

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,

Plaintiff,

v.

FIFTY-THREE VIRTUAL CURRENCY
ACCOUNTS,

ONE HUNDRED TWENTY-SEVEN
VIRTUAL CURRENCY PROPERTIES,

FIVE ACCOUNTS HELD AT
FINANCIAL INSTITUTION 1,

THE ALQASSAM.NET DOMAIN,

THE ALQASSAM.PS DOMAIN,

-- and --

THE QASSAM.PS DOMAIN

Defendants.

Civil Action No. 20-cv-2227

UNITED STATES' VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

COMES NOW, Plaintiff the United States of America, by and through the United States Attorney for the District of Columbia, and brings this Verified Complaint for Forfeiture *In Rem* against the defendant properties, namely: fifty-three virtual currency accounts (**Defendant Properties 1, 2, 3, 131 through 180**), one hundred and twenty-seven virtual currency properties (**Defendant Properties 4 through 130**), five accounts held at Financial Institution 1 (**Defendant Properties 181 through 185**), the alqassam.net domain (**Defendant Property 186**), the alqassam.ps domain (**Defendant Property 187**), and the qassam.ps domain (**Defendant Property**

188) collectively, the “**Defendant Properties**”, which are listed in Attachment A. The United States alleges as follows in accordance with Rule G(2) of the Federal Rules of Civil Procedure, Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions.

NATURE OF ACTION AND THE DEFENDANTS *IN REM*

1. This *in rem* forfeiture action arises out of an investigation by the Internal Revenue Service – Criminal Investigation’s Cyber Crimes Unit (“IRS-CI”), Homeland Security Investigations (“HSI”), and Federal Bureau of Investigation (“FBI”) into online fundraising activities conducted by Hamas’s military wing, the al-Qassam Brigades. The fundraising was facilitated, in part, through the use of social media and the organization’s three official websites, **Defendant Property 186, Defendant Property 187, and Defendant Property 188** (collectively the “al-Qassam Brigades’ Websites”).

2. The owners of the Defendant Properties, as well as the users and administrators of the al-Qassam Brigades’ Websites, knowingly and willfully conspired with others, and acted individually, to commit the following violations: laundering monetary instruments, in violation of 18 U.S.C § 1956(a)(2), operating unlicensed money transmitting businesses, in violation of 18 U.S.C. § 1960, and providing material support or resources to a designated foreign terrorist organization, namely Hamas, in violation of 18 U.S.C § 2339B. As such, the Defendant Properties are subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A), as property involved in, or traceable to, a financial transaction in violation of 18 U.S.C. §§ 1956 or 1960.

3. The Defendant Properties are also subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(G)(i), as all assets, foreign or domestic, or sources of influence, of Hamas, which is a designated foreign terrorist 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 as assets affording any person a source of influence over any such entity or organization.

JURISDICTION AND VENUE

4. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1345 and 1355. These statutes confer original jurisdiction to district courts of all civil actions, suits, or proceedings commenced by the United States and any action for the forfeiture of property incurred under any act of Congress.

5. Venue is proper pursuant to 28 U.S.C. §§ 1355(b)(1)(A) & (b)(2) and 28 U.S.C. § 1395(c).

FACTS GIVING RISE TO FORFEITURE

I. DEFINITION OF TERMS

A. Bitcoin

6. Bitcoin (“BTC”) is a decentralized virtual currency, which is supported by a peer-to-peer network. All transactions are posted to a public ledger, called the Blockchain (which can be seen at <https://Blockchain.info>). Although transactions are visible on the public ledger, each transaction is only listed by a complex series of numbers that do not identify the individuals involved in the transaction. This feature makes BTC pseudo-anonymous; however, it is possible to determine the identity of an individual involved in a BTC transaction through several different tools that are available to law enforcement. For this reason, many criminal actors who use BTC to facilitate illicit transactions online (*e.g.*, to buy and sell drugs or other illegal items or services) look for ways to make their transactions even more anonymous.

7. A BTC address is a unique token; however, BTC is designed such that one person may easily operate many BTC accounts. Like an e-mail address, a user can send and receive BTC with others by sending BTC to a BTC address. People commonly have many different BTC

addresses and an individual could theoretically use a unique address for every transaction in which they engage. A BTC user can also spend from multiple BTC addresses in one transaction; however, to spend BTC held within a BTC address, the user must have a private key, which is generated when the BTC address is created and shared only with the BTC-address key's initiator. Similar to a password, a private key is shared only with the BTC-address key's initiator and ensures secured access to the BTC. Consequently, only the holder of a private key for a BTC address can spend BTC from the address. Although generally the owners of BTC addresses are not known unless the information is made public by the owner (for example, by posting the BTC address in an online forum or providing the BTC address to another user for a transaction), analyzing the Blockchain can sometimes lead to identifying both the owner of a BTC address and any other accounts that the person or entity owns and controls.

8. BTC is often transacted using a virtual-currency exchange, which is a virtual-currency trading platform and bank. Virtual currency exchanges typically allow trading between the U.S. dollar, other foreign currencies, BTC, and other digital currencies. Many virtual-currency exchanges also act like banks and store their customers' BTC. Because these exchanges act like banks, they are legally required to conduct due diligence of their customers and have anti-money laundering checks in place. Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act, codified at 31 U.S.C. § 5311 *et seq.*, and must collect identifying information of their customers and verify their clients' identities.

9. BTC is just one of the virtual currencies and tokens available for trading on most virtual currency exchanges. Some of the other major virtual currencies, based on market capitalization, include Ethereum (ETH), XRP, EOS, Tether (USDT), BSV, Stellar (XLM), and LEO.

B. Blockchain Analysis

10. While the identity of the BTC address owner is generally anonymous (unless the owner opts to make the information publicly available), law enforcement can identify the owner of a particular BTC address by analyzing the Blockchain. The analysis can also reveal additional addresses controlled by the same individual or entity. For example, a user or business may create many BTC addresses to receive payments from different customers. When the user wants to transact the BTC that it has received (for example, to exchange BTC for other currency or to use BTC to purchase goods or services), it may group those addresses together to send a single transaction. Law enforcement uses sophisticated, commercial services offered by several different Blockchain-analysis companies to investigate BTC transactions. These companies analyze the Blockchain and attempt to identify the individuals or groups involved in the BTC transactions. Specifically, these companies create large databases that group BTC transactions into “clusters” through analysis of data underlying BTC transactions.

11. Through numerous unrelated investigations, law enforcement has found the information provided by these companies to be reliable. The third-party Blockchain-analysis software utilized in this case is an anti-money laundering software used by banks and law enforcement organizations worldwide. This third-party Blockchain analysis software has supported many investigations, and been the basis for numerous search and seizure warrants, and as such, has been found to be reliable. Computer scientists have independently shown that they can use “clustering” methods to take advantage of clues in how BTC is typically aggregated or split up to identify BTC addresses and their respective account owners.

12. Since the Blockchain serves as a searchable public ledger of every BTC transaction, investigators may trace transactions to BTC exchangers. Because those exchanges collect

identifying information about their customers, subpoenas or other appropriate process submitted to these exchangers can, in some instances, reveal the true identity of the individual responsible for the transaction.

C. Money Service Businesses

13. 18 U.S.C. § 1960(a) provides in relevant part that “[w]hoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business” shall be guilty of a federal offense. The term “money transmitting business” is defined as “includ[ing] transferring funds on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier.” 18 U.S.C. § 1960(b)(2).

14. Under 18 U.S.C. § 1960(b)(1)(B), it is a violation to operate a money transmitting business without “comply[ing] with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section.” In turn, 31 U.S.C. § 5330(a)(1) requires anyone who owns or controls a money transmitting business to register with the Secretary of the Treasury.

15. Federal regulations issued pursuant to 31 U.S.C. § 5330 define a category of “Money services businesses” (“MSBs”) which include “Money transmitter[s].” 31 C.F.R. § 1010.100(ff)(5). Money transmitters are defined broadly, and include anyone who “accept[s] . . . currency, funds, or other value that substitutes for currency from one person and . . . transmit[s] . . . currency, funds, or other value that substitutes for currency to another location or person by any means,” as well as “[a]ny other person engaged in the transfer of funds. 31 C.F.R. § 1010.100(ff)(5)(i)(A)-(B). All MSBs are required to register with the Financial Crimes

Enforcement Network (“FinCEN”), a division of the U.S. Department of Treasury, unless specific exemptions apply. 31 C.F.R. § 1022.380(a)(1).

7. Virtual currency exchangers qualify as a “money transmitting business” within the meaning of both 18 U.S.C. § 1960(b)(1) and 31 U.S.C. § 5300. *See United States v. Harmon*, No. 19-CR-395 (BAH) (D.D.C. July 24, 2020); *United States v. E-Gold, Ltd.*, 550 F. Supp. 2d 82, 87-97 (D.D.C. 2008).

16. FinCEN has issued formal guidance classifying virtual currency exchangers as MSBs, and thus subject to the federal registration requirement. *See Dep’t of the Treasury FinCEN Guidance, Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (Mar. 18, 2013), at 3 (“An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason *is* a money transmitter under FinCEN’s regulations, unless a limitation to or exemption from the definition applies to the person.”) (emphasis in original).

