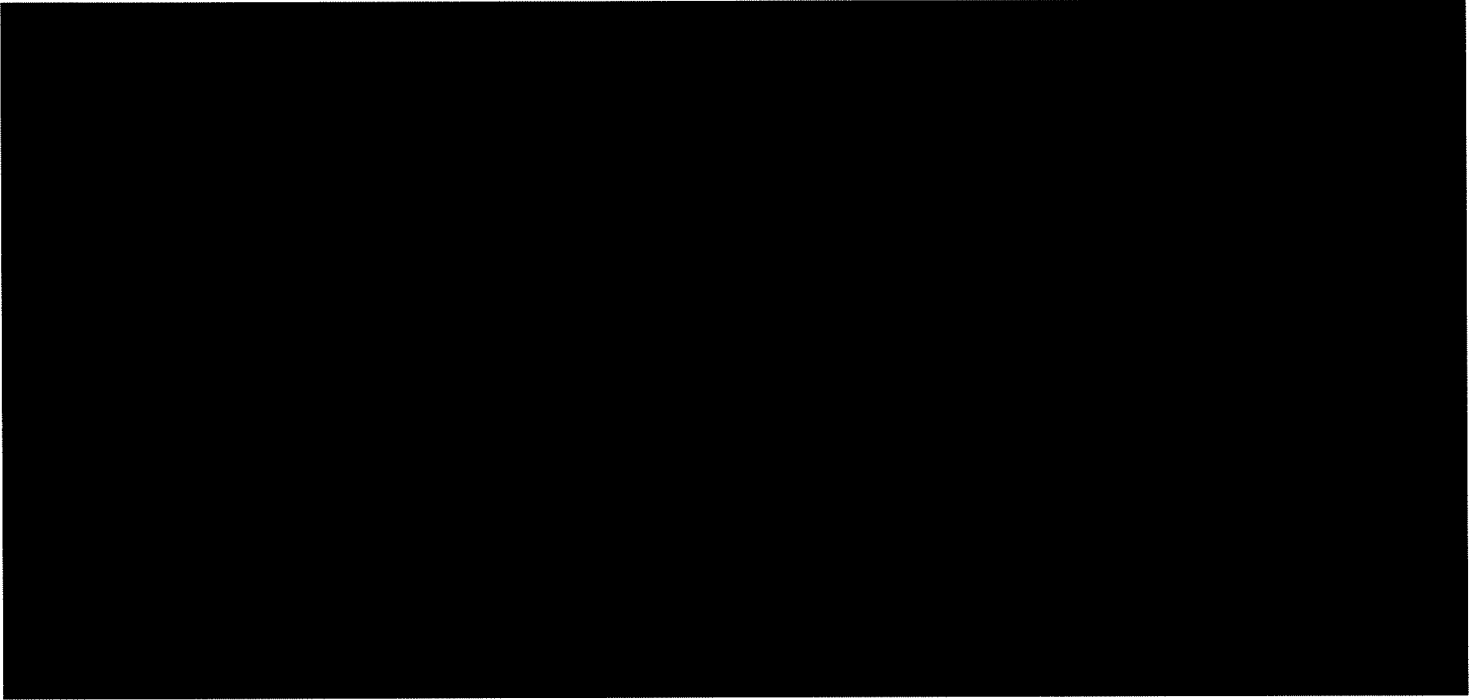
[REDACTED] s discussed in further detail below.

70. Another approximately \$1,200 was also sent from the same network of consolidation and intermediary addresses linked to [REDACTED] to a [REDACTED] eposit address. [REDACTED] is a virtual currency exchange and services platform domiciled outside the United States. [REDACTED] an owner of the account and revealed the Google email address used to register the account ("Financier 2"). Because the [REDACTED] account received virtual currency that was donated to HAMAS, investigators obtained a search warrant for that email account. Records from Google produced pursuant to that search warrant revealed an email from April 18, 2025, several days after the unsealing of the 25-SZ-20 affidavit, from the owner of the [REDACTED] account to KuCoin (a virtual currency provider that sells wallet services) claiming ownership over [REDACTED] TMMF2wEzg3yWHSWrAezttfdW-puBt1Az5TV). Below is that email:



71. Because of the disruption to accounts connected to [REDACTED] following the first

round of seizures that were publicly identified in 25-SZ-20, in your affiant's training and experience, the al-Qassam Brigades financing network began using other [REDACTED] [REDACTED] to fund the movement of donations. A graph depicting these observations is shown below.⁹



Above: A graphical representation of activity showing transitions from [REDACTED] [REDACTED] the cluster of 80 addresses to the Consolidation wallet.

72. On or around April 29, 2025, I observed another [REDACTED]

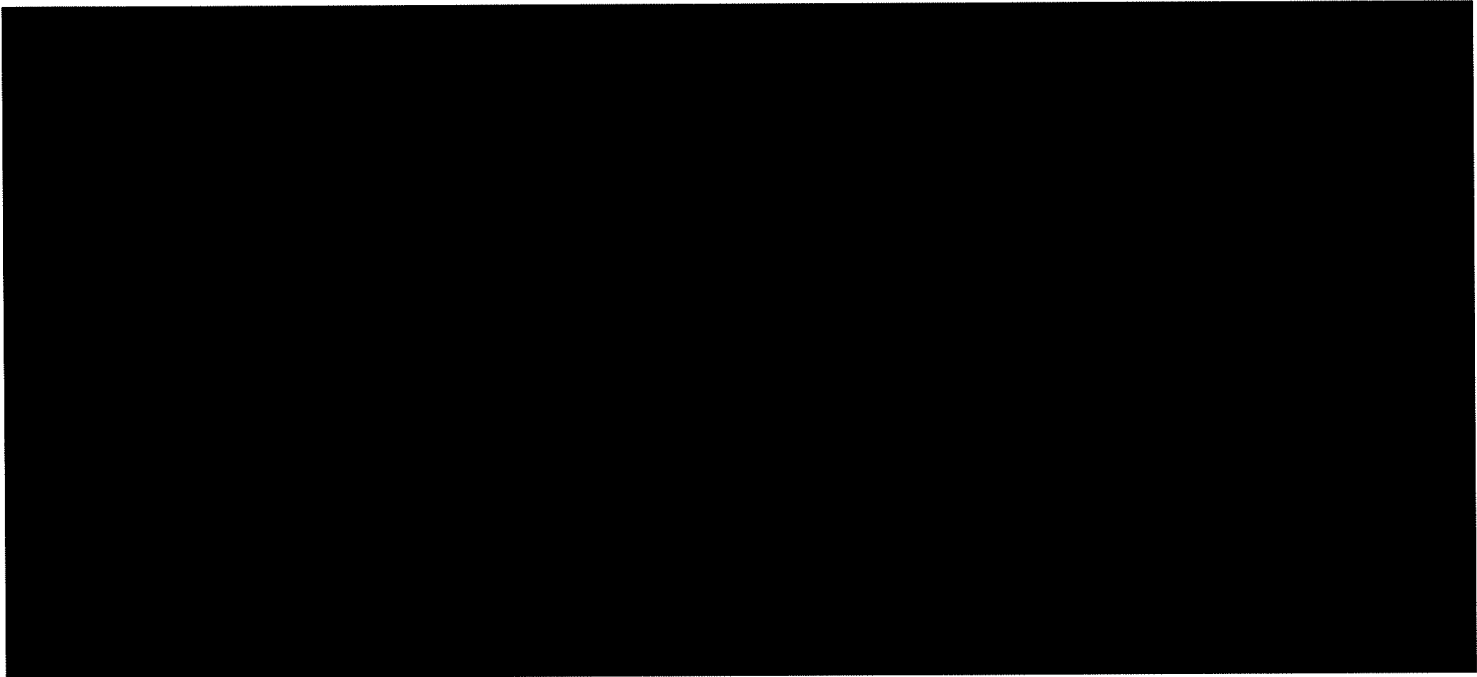
[REDACTED]
[REDACTED] and provide TRX to the network in a very similar manner as

⁹ Target Property 45, or TP 45 in the graph, is discussed further below.

[REDACTED]

In your affiant's training and experience [REDACTED] was a transitional wallet, meant for temporary usage to move funds from the publicly exposed account [REDACTED] to a new [REDACTED] that was not directly tied to [REDACTED]. In your affiant's training and experience, such layering or structuring activity is consistent with known money laundering techniques being utilized to attempt to further the illicit source and destination of illicit funds.

73. On May 2-3, 2025, the funds in 29 addresses were consolidated into one address (TSrPQijgQp5E55uH7c8jsheUQvqW6Xofja, hereafter the "TSrPQ Address"). As shown in the graph below, the consolidation of the 29 addresses as well as subsequent transactions from the consolidated cluster were [REDACTED]. Transactions out of the TSrPQ Address were also funded with [REDACTED]. Furthermore, the network funded by [REDACTED] also sent a portion of its funds to an intermediary address, which then forwarded those funds to the [REDACTED] address that also received transactions funded by [REDACTED].



Above: A graphical representation of activity showing transactions [REDACTED] and transactions ([REDACTED]) moving funds from 29 addresses to consolidate into the TSrPQ Address and from the TSrPQ Address to the [REDACTED] address.

74. Around the same time as the [REDACTED] transitioned, the donation addresses obtained by FBI CHSs through fund[[@](mailto:fund@alqassam.ps)]alqassam.ps did not show any blockchain transactions. In other words, it appears that the funding network had taken operational security steps to eliminate the re-use of funding wallets for multiple donors, such that when the FBI CHSs would receive an address from fund[[@](mailto:fund@alqassam.ps)]alqassam.ps, it appears HAMAS was not using that address to send to other potential donors.

75. These changes in laundering tactics were observed for multiple weeks. Based on my training and experience, the actors controlling this financing network became aware of disruptions via frozen and seized funds pursuant to the previously issued seizure warrants. Because of the disruptions, I believe these actors decided to change their laundering tactics to better conceal

the flow of HAMAS donations. Part of this effort included moving toward one-time use addresses. Because these addresses became unique to the requestor, all donation addresses directly obtained [REDACTED] showed no activity.