17. Virtual currency exchangers abroad are covered by 18 U.S.C. § 1960, and thereby must comply with the registrations requirements of 31 U.S.C. § 5300, if, as part of their money transmitting business, they “transfer[] funds on behalf of the public by any and all means including but *not limited to transfers within this country or to locations abroad by wire*, check, draft, facsimile, or courier.” *See* 18 U.S.C. § 1960(b)(2) (emphasis added). Notably, the statute explicitly contemplates the regulation of foreign commerce under its purview, defining “money transmitting businesses,” as those affecting “interstate *or foreign commerce*.” *See* 18 U.S.C. § 1960(b)(1) (emphasis added).

18. FinCEN has also issued formal guidance classifying “foreign entities” who engage in MSB “activities in the United States” as subject to the federal registration requirement. *See*

Dep't of the Treasury FinCEN Guidance, FinCEN Clarifies Money Services Businesses Definitions Rule Includes Foreign-Located MSBs Doing Business in U.S., FIN-2011-3 (Jul. 18, 2011), at 1. “This requirement arose out of the recognition that the Internet and other technological advances make it increasingly possible for persons to offer MSB services in the United States from foreign locations.” *Id.* at 2.

II. CURRENT INVESTIGATION OF TERRORIST FUNDING

A. Designation of Hamas and the al-Qassam Brigades

19. On October 8, 1997, by publication in the Federal Register, the United States Secretary of State designated Hamas as a Foreign Terrorist Organization (“FTO”) pursuant to 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. As part of this designation, the Secretary of State listed a number of aliases for HAMAS, including, 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.

20. The Office of Foreign Assets Control (“OFAC”) has also targeted Hamas with three sanctions programs, codified at 31 C.F.R. Part 594, 31 C.F.R. Part 595, and 31 C.F.R. Part 597.

21. The State Department’s 2018 Country Report on Terrorism noted that the al-Qassam Brigades branch of Hamas had conducted numerous attacks, including large-scale suicide bombings against civilian targets in Israel. This annual reporting also explains that Hamas and its components, including the al-Qassam Brigades, rely heavily on donations from Palestinian expatriates around the world, including in North America.

B. Terrorist Fundraising Campaign

22. The al-Qassam Brigades began a BTC fundraising campaign in early 2019. This campaign progressed in three stages as outlined below. In stage one, the al-Qassam Brigades solicited donations from supporters and requested BTC be sent to a single BTC address, **Defendant Property 1**, hosted at a U.S.-based BTC exchange. In stage two, the al-Qassam Brigades requested donations be sent to a single BTC address, **Defendant Property 4**, located within the al-Qassam Brigades' controlled infrastructure, rather than at a third-party hosted BTC exchange. Finally, in stage three, the al-Qassam Brigades developed and relied on technology that generated new unique BTC addresses for each donation, specifically, **Defendant Properties 14-130**.

a. STAGE ONE

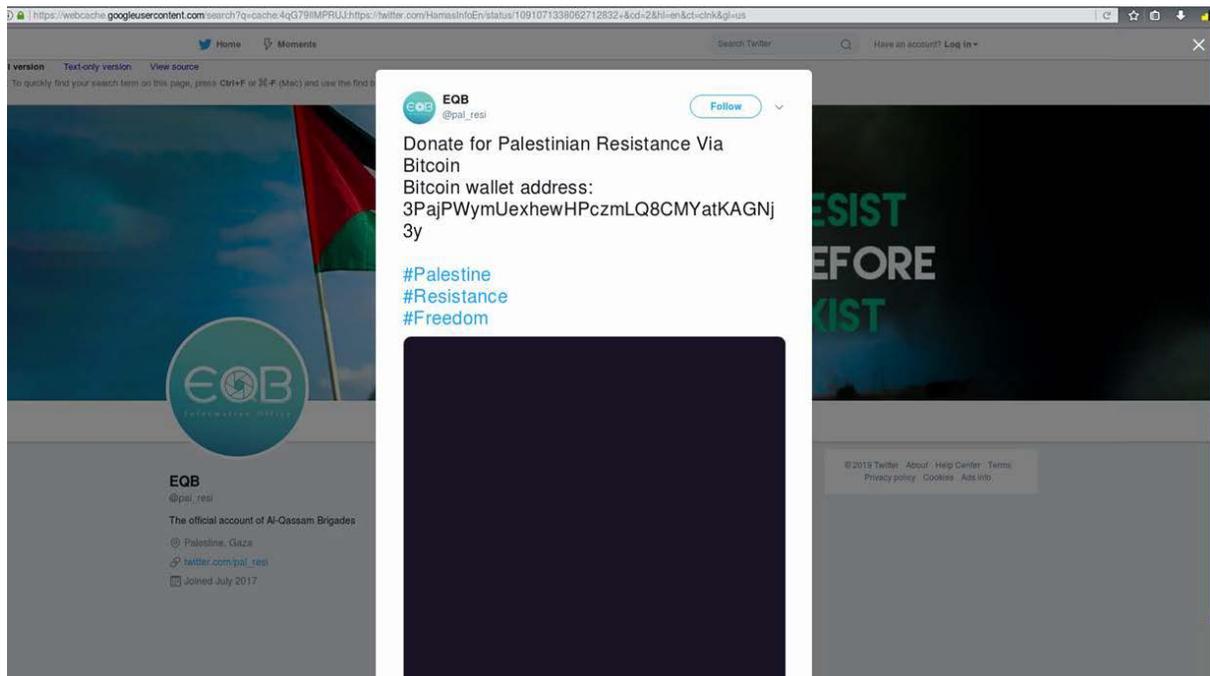
23. Stage one involved the following **Defendant Properties**, as described below:

Defendant Property #	Account Identifier
1	3PajPWymUexhewHPczmLQ8CMYatKAGNj3y
2	3LrjAKNfnyX2BGmor6ZNxvZutM1Q3KEejZ
3	1HrPF5CPqJiWbkroxheU5LcHL7bZNDi76v
177	1D9jDMKhss9vtmeRWeBA6tmts52JoQyezk
178	1JJrTJgxSNqEPDrRBogD7odjvCwuog9Cqb

24. On or about January 31, 2019, a user with the registered name, "alqassam brigades" opened **Defendant Property 1** at Virtual Currency Exchange 1 and was given a BTC deposit address starting with 3Paj. The user of **Defendant Property 1** provided Virtual Currency Exchange 1 with the e-mail address and a Palestinian phone number to register the account.

Defendant Property 1 was accessed from an IP addresses located within Gaza in the Palestinian territory.

25. Also on or about January 31, 2019, the al-Qassam Brigades began a public fundraising campaign, soliciting BTC donations on social media. Specifically, a Twitter account identified as the “official account of the Al-Qassam Brigades” posted a call for supporters to “Donate for Palestinian Resistance via Bitcoin.” The post displayed **Defendant Property 1**, the aforementioned BTC deposit address starting with 3Paj, as the address to which donors could send their funds to the al-Qassam Brigades.



26. That same day, on or about January 31, 2019, **Defendant Property 2** was created at Virtual Currency Exchange 1 and assigned an account number ending in 1ae06. The account was registered with a Palestinian phone number and the email address allmohbllah@gmail.com. The Palestinian IP address used to create **Defendant Property 2** resolved to the same Palestinian IP address that was used to log into **Defendant Property 1** on the same date. Additionally,

Defendant Property 1 and **Defendant Property 2** were created within a couple hours of each other, as were their respective linked email accounts. **Defendant Property 2** conducted no transactions.

27. Persons creating “burner accounts” often create multiple accounts at the same time from the same computer. **Defendant Property 2** appears to be a burner account used by the same co-conspirators seeking donations for the al-Qassam Brigades.

28. On or about May 11, 2017, **Defendant Property 3** was created at Virtual Currency Exchange 1. The account was registered using a physical address in the Palestinian territory, a verified Palestinian phone number, and was logged into from IP addresses resolving to the Palestinian territory.

29. Based on Blockchain analysis, on or about January 31, 2019, **Defendant Property 3** sent two BTC payments, each worth approximately \$1, to **Defendant Property 1**. These transactions occurred within hours of the opening of **Defendant Property 1**. These types of payments are consistent with “test transactions,” typically nominal deposits, which in this case were likely intended to confirm that **Defendant Property 1** was open and able to receive funds.

30. **Defendant Property 3** also received funds from two additional accounts that belonged to the same accountholder, **Defendant Property 177** and **Defendant Property 178**, which were held at Virtual Currency Exchange 11 and Virtual Currency Exchange 9, respectively.

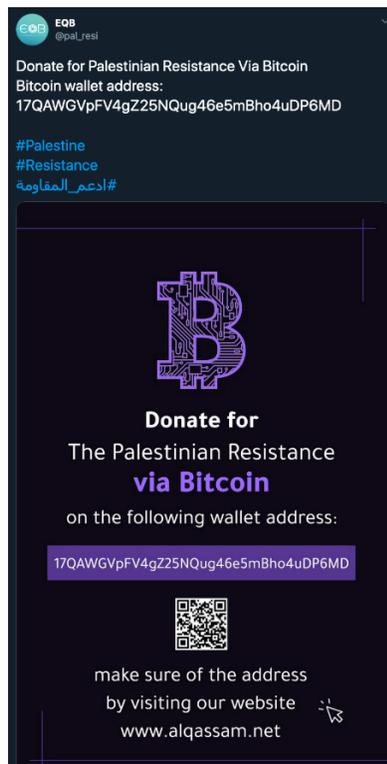
b. STAGE TWO

31. Stage two involved the following **Defendant Properties**, as described below:

Defendant Property #	Account Identifier
4	17QAWGVpFV4gZ25NQug46e5mBho4uDP6MD

5	1KDFQFnFfy9gJgXF18U3vpfeJQAeixPp1K
6	1HQhQfFPesW8znZdsdizHnA8ggvtc6NJ4k
7	1AW9z69zW2Wpg5i2gFs9YzkvZLjzDNx5VG
8	14EwXyqiB3yVLDJ1zVNevvEDpyyhBdnzjk
9	14S3GUHsqSY2am6yCPqEhb72sECUUbnRtE
10	14dRMzjmatz7zkc7iRYaitMvw4YPxXJYHf
11	1JJQceg2YZuCsJxUvAAVwU2YH4wDwxQoy6
12	1EQFWyM1gTus8cnuwHQErnaED3um1py2pF
13	19ncZQTCBfvfW5bsM7v3Pe7t6nzu4GZy4r

32. On or about February 1, 2019, the al-Qassam Brigades expanded its social media fundraising campaign, seeking additional BTC donations to be sent to a new BTC deposit address starting with 17QAW (“**Defendant Property 4**”). **Defendant Property 4** was registered using the same email account used to register **Defendant Property 1**.



33. Using commercially-available reliable third-party Blockchain analytics software, law enforcement learned that **Defendant Property 4** has been clustered (a process described above) with nine other BTC addresses, specifically, **Defendant Properties 5** through **13**. These ten BTC addresses comprise stage two, as the clustering together of BTC addresses reflects common ownership/control.

34. As of August 7, 2020, Blockchain analysis shows that the stage two operation has collected approximately 1.16938125 BTC via 65 transactions.

c. STAGE THREE

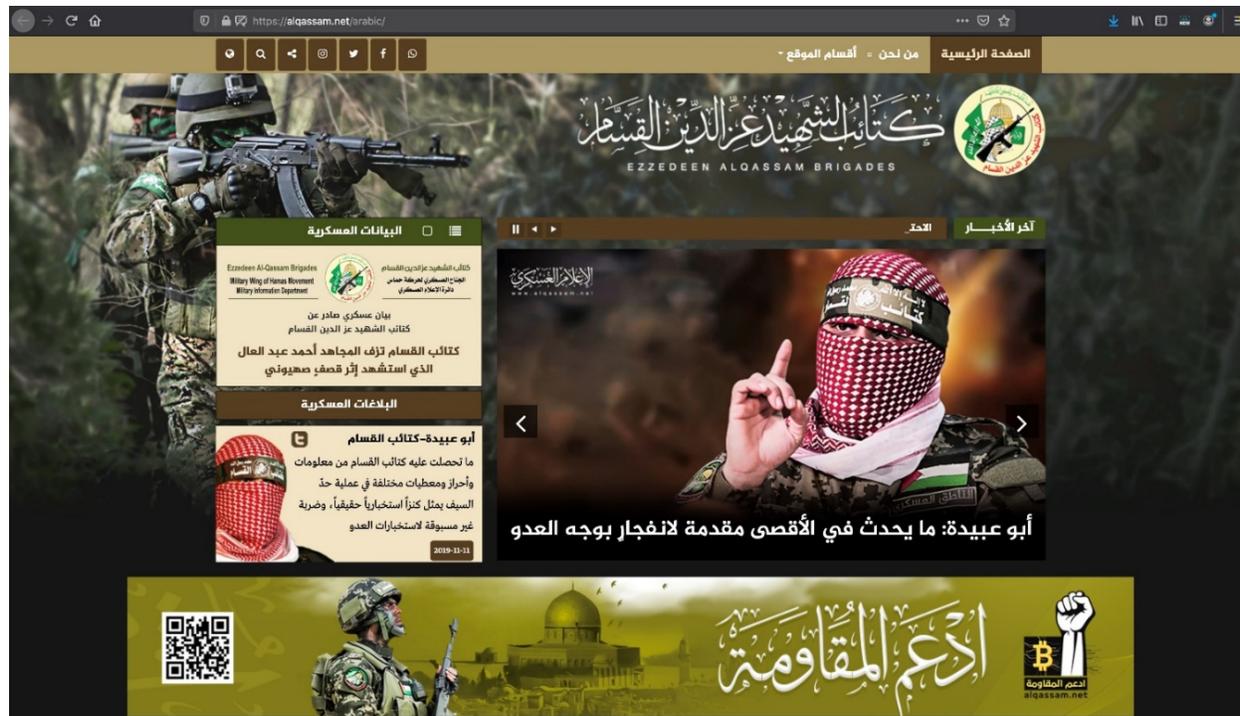
35. The first two stages relied on static BTC addresses, *i.e.*, a single fixed account number that could receive donations from anyone. Virtual currency exchanges could easily monitor the single static address on the Blockchain and evaluate their exposure to this terrorist funding campaign, and subsequently began to freeze transactions associated with these BTC addresses.

36. In stage three, the al-Qassam Brigades, instead, began providing donors on its official website, **Defendant Property 186**, which law enforcement accessed while in Washington, D.C., a dynamic BTC address system, wherein the website created a new unused BTC address for each individual wishing to fund the al-Qassam Brigades. Like an e-mail address, there is typically no charge to create a new BTC address. There are hundreds of millions of BTC addresses currently in use.

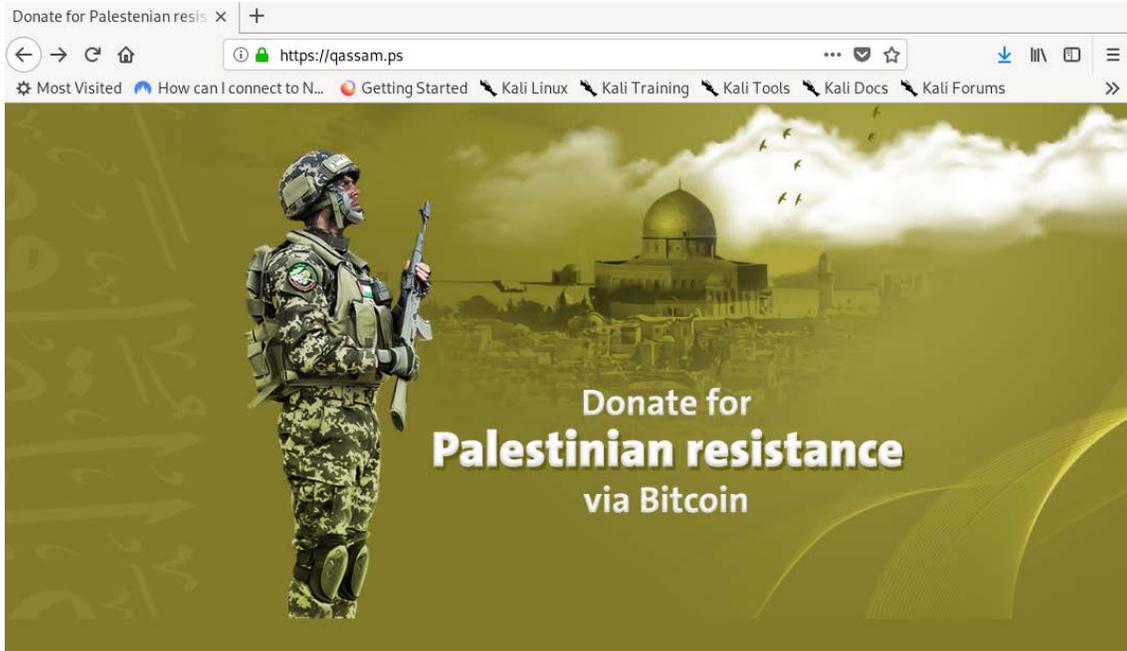
37. The al-Qassam Brigades' website included a reCAPTCHA human verification system provided by Google so that BTC addresses could not be harvested automatically. The al-Qassam Brigades also created two additional official sites located on the Palestinian domain to raise BTC for the campaign, **Defendant Property 187** and **Defendant Property 188**. All three

websites, according to subpoena, publicly available information, and search warrant returns, were registered and administered by the same individual.