76. Additional investigation into the funding network identified other information that allowed the FBI to identify additional accounts controlled by the HAMAS funding scheme. Records obtained from Microsoft showed that an email address, selimhakan[[@](mailto:selimhakan@hotmail.de)]hotmail.de, sent a message to fund[[@](mailto:fund@alqassam.ps)]alqassam.ps on May 6, 2025. The same records showed a reply to that same address from fund[[@](mailto:fund@alqassam.ps)]alqassam.ps on May 7, 2025. As discussed above, this interaction is consistent with HAMAS sending a unique wallet address to that donor.

77. Records from Binance showed that selimhakan[[@](mailto:selimhakan@hotmail.de)]hotmail.de was the registered email address for a Binance account belonging to a resident of [REDACTED] (“Donor 1”). Binance records showed that Donor 1 sent 259.7185 USDT to TZE86gg4eb9EDMQmA5qn2vuyiLwC4hFbEb (the “TZE86 Address”) the same day Donor 1 received a reply email from fund[[@](mailto:fund@alqassam.ps)]alqassam.ps.

78. Several days later, on May 11, 2025, the TZE86 Address sent the funds it received from the Donor 1 Binance account to an address that received a total of 41527.728928 USDT from TZE86 and 65 other addresses. All of those transactions were [REDACTED]

[REDACTED] This same donation and consolidation pattern was duplicated on June 5, 2025. On that day, the Donor 1 Binance account sent 321.5155 USDT to TVie6wdG27ypweV-XiivWaaaDycgB6R4G4R (the “TVie6 Address”). Several days later, on June 9, 2025, the TVie6 Address sent its funds to another address that received a total of 17533.403026 USDT from TVie6 Address and 25 other addresses. Those transactions were [REDACTED]

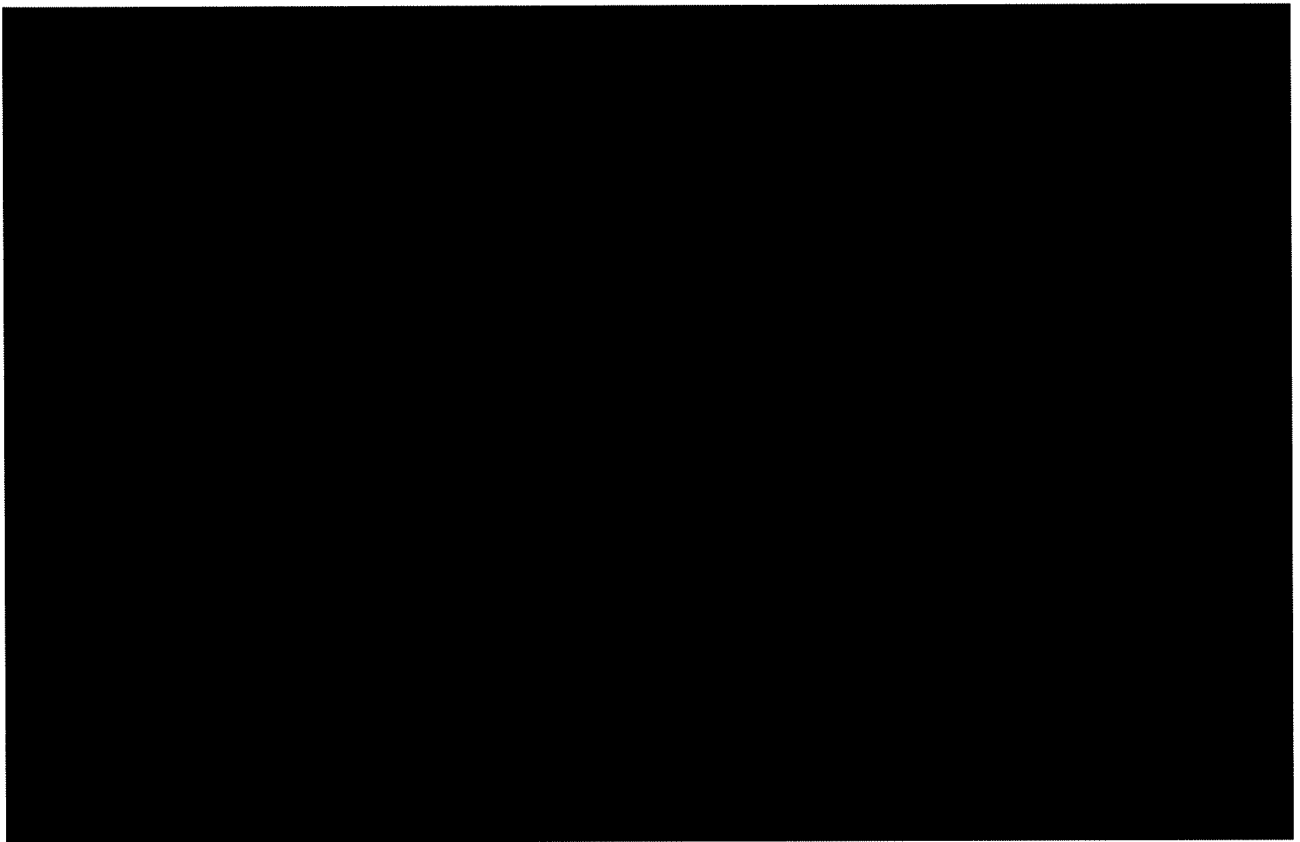
■. As shown in the graph below, ■ that sent funds from the addresses that received virtual currency from the TVie6 and TZE86 Addresses to “Bridgers[.]xyz” – an automated virtual currency instant exchange or swap service. Based on my training and experience, I know “Bridgers[.]xyz” to be an automated, cross-blockchain swap service, that is commonly used to automatically bridge cryptocurrency from one blockchain to another. “Bridgers[.]xyz” advertises that it enables transactions “without KYC,” meaning that it does not collect customer identifying information about the users of its swap service. “■