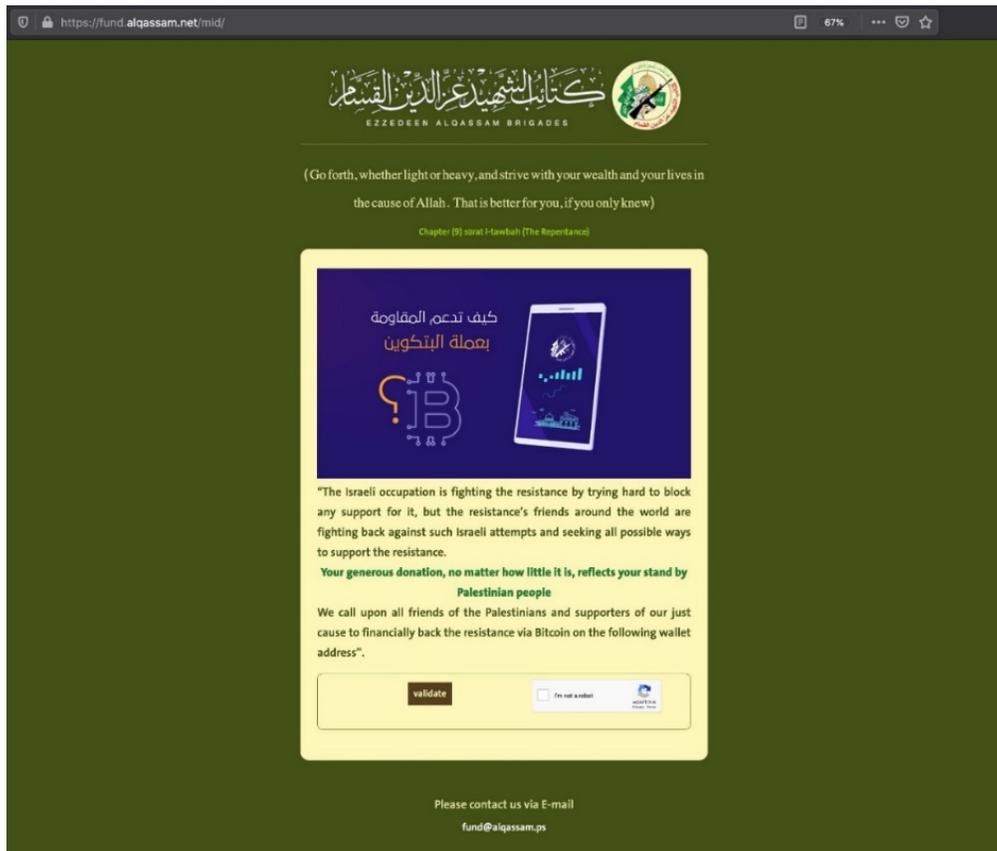
38. One of the Palestinian domain sites, **Defendant Property 187** appears identical to **Defendant Property 186**, providing the exact same information and instructions for contacting and donating to the organization.



39. The other official website, **Defendant Property 188**, while not identical, relies on the same military photographs and information as the other two websites. Additionally, it similarly seeks BTC donations, linking users, with a click on the below image, directly to **Defendant Property 187** for this purpose.



40. Clicking on the BTC symbol at the bottom right corner of the homepage of **Defendant Property 186** and **Defendant Property 187**, shown here, led to a BTC donation page embedded within the same domain. Donors clicked on this donation page, which generated 117 unique BTC addresses. These 117 addresses represent **Defendant Properties 14-130**.



41. Stage three is still active and ongoing. As of August 7, 2020, **Defendant Properties 14** through **130** received approximately 2.39361558 BTC via 124 transactions. Many of these BTC addresses clustered together within third-party Blockchain analytics software demonstrating common ownership. These Properties are identified as follows:

Defendant Property #	Account Identifier
14	31hnjnw7Xe8e183u2qffHt4qpLFLfergmF
15	31idyYGpkmev8S1Kve8TvHEXyDfEDM2saV
16	31iUH4sRXJt9F8MnnpVY1HAxUZ1qZQ4Z7x
17	31iZbakXU1arYMMyiCgceipKjUxCF19N5j
18	31jbxhdDYxkB6ULhsk7VMLsNB3KQgTREUZ
19	31k6eLZLTP1adv7EqZNkbnd8Jm1oHnULuP
20	31mnD8FtBVyHh6CCFsUwiTFHuu6RMTCjcR
21	31mUJqpqH8HLsGaxMdARTgdPHkbWbq2yuQ
22	31n5MTyfWEFFm7pXf7e9Qt2i5Ec8jKA1py
23	31nob3VbXpByQZBuvHdFF1vcwjBoSd1xJF
24	31o5C1u66MjVZMrcJHzHYuQFk9XuDUznqX
25	31osZ4w7nPC2wbezG3fhu7fraUNBeEfdyA
26	31ot27eWxmxqQtVWmpiSyuakJNKqwc4uSZ
27	31otG9J9PWZ5GuUaAFVwuzP5nrAX6sVNH8
28	31p9vft5AqYgt7uPxTXCis97zHE2E8RkTG
29	31pmPV1XpevjEUzPtmr5sDXm8s4YzTyaS2
30	31pWw13YTX5h9EY6T5hjcRDT4bDF6cQMXR
31	31pYNazDxCwnhAyVCNqpELTE66qi4KcEA5

32	31qeJQa6Y6LL74HDBe5ZkuE7GxfMvUAh7t
33	31qk3S4hqj5KfedbVo45nFdvrXQ6TnYtY2
34	31qMgW6GideWcAHTdYf4GN3UEKEzVTP6jb
35	31qv732ydN8kbUyLYbv5QBNDyHRbRqL5wo
36	31rbKDq1pwA1GLHwa82cySVrkTo1R6htMK
37	31rhvmw3BPW9bYXvV6RJ4ZuwgUP2QbN6Wp
38	31rQoLSQkVa2SQhgRByhrM5e69KaKPntpp
39	31rZQb9DM2Fz5Yqi47UTsZ3FttETRAvbeu
40	31s1NZm8S16JsedBDJcSX815ikhNCKro28
41	31spTrrz7g2nCtf7JPVFrSawiQi6SGJygU
42	31tKBTcV4bWYLEXzSwByPuJWmEnWkNUXNs
43	32LjBurh7tKVpxmhhEhfPUnKYzV7jxzane
44	33mskKAPj8RVaFcSaCDtWtpCQYNCP4dFLw
45	344Aycb4ZzEZXEf26qgbGrfYjFEqMJBn6F
46	38vt9RRxHJboCyFbTieWT1sFKxbacKeBgg
47	3AHkpUF4zgvxVxRPKNrTQyo4NrZ1PH8x5Z
48	3CafimPzKw8ZhXQyQjojD2GDNpwsaQb12J
49	3DTLocTRA6s4LyZGnSN5g4aRfLd8FVaxHh
50	3Ea4umPPeQGELifMTXWmkJAZCzijBuYtVm
51	3EaD7SfNXda1LujuB1fyi8mzuA1qmrsUAq
52	3EaGnTmpjGYRSV2KAkrpP6zg2uhPHAw15o
53	3EaKhQrXE2oZ6b74H7ML2SipNU7cdXhqDz
54	3EaPVCEnRRWZ96qJR8p6JgvgeTmGshvZRY

55	3EbyqWHMMzE96mMmB6bASnXsaGinwq7now
56	3EciaU3UgTycJvmD2KC4YG4NBoh6fqpZFU
57	3EcQ7XQXQiSS27LgV3hrvsXFntN7GxAxxf
58	3EdXMhAWLKg7PJfLbEKRCMm8Ldm6dsZDzT
59	3EeAr4pt2n9wjeFWY5XXTK1AGcmfTLG2hB
60	3Eein3xzdKxrvKQQJp5Y5H8cbqrhoEKW1N
61	3EekremuSe1bnR43w9nZMG2W7YMkbgvPEa
62	3EemNUbRZoov3jp38BZuAJhSXxnSKQRN9F
63	3EeNxvKupEyozejPEvoccaZBQN2TVTgndgP
64	3EeqkFMzUEPMpB4PZeDe1yHBmLVSiQ6QdX
65	3EeyeaD1YXwrkQGeYgo7QsoJi9tL9CZrxw
66	3EfH1Jk9JBqu6cHqXWUysRiM16HS5bjeK6
67	3EfKyF6eCRVTmvoMXPk8jUgDWfMXXAhhVq
68	3EfUV43ULkkxsezDDbfh9acBWhCNXQw3p
69	3EfYuiuGvoU6quCSD7RNHBQAngqkfjtu75
70	3EfzSMen4ds6HXTWP4FZeVZynJTSvvtUgN
71	3EgLDTol4NS51KC7LzY8rw6CsLeaoUVzzz
72	3Egn1PtQuctJViaK5E9gn2BYUZ9vkoyhQY
73	3Egrrh9KqgYYnwoTic2mGrNNqUg7H2xMzt
74	3EguPmkenPJa5ezKgRi41nnnz7JwUvexfy
75	3EWxNDQg52QH7ZXRafxU22T5XyKCtxUG8Q
76	3EX4bu9vjudVXnFEXJq7pRW7qboPLPcCpU
77	3EX9MLM6pTK6nvajFj4woTx2nT7NXBXRlZ