■

■

■

■



Above: A graphical representation of activity showing [REDACTED] funding transactions from an individual who communicated with fund[[@](mailto:fund@[REDACTED].ps)]alqassam.ps

Identification of Tether Addresses

80. On April 11, 2025, CHS-2 obtained a donation address, TVMAEC-byzJJa65ko4Djg1FbwCxSq6JjNXY (the “TVMAE Address”), via emailing fund[[@](mailto:fund@[REDACTED].ps)]alqassam.ps.

A screenshot of the email obtained by CHS-2 is below.

fund@alqassam.ps

How do I donate cryptocurrency?

fund@alqassam.ps <fund@alqassam.ps>

بسم الله الرحمن الرحيم

263-02

{وما تَنفِقُوا مِنْ شَيْءٍ فِي سَبِيلِ اللَّهِ يُوَفِّ إِلَيْكُمْ وَأَنْتُمْ لَا تُظْلَمُونَ} [الأنفال:60]

الأخ/ست الكريم/ة: حفظكم الله ورعاكم

السلام عليكم ورحمة الله وبركاته...

جزاكم الله خيراً على حرصكم لتأدية واجب النصرة والدعم لإخوانكم المجاهدين في غزة؛ ونسأله تعالى أن يتقبل منكم بذلكم وعطاءكم، ونعلمكم بأن الآلية المتاحة لتأدية الواجب حالياً بسبب ظروف المعركة المساهمة عبر العملات الرقمية، وفي حال لم يكن لديكم معرفة وخبرة بالتعامل معها، بإمكانكم الاستعانة بصدق داخل أو خارج بلدكم أو التوجه إلى مكتب حوالات مالية أو صرافة في بلدكم يتوفر لديه عملات رقمية، وإظهار بيانات المحفظة فقط من هذا الرسالة والموضحة أدناه؛ ليتم تحويل مبلغ الدعم عليها؛ مع ضرورة عدم إعلام الجهة التي ستتولى مهمة التحويل نيابة عنكم بهويتنا؛ حفاظاً على أمنكم.

مرفق عنوان وبيانات محفظة العملات الرقمية الخاصة بنا حالياً، والتي تستقبل من جميع المنصات الأخرى:

عنوان المحفظة الحالية:

TVMAECbyzJJJa65ko4Djg1FbwCxSq6JjNXY

يرجى التأكد من نسخ الحروف فقط بدون أي مسافات قبل وبعد الأحرف؛ ويفضل سحب العنوان من الرمز أدناه:

USDT



TVMAECbyzJJJa65ko4Djg1FbwCxSq6JjNXY

Above: Email received by CHS-2 via fund[@]alqassam.ps

This donation address received one donation of 227 USDT from another source on April 19, 2025 – indicating that the funding network’s operators had relaxed their procedures and may have reverted back to reusing donation addresses for multiple donors.