78	3EXBCqAR9jW2XJsGK6pAifLhZrg76vDJxF
79	3EXUxdgs5JmBTvhpCCtyYXveHXW9Ykxmc
80	3EXzujBDN5cVDeRgysMpQjyK8AZ3eZ7m5L
81	3EY8Ln5c51jwY4x7pKroCETEAK6Ch4EDVu
82	3EYc9agtyf5xjdX6gjXNXQVvxUb3UNtTzc
83	3EYwWQxei7iFcocr99LcJAa5pFtFdyQrYX
84	3EZ6VeppfgZc3bGuefA7V5g17i9BnnNVWD
85	3EZetpgN7K5jow7sv9dKQZ2tL6JfNJU4Hy
86	3EZf21ULWjqpLDtzJU1qbfqygHqaPDpdUD
87	3EZfMVxWBNBUm23HUvvaQXcET3Wbkr34oS
88	3EZG4CNSAiDchj5mU5NehxtqVZgJqj3tuN
89	3EZQYLt6XAaWgwqm6PUHAKPGcfNtt3oY6T
90	3EZvc5LA6WjchP7VWY3BohXZ6u73xo3WcE
91	3EZx1DuWqwuRhErsoZJva2ibp8FUuYjBvC
92	3Fq8LkKoJU61MVqL7HJiPR3ecEpxEmqKkU
93	3FqsDefk77P9jQKbnM9qyQiyF13JFYcHTR
94	3FqsDefk77P9jQKbnM9qyQiyF13JFYcHTR
95	3FqV49yKKscsMV3JLmEX6NBm92bdZB83SZ
96	3FqV49yKKscsMV3JLmEX6NBm92bdZB83SZ
97	3Fr2ejXvkk7ccWx4of2TTBkkN4Z8PhmBkW
98	3Fr2ejXvkk7ccWx4of2TTBkkN4Z8PhmBkW
99	3Fr4DFkumQffMD9crpSxSP4oQ2dQRA75Ev
100	3Fr4DFkumQffMD9crpSxSP4oQ2dQRA75Ev

101	3Fr9hEMfYCnRoNyd9wEBJPMVgSEgVRxFXT
102	3FraSMiSHqntVAxiAiaPaD2z2K1YMvmSu9
103	3Freatgh7mpUhSjvrzUvDR4kR23ERYu3Gz
104	3FrfgNJ6cMoLt4DvSokLRWJYhs3iR58uG6
105	3FrGKydhTg1mgrwzaBdCF2TLq6dne7sQW
106	3FrgLnW4DQWJQXkaHQm1rvH4GFk7MPpRzy
107	3Frh4A8Tecb1YFs9T64TCvE6XCqv17Mse
108	3FricPpCwRFkL7zvYBKNEYMGUQp5F7Qj47
109	3FrP22X7MGdQZX66FHDPsrMvGoxFzFxxSD
110	3FrPk5dAyqSpvs1bM43hRFHwHVmnosHw3B
111	3FrRV3hZKuBJmd9oEHuwPbq4Dq1f49yzus
112	3FrS1Vm2Vha1JrMTrGiyCxpwjvEx27cfS8
113	3FrSvZWjvDSGrRDPG6fdwEEEsUkrY65ZU7
114	3FrTayH9wkCnNkTTkfuqx7SVQQzzCQd5Cp
115	3FrUtZ3dXoGNDWejDbXanYEfZR56JyiLsT
116	3FrVsAxKhtau1kcjVY8iXQNo2i1uZD6orS
117	3FrZphLBUTm9aTiXhnZTA3piVJ4oTxjpBU
118	3FtDtZdVMY53Jjk8fCPxydXb633jFdj3wo
119	3FtHfUNd2zgSY8FNW4Aq2f88wwSYiyVacg
120	3Ftpn5gXf79Zurdf7PYGfQZiipgVqEiUkg
121	3FvrNAv5KaEWVA7o8JJKFqeCfCP28JqRDt
122	3FvV3xyheg6BWAjX8Yy6dcENRfmhMnAZ6a
123	3Fw3NTwtmk8zQuwg6s2FPniXWPKirfqAgP

124	3FWSkG5NmyXF3rqMav7piXiJUDYzKpgFRT
125	3JaDQWNPyysYRcNNQxgkwSUpApXvn3XkBW
126	3La8eKaybxVeBLDxGNSyydVRoX9ZxjrDCW
127	3LhP8JYJ77cj2eVXBasY92Z6omTyRbUdbh
128	3Ngo99WAQieMEJGf5WJz2ycH1reFkjd6yg
129	3QGyLXfEdN1iPt21toAf4qhM4zQ8zsDMMY
130	3Qms9Dk4ViL2LNfup8J5fYLXYCWsXj43Qa

42. Notably, the al-Qassam Brigades' Websites listed the email address fund@alqassam.ps as the point of contact. On or about October 24, 2019, an HSI undercover agent (UCA) e-mailed fund@alqassam.ps to ask if his/her donation would be used to "fight the occupation."

43. Later that same date, the UCA received an e-mail from fund@alqassam.ps which stated that donations would "be used to fight the occupation." The e-mail also asked the UCA to clarify the amount he/she intended to send so that "we can tell you the proper way to send."

44. On or about October 25, 2019, the UCA sent an e-mail to fund@alqassam.ps and asked the sender to "describe how my money will be used." The UCA further explained that he/she intended to donate \$1,100.

45. On or about October 27, 2019, the UCA received an e-mail from fund@alqassam.ps which stated that "your donation will make difference as no jihad will be committed without money for buying weapons and training mujahideen. Moreover, the doors of jihad are many: by word, by money, by fighting, etc." Furthermore, the e-mail indicated that donations could be sent via MoneyGram or Western Union.

III. INFRASTRUCTURE OF THE AL-QASSAM BRIGADES' WEBSITES

46. During the course of the investigation, law enforcement discovered five accounts held at Financial Institution 1, **Defendant Properties 181** through **185**, which were linked to the al-Qassam Brigades' Websites and supporting infrastructure. As detailed below, these accounts either attempted to fund the server companies hosting the al-Qassam Brigades Websites or are linked to the email accounts underlying the al-Qassam Brigades' Websites.

Defendant Property #	Account Ending	Email Address
181	40816	Hamas Email 1
182	17365	Hamas Email 1 Hamas Email 2
183	01709	Hamas Email 2 Hamas Email 3
184	08539	Hamas Email 4
185	52104	Hamas Email 4

47. These Defendant Properties were utilized to support, maintain, and finance the fundraising campaign, as follows:

a. On or about June 22, 2014, **Defendant Property 181** attempted to send two payments to the website hosting companies for services provided for the al-Qassam Brigades' Websites.

b. On or about October 14, 2018, **Defendant Property 182** was registered with Financial Institution 1 using Hamas Email 1 and Hamas Email 2. These two email addresses are directly linked to the al-Qassam Brigades' Websites. On or about December

24, 2018, **Defendant Property 182** attempted to pay an outstanding website hosting service invoice relative to the al-Qassam Brigades' Websites.

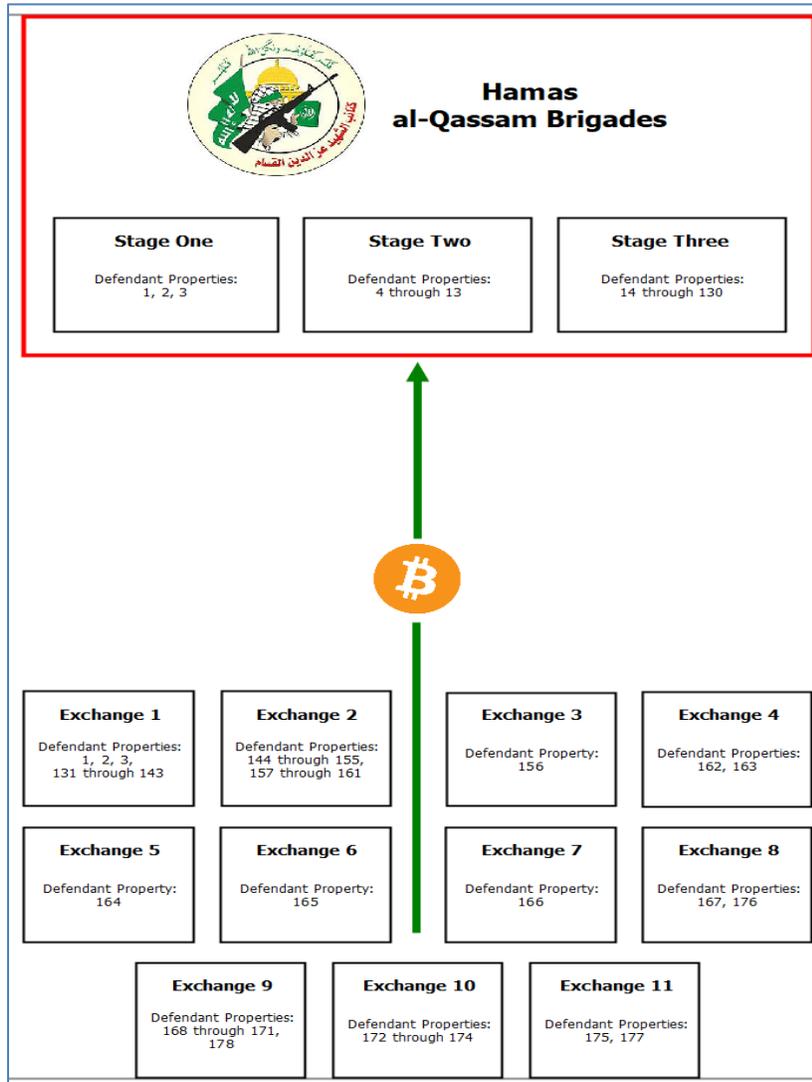
c. On or about March 24, 2014, **Defendant Property 183** was registered with Financial Institution 1 with Hamas Email 2. On or about June 22, 2014 and June 25, 2014, **Defendant Property 183** was used in an attempt to pay for website hosting services relative to the al-Qassam Brigades' Websites.

d. On or about December 5, 2018, **Defendant Property 184** was registered with Financial Institution 1 with Hamas Email 4. On or about December 5, 2018 and May 17, 2019, **Defendant Property 184** attempted to make two payments to a web design company.

e. On or about May 17, 2019, **Defendant Property 185** was registered with Financial Institution 1 with Hamas Email 4.