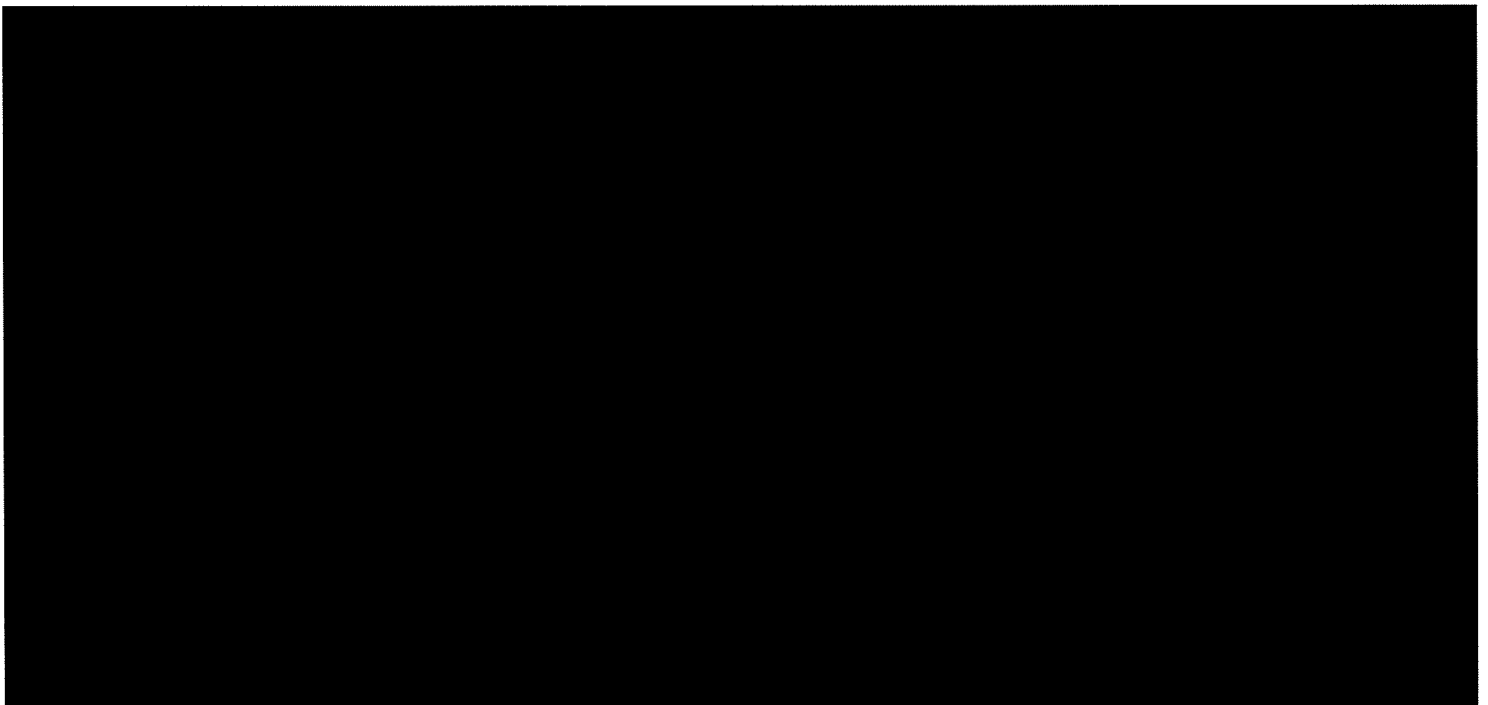
81. On May 22, 2025, the TVMAE Address sent funds to a consolidation address

On that day, 39 other addresses also sent funds to the same consolidation address. All of these transactions were also

, including an attempted transaction out of the address

TA5C5hoom3mktAGf3KZBNdxhEEujdUtpWG – which was previously frozen and included in 25-sz-34 as “Target Property 29.”

82. The 39 addresses, which all had associated transactions [REDACTED], are depicted on the bottom left of the below graph. I traced the subsequent transactions out of these addresses, totaling approximately 20,000 USDT, and found that they were sent to four unhosted wallets, shown on the right side of the below graph as **Target Properties 40-43**.



Above: A graphical representation of activity showing transactions funding Target Properties 40-43

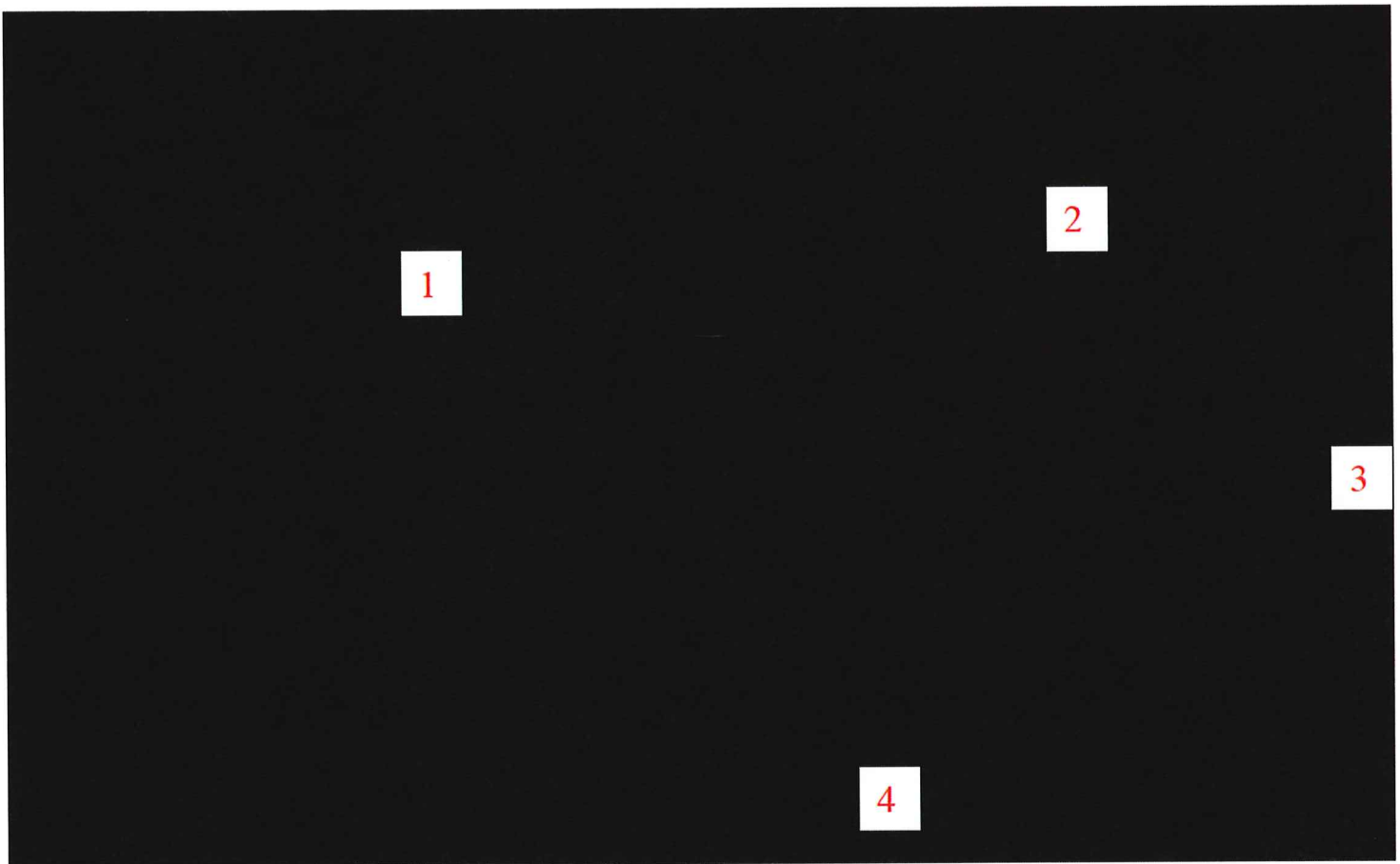
83. On May 22, 2025, the FBI submitted a request to Tether to freeze the funds contained in **Target Properties 40-43**. Later that same day, Tether enacted the freeze, confirming the below amounts were frozen.

TP 40: TGjgiiXSft9X3Q2894S1hLBxRx9icfKv74	15255.283984 USDT
---	-------------------

TP 41: TE3RXGtd6YJZkDtv9CWDzLFbRbd8WHWUBB	0 USDT
TP 42: TXvK7Bikg9To8G78DtM6JK8jWwNTAxJkGT	4300 USDT
TP 43: TR4U6oY95e2wQLYe9izoCt9hsAHVqiuFWs	397.260782 USDT

84. I conducted additional blockchain analysis to follow the [REDACTED] and found a new laundering pattern on June 12, 2025. Specifically, [REDACTED] was funding transactions that sent donations to 13 consolidation wallets from June 3 to June 12. Within those 13 consolidation addresses were amounts ranging from approximately 5,000 USDT to 25,000 USDT. One of these consolidation addresses contained the funds discussed above from Donor 1 Binance account. Each of these consolidations bridged USDT from TRC20 to the Binance Smart Chain (BSC), another blockchain, [REDACTED]

85. [REDACTED] and saw the donated USDT bridge from the TRC20 blockchain to the Binance Smart Chain. After being sent to Bridgers[.]xyz, the donated funds consolidated into two addresses, depicted on the right side of the below graph, before bridging back into the TRC20 blockchain. These repeated transactions incur fees and serve no economic purpose, except to facilitate operational security for money laundering, and appear to be a blatant attempt to obfuscate the direct involvement of a gas wallet in the transactions. After bridging back to TRC20, [REDACTED] approximately 137,500 USDT to an address that received and sent the same amount approximately 24 minutes later to TVyENJr9iRdV4sqrbquoXX5StjYvXYhK9t, hereinafter referred to as **Target Property 44**.



Above: A graphical representation of activity showing how Target Property 44 received its funds. The numbers break down the pattern described above and depicted in the graph. The number 1 shows the consolidation addresses sending their USDT funds to Bridgers[.]xyz – transactions that are [REDACTED]. The number 2 shows those funds being sent out of Bridgers[.]xyz to Binance Coin addresses. The number 3 shows the funds being consolidated again in a single Binance coin address and sent back to Bridgers[.]xyz. The number 4 shows the funds (now transformed back into USDT) being sent from Bridgers[.]xyz to a single USDT address (Target Property 44) – a transaction that [REDACTED].

86. On June 12, 2025, I submitted a freeze request to Tether to freeze the funds contained in **Target Property 44**. On June 14, 2025, Tether enacted the freeze, confirming **Target Property 44** held 155,438.916796 USDT.