IV. ACCOUNTS OF DONORS TO THE FUNDRAISING CAMPAIGN

48. Throughout all three stages of the al-Qassam Brigades' fundraising campaign, the terrorist organization received donations from cryptocurrency accounts located at a variety of virtual currency exchanges. As visualized in the chart below, **Defendant Properties 131** through **178** sent virtual currency to the al-Qassam Brigades during one or more of the three stages of the BTC fundraising campaign.



a. **Virtual Currency Exchange 1:**

49. The following donor accounts are located at Virtual Currency Exchange 1:

Defendant Property #	Account Identifier
131	17cZ7CBhSPHn2gDkfNgrwNmHFDDHX7zC6q
132	1J6665h8Njpva6crm1VSFwW8BTtoNFxaPxz
133	1GeLggwn8GqtTW6CYFUwerybHkzcNqPqaX

134	1Jp1Kwn43qzHWt7bGMdgZS9ZPbTi7rK9AY
135	1MgudcZEMXpB8uXUswuGHgDBTNmUZ8ZkZD
136	1PmAgUZXXVvKMRcS37Hu2XVqdkovKG8ZPTk
137	1FUgt1eY69Ric3oaqtNK1xUex7dqph1eEv
138	3HB3GQhNxfvPYKBYfUZwUVpSatqE8tHBb
139	3QqerQBe5duLc9YwqvKvDPAc3TJZxcfrsw
140	3E8yaNXEKQnnFMvnyyrwxam9DaqNxHpFzP
141	3FeZrRq9nisxeR4RxBdj4DnhJSsABtGBAC
142	119Yw1qsUihJmBu68gcqgN36CrGy92d4aNx
143	32sVYnjTbnULtPKT8wuSNc7mzdwyuDDuAr

50. **Defendant Properties 131** through **140** were registered at Virtual Currency Exchange 1, under one account, using the same email address. During the approximate period of April 3, 2019 to May 6, 2019, this account at Virtual Currency Exchange 1 containing **Defendant Properties 131** through **140** sent approximately 0.0035672 BTC via four transactions to **Defendant Properties 34, 38, 39, and 80**, all of which, as noted above, were generated by the al-Qassam Brigades during stage three.

51. During the approximate period of May 7, 2019 to June 23, 2019, **Defendant Property 141**, another account at Virtual Currency Exchange 1, sent approximately 0.01641437 BTC via six transactions to **Defendant Properties 52, 65, 55, 90, 63, and 89**, which as noted above were generated by the al-Qassam Brigades during stage three. This funding of the al-Qassam Brigades, was the **Defendant Property 141**'s only activity.

52. **Defendant Properties 142** and **143** were registered at Virtual Currency Exchange 1, under one account, using the same email address. On or about March 24, 2019, an account at

Virtual Currency Exchange 1 holding **Defendant Properties 142** and **143** sent approximately 0.00182397 BTC to **Defendant Property 18**, which as noted above was generated by the al-Qassam Brigades during stage three.

b. **Virtual Currency Exchange 2:**

53. The following donor accounts are located at Virtual Currency Exchange 2:

Defendant Property #	Account Identifier
144	13gGNrqWGPN5XxYNnceWEgGykuHuaFhPFM
145	1LuGcrfVyQ8KK1QuQysZcgoRtg7nuU55DH
146	User ID: 35764207
147	1DjYVV19zAuJPcXjn44is2CsAn4sW4it5W
148	15WrJ9vkvw46HGaD9PKpDLkGD6MCX8CEVR
149	14sXBGZZzeunJuyyA1fJY4tKyC5RM7WYTP
150	1LGcSmCwR2eMurxgwLeJtV9iRoLHCvNv3G
151	1Fyyfjqjo4pvxwv6yqW5FrzrNspsYrX6ErX
152	User ID: 20920319
153	1P49duqmF5PwRSEpmL13F9QS8y3jVe4zjW
154	1BU8uxGuoFeATAey8XG91Q6Ux23tTTeYyx
155	1DPuLoyzjjTsbGFncWfu7eK52uYg1qFHtr
157	User ID: 22237397
158	1XD6XifgGCsvcGBUzXqpNNnvC5j3y8gey
159	133sCL2aCviV8N1TLngFGco7CDhHDmwChR
160	1A55bZqCNtFgASJHG4FXTNiAsU3jTt7DVo

161	1B7etAU8bG848QNXJjpe9XH9a1WrcWFm2Q
-----	------------------------------------

54. On or about February 1, 2019, **Defendant Property 144**, an account at Virtual Currency Exchange 2, sent approximately 0.0295 BTC to **Defendant Property 1**, which as noted above was the account registered to “alqassam brigades” at Virtual Currency Exchange 1 that was used during stage one.

55. On or about January 31, 2019, **Defendant Property 145**, an account at Virtual Currency Exchange 2, sent approximately 0.1428639 BTC to **Defendant Property 1**.

56. On or about February 1, 2019, **Defendant Property 146**, an account at Virtual Currency Exchange 2, sent approximately 0.13747974 BTC to **Defendant Property 1**.

57. On or about January 31, 2019, **Defendant Property 147**, an account at Virtual Currency Exchange 2, sent approximately 0.03130579 BTC to **Defendant Property 1**.

58. On or about January 1, 2019, **Defendant Property 148**, an account at Virtual Currency Exchange 2, sent approximately 0.01112477 BTC to **Defendant Property 1**. Additionally, **Defendant Property 148** sent approximately 0.00765096 via two transactions to **Defendant Property 4**, which as noted above was the BTC address used by al-Qassam Brigades during stage two.

59. On or about February 1, 2019, **Defendant Property 149**, an account at Virtual Currency Exchange 2, sent approximately 0.01058924 BTC to **Defendant Property 1**.

60. On or about April 4, 2019, **Defendant Property 150**, an account at Virtual Currency Exchange 2, sent approximately 0.42139 BTC to **Defendant Property 32**, which as noted above was generated by the al-Qassam Brigades’ Websites during stage three.

61. On or about April 23, 2019, **Defendant Property 151**, an account at Virtual Currency Exchange 2, sent approximately 0.473 BTC to **Defendant Property 150**. Network logs

from Virtual Currency Exchange 2 revealed that **Defendant Property 150** and **Defendant Property 151** were logged into using the same devices from identical IP addresses on at least three occasions, April 23, April 26, and May 22, 2019. The overlap of logins at the same period of the BTC transfer indicates common control and related involvement in this scheme.

62. On or about February 3, 2019, **Defendant Property 152**, an account at Virtual Currency Exchange 2, sent approximately 0.01542738 BTC to **Defendant Property 4**.

63. On or about February 4, 2019, **Defendant Property 153**, an account at Virtual Currency Exchange 2, sent approximately 0.1338358 BTC via two transactions to **Defendant Property 4**.

64. On or about February 28, 2019, **Defendant Property 154**, an account at Virtual Currency Exchange 2, sent approximately 0.01604317 BTC to **Defendant Property 4**.

65. On or about February 5, 2019, **Defendant Property 155**, an account at Virtual Currency Exchange 2, sent approximately 0.03448398 BTC to **Defendant Property 4**. Notably, the owner of **Defendant Property 155** did not provide identifying information upon opening the account.

66. On or about March 13, 2019, **Defendant Property 157**, an account at Virtual Currency Exchange 2, conducted its only transaction by sending approximately 0.00988427 BTC to a BTC address starting with 17oT. Approximately thirty-five minutes later, BTC address 17oT conducted its only transaction, sending approximately 0.00983953 BTC to **Defendant Property 4**.

67. On or about March 24, 2019, **Defendant Property 158**, an account at Virtual Currency Exchange 2, sent approximately 0.0059799 BTC to a BTC address starting with 1Ewb. Less than an hour later, BTC address 1Ewb sent approximately 0.00983953 BTC to **Defendant**

Property 14, which, as noted above was generated by the al-Qassam Brigades' Websites during stage three.