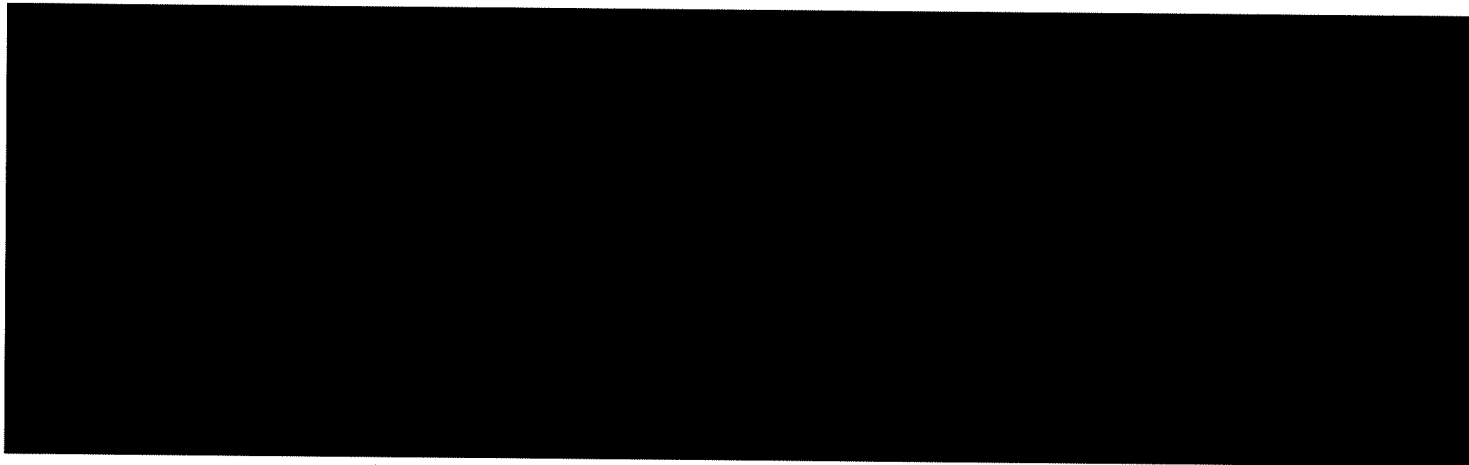
Identification of Binance Accounts

87. Your affiant is aware that some cryptocurrency exchanges, such as Binance, have instituted their own private efforts to combat certain criminal activity on their exchanges. On April 17, 2025, Binance alerted the FBI that based on its own internal investigation into this terrorist financing network, they had instituted a proactive account freeze based on their own blockchain analysis. Binance indicated it had frozen all withdrawals from TMsBHJcchJXbYxssV7gLiv1XWCqqBHNcWm, belonging to Binance User ID 193278016 ("Donor 2"), hereinafter referred to as **Target Property 45**, on April 29, 2025. The FBI had previous knowledge of the Donor 2 Binance Account, as it had previously received 20,200 USDT in funds traceable to the network of suspected HAMAS consolidation wallets and funded in part by [REDACTED], which is duplicated below.

88. **Target Property 45** was frozen by Binance with 27,237.67809057 USDT in the account. Records from Binance showed that Donor 2, who controls **Target Property 45**, was a resident [REDACTED] account records showed that this user has received and sent over 1,000,000 USDT since the beginning of 2024 to many different destinations. Based on my training and experience, I know this financing network has previously utilized virtual currency exchange accounts and over the counter brokers to hide the destination of the donated funds and exchange the donated virtual currency for fiat money. Due to the large amount of virtual currency and the volume of transactions passing through **Target Property 45**, I believe the account holder controlling **Target Property 45** launders illicit funds for profit by receiving and sending large amounts of USDT.

89. Similarly, Binance, which has provided reliable information in the past, notified me on June 27, 2025 of a Binance deposit of 20,000 USDT from what was assessed to be a consolidation point in the donation network. Binance independently identified [REDACTED] and noted that 33 addresses appearing to have received donations sent their funds to consolidation wallets using [REDACTED] These funds were then exchanged for Binance Coin using Bridgers[.]xyz. The Binance Coin was then forwarded through several different wallets before it stopped at the address 0x52144245809285A91c46B445fbbB15E6FB010d86, hereinafter

referred to as **Target Property 46**. Binance proactively froze funds in this account as well. A graphical representation of this movement connected to [REDACTED] is shown below.



90. **Target Property 46** was frozen by Binance with 23,795.98832405 USDT in the account. Records from Binance showed that the user controlling **Target Property 46** was a [REDACTED] national and resident of [REDACTED]. Account records showed that this user had received the subject 20,000 USDT deposit on June 23, 2025, but 19,999 USDT was withdrawn several hours later. However, Binance still froze funds in the account due to the activity exhibited in support of the terrorist financing network. Similar to **Target Property 45**, **Target Property 46** received over 1,000,000 USDT and subsequently sent over 940,000 USDT since the beginning of 2025. In your affiant's training and experience, the large amount of virtual currency and the volume of transactions passing through **Target Property 46**, are consistent with the conclusion that the

account holder controlling **Target Property 46** launders funds for profit, receiving and sending large amounts of USDT, and has done so to benefit HAMAS, an FTO.

91. The above Binance user accounts are included in the requested seizure warrant based on the deposits they received from this HAMAS financing network. In your affiant's training and experience, there is probable cause to believe that **Target Properties 45 and 46**, belong to professional launderers used by HAMAS to obfuscate the flow of large consolidations of funds.

92. In your affiant's training and experience, the cryptocurrency contained in **Target Properties 40 through 46** is being used to provide material support to HAMAS and: (i) derives from funds intended for HAMAS, (ii) is comingled with other funds to obscure the source and destination, (iii) is being used to further money laundering efforts to conceal contributions to HAMAS, or (iv) is involved with money laundering offenses, to include funds being laundered, commissions, fees, and other property used to facilitate money laundering for HAMAS.

SEIZURE PROCEDURE FOR THE TARGET PROPERTIES

93. A protective or restraining order issued pursuant to 21 U.S.C. § 853(e) would be insufficient to ensure the availability of the funds in the Target Addresses. Virtual currency can be transferred faster than traditional bank funds, and once transferred, generally cannot be recalled to an original wallet. Moreover, there is a risk that the funds may be moved to a location where no forfeiture or seizure would be possible, at which point the funds could be further laundered into a "privacy" (i.e., untraceable) virtual currency. Thus, a seizure warrant is the only means to reasonably assure the availability of the funds in the Target Properties for forfeiture.

94. Based on the forgoing, I request that the Court issue the proposed seizure warrant. Because the warrant will be served on Tether and Binance, who will then collect the funds at a

time convenient to them and provide the seized funds to the Government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

95. Should this seizure warrant be granted, law enforcement intends to work with the providers listed above in Paragraph 1 to seize the funds contained within the Target Properties by transferring the funds (or the equivalent value of currently frozen funds) to U.S. government-controlled virtual currency wallets.

96. The seized funds will remain in the custody of the U.S. government pending completion of the forfeiture proceedings, to ensure that access to or manipulation of the forfeitable property cannot be made absent court order or, if forfeited to the United States, without prior consultation by the United States.

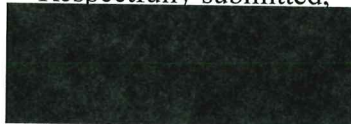
REQUEST TO SUBMIT WARRANT BY TELEPHONE
OR OTHER RELIABLE ELECTRONIC MEANS

97. I respectfully request, pursuant to Rules 4.1 and 41(d)(3) of the Federal Rules of Criminal Procedure, permission to communicate information to the Court by telephone in connection with this application for a Seizure Warrant. I submit that staff from the U.S. Attorney's Office or the National Security Division are capable of identifying my voice and telephone number for the Court.

CONCLUSION

98. Based on the forgoing, I request that the Court issue the proposed seizure warrants. Because the warrants will be served on the virtual asset service providers, which will then collect the funds at a time convenient to them and transfer those funds to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on October 10, 2025.



MOXILA A. UPADHYAYA
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1: PROPERTY TO BE SEIZED

Pursuant to this warrant, Tether Limited (“Tether”) shall provide the law enforcement officer/agency serving this document with the equivalent amount of USDT tokens that are currently associated with the virtual currency addresses referenced below. Tether shall effectuate this process by (1) burning the USDT tokens currently associated with the virtual currency addresses referenced below and (2) reissuing the equivalent value of USDT tokens to a U.S. law enforcement-controlled virtual currency address. That U.S. law enforcement-controlled virtual currency address will be supplied to Tether via separate cover. Tether shall provide reasonable assistance in implementing the terms of this seizure warrant and take no unreasonable action to frustrate its implementation.

- TGjgiiXSft9X3Q2894S1hLBxRx9icfKv74 (“Target Property 40”)
- TE3RXGtd6YJzkDtv9CWDzLFbRbd8WHWUBB (“Target Property 41”)
- TXvK7Bikg9To8G78DtM6JK8jWwNTAxJkGT (“Target Property 42”)
- TR4U6oY95e2wQLYe9izoCt9hsAHVqiuFWs (“Target Property 43”)
- TVyENJr9iRdV4sqrbquoXX5StjYvXYhK9t (“Target Property 44”)

ATTACHMENT A-2: PROPERTY TO BE SEIZED

Pursuant to this warrant, Nest Services Limited (“Binance”) shall send the entire contents of the virtual currency balances held on their platform and contained within their respective wallets and/or on their respective exchanges associated with the Binance User Identification Numbers referenced below (“SUBJECT ACCOUNTS”) and provide the property to the law enforcement officer serving the warrant in a reasonably practicable manner. Binance shall provide reasonable assistance in implementing the terms of this seizure warrant and take no unreasonable action to frustrate the implementation of it. Binance shall send the property from the SUBJECT ACCOUNTS to securely established law enforcement-controlled virtual currency wallet(s) provided by the FBI which will be supplied to Binance via separate cover. The SUBJECT ACCOUNTS are:

- 193278016 (“Target Property 45”) (TMsBHJcchJXbYxssV7gLiv1XWCqqBHNcWm)
- 1057117034 (“Target Property 46”) (TKmPwAJejTGPBRZptfkfyqPvCbSk2HVcdK)