68. On or about February 5, 2019, **Defendant Property 159**, at account at Virtual Currency Exchange 2, conducted its only transaction by sending approximately 0.00932416 BTC to **Target Property 51**, which, as noted above was generated by the al-Qassam Brigades' Websites during stage three.

69. On or about May 26 and 28, 2019, **Defendant Property 160**, an account at Virtual Currency Exchange 2, sent approximately 0.0058 BTC and 0.00580817 BTC, respectively, to **Defendant Property 84**, an address also generated during stage three.

70. On or about April 1, 2019, **Defendant Property 161**, an account at Virtual Currency Exchange 2, conducted its only transaction by sending approximately 0.03675106 BTC to a BTC address starting with bc1q. Approximately forty minutes later, BTC address bc1q sent approximately 0.03743901 BTC to **Defendant Property 29**, an address generated by the al-Qassam Brigades' Websites during stage three.

c. **Virtual Currency Exchange 3:**

71. The following donor account is located at Virtual Currency Exchange 3:

Defendant Property #	Account Identifier
156	34vKeiCwwu5guBZhr4J8RbnKTus8q1j7Sa

72. On or about March 11, 2018, **Defendant Property 156**, an account created with the same phone number and email address as **Defendant Property 155**, a donor account at Virtual Currency 2, was created at Virtual Currency Exchange 3. As stated above, the owner of **Defendant Property 155** did not, and was not required to, provide identifying information to Virtual Currency

Exchange 2. This was not the case, however, with Virtual Currency 3. Rather, upon opening the account, the owner had to provide Virtual Currency Exchange 3 with personally identifying information, to include a name and photo ID. Between March 29, 2018 and May 5, 2018, **Defendant Property 156** sent approximately 0.28121121 BTC to **Defendant Property 155**. By purchasing BTC at Virtual Currency Exchange 3 and then sending it the BTC to **Defendant Property 155**, which did not require personally identifying information to create, the accountholder could layer and obfuscate payments to the al-Qassam Brigades.

d. **Virtual Currency Exchange 4:**

73. The following donor accounts are located at Virtual Currency Exchange 4:

Defendant Property #	Account Identifier
162	3A2KA243cB17yFFWEcWqffTi3c9CAvq8Dh
163	3JXrtFWn7kaoz75bPqD23kPpMtKZiK3j2w

74. On or about June 17, 2019, at account at Virtual Currency Exchange 4 controlling **Defendant Properties 162** and **163** sent approximately 0.007802 BTC to a BTC address starting with 1GBm. Two days later, BTC address 1GBm conducted its only two transactions by sending a total of approximately 0.00760121 BTC to **Defendant Properties 61** and **62**, which, as noted above were generated by the al-Qassam Brigades' Websites during stage three.

e. **Virtual Currency Exchange 5:**

75. The following donor account is located at Virtual Currency Exchange 5:

Defendant Property #	Account Identifier
164	35Yn5sRoasPArcXhN3Uz2HANn34rYg7ihG

76. On or about May 12, 2019, **Defendant Property 164**, an account at Virtual Currency Exchange 5, sent approximately 0.0132432 BTC to a BTC address starting with 35Yn. Approximately ten minutes later, BTC address 35Yn sent approximately 0.00711878 BTC to **Defendant Property 83**, which, was generated during stage three by the al-Qassam Brigades' Websites, and approximately 0.00599242 BTC to a BTC address starting with 34rV. On or about June 4, 2019, BTC address 34rV sent approximately 0.00505708 BTC to **Defendant Property 57**, which was also generated during stage three.

f. **Virtual Currency Exchange 6:**

77. The following donor account is located at Virtual Currency Exchange 6:

Defendant Property #	Account Identifier
165	31mT7hQ7V6B58hfNVJchZTXP7gANpZjUjK

78. On or about March 25, 2019, **Defendant Property 165**, an account at Virtual Currency Exchange 6, sent approximately 0.54374 BTC to **Defendant Property 21**, which, as noted above was generated by the al-Qassam Brigades' Websites during stage three.

g. **Virtual Currency Exchange 7:**

79. The following donor account is located at Virtual Currency Exchange 7:

Defendant Property #	Account Identifier
166	Account at Virtual Currency 7 identified by email

80. During the approximate period of July 11, 2019 to January 17, 2020, **Defendant Property 166**, an account at Virtual Currency Exchange 7, sent approximately 0.02075 BTC via nine transactions to **Defendant Properties 70, 72, 95, 97, 117, 120, and 121**, all of which were generated by the al-Qassam Brigades' Websites during stage three.

h. **Virtual Currency Exchange 8:**

81. The following donor accounts are located at Virtual Currency Exchange 8:

Defendant Property #	Account Identifier
167	3AwD6c5H2Hp6v73Md7Aon5n6HJU5YoBpDz
176	373k2ZQFXVsCtqdFyzRj7zmtsz1aP9dWoZ

82. On or about January 25, 2019, **Defendant Property 167**, an account at Virtual Currency Exchange 8, sent approximately 0.02776332 BTC to a BTC address starting with 1KLY. On or about February 1, 2019, BTC address 1KLY sent approximately 0.00287911 BTC to **Defendant Property 1**, which as noted above, was the address used by the al-Qassam Brigades in stage one of the fundraising scheme.

83. On or about January 31, 2019, **Defendant Property 176**, an account at Virtual Currency Exchange 8, sent a total of approximately 0.01006699 BTC to a BTC address starting with 17Wq. Less than an hour later, BTC address 17Wq conducted its only transaction, sending approximately 0.00740805 BTC to a BTC address starting with 1DLf. On or about January 31, 2019, BTC address 1DLf then transferred approximately 0.0028948 BTC to **Target Property 1**.

i. **Virtual Currency Exchange 9:**

84. The following donor accounts are located at Virtual Currency Exchange 9:

Defendant Property #	Account Identifier
168	Account number: 11398678
169	1GgELQKEcqn572mvHKtzPBrjZ9L3bpKiLi
170	Account number: 11436806

171	1Eg7YSoJiqUV7ERsDXiGKExyJkkXR7NHr
-----	-----------------------------------

85. On or about February 2, 2019, **Defendant Property 168**, an account at Virtual Currency Exchange 9, sent approximately \$806.98 worth of virtual currency to **Defendant Property 1**, which as noted above, was the primary al-Qassam Brigades' account for stage one fundraising.

86. On or about February 7, 2018, **Defendant Property 169**, an account at Virtual Currency Exchange 9, sent approximately 0.24577091 BTC to a BTC address starting with 1L8a. On or about February 1, 2019, BTC address 1L8a sent approximately 0.02905279 BTC to **Defendant Property 1**. Later that same day, BTC address 1L8a sent approximately 0.0286916 BTC to **Defendant Property 4**, the al-Qassam Brigades' fundraising account for stage two.

87. On or about February 12, 2019, **Defendant Property 170**, an account at Virtual Currency Exchange 9, attempted to send approximately \$534.83 worth of virtual currency to **Defendant Property 4**. This transaction failed because it was not conducted using BTC, the only currency accepted by the al-Qassam Brigades in stage two. The donor then converted virtual currency within **Defendant Property 170** into BTC and tried once more to send the BTC to **Defendant Property 4**. The potential donor was once again unsuccessful, as Virtual Currency Exchange 9 blocked the transaction as part of its terrorist detection efforts.

88. On or about March 24, 2019, **Defendant Property 171**, an account at Virtual Currency Exchange 9, sent approximately 0.00196498 BTC to **Defendant Property 16**, which as noted above was generated by the al-Qassam Brigades' Websites during stage three.

j. **Virtual Currency Exchange 10:**

89. The following donor accounts are located at Virtual Currency Exchange 10:

Defendant Property #	Account Identifier
172	Account number: 5806702
173	Account number: 6971221
174	3QRGcu41GN8cGYkp49xrv8VB7prLkokzLk

90. On or about February 1, 2019, **Defendant Property 172**, an account at Virtual Currency Exchange 10, sent approximately 0.00012 BTC to **Defendant Property 1**.

91. On or about February 4, 2019, **Defendant Property 173**, an account at Virtual Currency Exchange 10, sent approximately \$5.87 worth of virtual currency to **Defendant Property 1**.

92. During the approximate period of April 12, 2019 to May 25, 2019, **Defendant Property 174**, an account at Virtual Currency Exchange 10, sent a total of approximately 0.004785 BTC via six transactions to **Defendant Properties 39** and **91**, which as noted above were generated by the al-Qassam Brigades' Websites during stage three.

k. **Virtual Currency Exchange 11:**

93. The following donor account is located at Virtual Currency Exchange 11:

Defendant Property #	Account Identifier
175	1Mduu84x4Wm7FWm5vgaNvtk3APhEw1661t

94. On or about February 2, 2019, **Defendant Property 175**, an account at Virtual Currency Exchange 11, sent a total of approximately 0.15659642 BTC via two transactions within 15 minutes to a BTC address starting with 182r. Within an hour, BTC address 182r sent approximately 0.086496 BTC to **Defendant Property 4** and approximately 0.0028812 BTC to

Defendant Property 12, accounts both generated by the al-Qassam Brigades during the fundraising campaign.

V. UNLICENSED MONEY SERVICE BUSINESS LINKED TO THE AL-QASSAM BRIGADES' FUNDRAISING SCHEME

95. Once the al-Qassam Brigades amassed BTC from the above donor accounts in this fundraising campaign, the organization typically converted the virtual currency to traditional fiat currency or exchanged it for something of value, such as a gift card, in order to spend the BTC.

96. At least one unlicensed money service business (“MSB”) using **Defendant Property 179** at Virtual Currency Exchange 12, served this purpose for the al-Qassam Brigades, and was linked to the terrorist fundraising scheme, as detailed below. **Defendant Property 179**, was also connected to another account at Virtual Currency Exchange 12, **Defendant Property 180**, which operated an intertwined unlicensed MSB. These two **Defendant Properties**, together conspired to launder monetary instruments and violate MSB registration requirements.

Defendant Property #	User ID
179	931770
180	2319627

97. Using Blockchain analysis, law enforcement traced at least one “cash-out” transaction from the al-Qassam Brigades to **Defendant Property 179**. Specifically, on or about February 14, 2019, approximately 0.066 BTC was sent, collectively,¹ from **Defendant Property 4**, **Defendant Property 8**, and **Defendant Property 9** to a BTC address starting with

¹ BTC transactions can include multiple inputs and outputs. In this example, BTC stored in three separate BTC addresses were collectively sent to one BTC address.

1L7N. Within a few hours, BTC address 1L7N sent approximately 0.069 BTC to **Defendant Property 179**, an account at Virtual Currency Exchange 12.

98. On or about October 16, 2017, **Defendant Property 179** was registered to a Turkish national, Mehmet Akti (“Akti”) who later told Virtual Currency Exchange 12 that he used the account for the “purchase and sale of cryptocurrency, as well as the provision of services related to this activity.” Akti was not registered with the Financial Crimes Enforcement Network (“FinCEN”) as an MSB at the time of this statement.

99. In spite of this lack of registration, Virtual Currency Exchange 12 records show that Akti operated a prolific virtual currency MSB from **Defendant Property 179**. Specifically, between October 2017 and March 2019, **Defendant Property 179** was in receipt of approximately 2,328 BTC, 2,296 ETH, and U.S. dollar wires totaling \$82.8 million. All of the U.S. dollar wires originated from one bank account. Due to the nature of correspondent bank transactions, these international wires transited from outside the United States into the United States and then back out to the intended destination. Akti then used these U.S. dollar wires to acquire additional virtual currencies, primarily BTC and ETH.

100. During the same period, Akti withdrew large amounts of virtual currency from **Defendant Property 179**, to include approximately 11,228 BTC, 7,063 ETH, 957,109 XRP, and 118,008 EOS. Notably, these withdrawals were sent to over 250 unique cryptocurrency wallet addresses and involved transactions totaling over \$90 million. Akti used **Defendant Property 179** to service hundreds of customers for whom he transmitted these funds, as an unlicensed MSB.

101. Virtual Currency Exchange 12 records further show that at least six of Akti’s customers lived in the United States at the time of the transactions with **Defendant Property 179**, or relied on an account at a U.S.-based virtual currency exchange to use Akti’s services. In total,

Akti sent these U.S. nexus customers, approximately 373 BTC from **Defendant Property 179**, as part of his unlicensed money transmitting business.

102. On or about February 25, 2019, Virtual Currency Exchange 12 requested “Know-Your-Customer” (“KYC”) information from Akti. On or about March 8, 2019, Akti provided the requested KYC information. Three days later, Akti liquidated most of **Defendant Property 179** by transferring almost all of his cryptocurrency to other wallet addresses.

103. Nearly half of Akti’s cryptocurrency was redeposited into a second account at Virtual Currency Exchange 12, **Defendant Property 180**. In total, approximately 42.2 BTC, 2,465 ETH, 123,500 XRP, and 70,055 EOS was transferred through a network of intermediary wallet addresses from **Defendant Property 179** to **Defendant Property 180**.

104. Records show that **Defendant Property 180** was opened by, and registered to Husamettin Karataş (“Karataş”), on March 20, 2019, nearly the same time as **Defendant Property 179**’s liquidation.

105. Karataş admitted in a signed affidavit that he operated a cryptocurrency exchange from **Defendant Property 180**. Financial records and Blockchain analysis confirm this fact. These records and analysis also reveal the **Defendant Property 180** relied on the U.S. financial system to operate this exchange business, without the requisite FinCEN registration.

106. Specifically, in addition to the cryptocurrency received from Akti, **Defendant Property 180** received cryptocurrency and U.S. dollar wires valued at approximately \$2.1 million dollars between April 2019 and July 2019. During this same time period, **Defendant Property 180** withdrew cryptocurrency valued at approximately \$2.3 million dollars, transferring this cryptocurrency to approximately 17 unique wallet addresses.

107. One of Karataş's customers transacted within a U.S.-based virtual currency exchange. In total, this customer received approximately \$19,290 USD from **Defendant Property 180**. Notably, this same customer and account had previously transacted with Akti at **Defendant Property 179** in the amount of 2 BTC.

108. **Defendant Property 179** and **Defendant Property 180** shared a number of other customers. This included a customer that sent U.S. dollar wires, totaling approximately \$82.8 million dollars and \$500,000 respectively, to **Defendant Property 179** and **Defendant Property 180**.

109. **Defendant Property 179** and **Defendant Property 180** also shared common IP addresses and log in identifiers, further linking the accounts and their owners: **Defendant Property 179** and **Defendant Property 180** were both logged into within minutes of each other using a mobile device utilizing the same IP address, operating system version, and internet browser version between May 2019 and August 2019. One of these IP addresses, 78.180.183.249, was the primary IP address utilized to access both accounts.

COUNT ONE – FORFEITURE
(18 U.S.C. § 981(A)(1)(G)(I))

110. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 107 above as if fully set forth herein.

111. Hamas is a designated foreign terrorist organization.

112. The above described scheme involves the fundraising campaign of this designated foreign terrorist organization, and its military wing, the al-Qassam Brigades, to finance terrorism via BTC solicitations involving the **Defendant Properties**.

113. The Defendant Properties are subject to forfeiture to the United States, pursuant to 18 U.S.C. § 981(a)(1)(G)(i), as assets of a foreign terrorist organization engaged in planning or

perpetrating any federal crime of terrorism (as defined in section 2332b(g)(5)) against the United States, citizens or residents of the United States, or their property, and as assets affording any person a source of influence over any such entity or organization.

COUNT TWO – FORFEITURE
(18 U.S.C. § 981(a)(1)(A))

114. The United States incorporates by reference the allegations set forth in Paragraphs 93 to 107 above as if fully set forth herein.

115. The **Defendant Properties** were involved in a conspiracy to launder and the laundering of monetary instruments intended to promote the carrying on of a specified unlawful activity, that is, providing material support or resources to a designated foreign terrorist organization, namely Hamas, in violation of 18 U.S.C § 2339B.

116. **Defendant Property 179** and **Defendant Property 180** were also involved in a conspiracy to launder and the laundering of monetary instruments intended to promote the carrying on of a specified unlawful activity, that is, operating an unlicensed money transmitting business, violations of 18 U.S.C. § 1960.

117. As such, the **Defendant Properties** are subject to forfeiture, pursuant to Title 18, United States Code, Section 981(a)(1)(A), as property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or property traceable to such property.

PRAYER FOR RELIEF

WHEREFORE, the United States of America prays that notice issue on the Defendant Properties as described above; that due notice be given to all parties to appear and show cause why the forfeiture should not be decreed; that a warrant of arrest *in rem* issue according to law; that judgment be entered declaring that the **Defendant Properties** be forfeited for disposition

according to law; and that the United States of America be granted such other relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Dated: August 13, 2020

Respectfully submitted,

MICHAEL R. SHERWIN
Acting United States Attorney
N.Y. Bar No. 4444188

By: /s/ Jessi Camille Brooks
Jessi Camille Brooks, C.A. Bar No 983055
Zia M. Faruqui, D.C. Bar No. 494990
Assistant United States Attorneys
555 4th Street, N.W.
Washington, D.C. 20001
(202) 252-7745
Jessica.brooks@usdoj.gov

Danielle Rosborough D.C. Bar No. 1016234
Trial Attorney
National Security Division
United States Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20004
Office: (202) 514-0849 (main line)

ATTACHMENT A:**VIRTUAL CURRENCY EXCHANGE ACCOUNTS**

Accounts at Virtual Currency Exchange 1:

Defendant Property #	Account Identifier
1	3PajPWymUexhewHPczmLQ8CMYatKAGNj3y
2	3LrjAKNfnyX2BGmor6ZNxvZutM1Q3KEejZ
3	1HrPF5CPqJiWbkroxheU5LcHL7bZNDi76v
131	17cZ7CBhSPHn2gDkfNgrwNmHFDDHX7zC6q
132	1J6665h8Njpvva6crm1VSVwW8BToNFxaPxx
133	1GeLggwn8GqtTW6CYFUwerybHkzcNqPqaX
134	1Jp1Kwn43qzHWt7bGMdgZS9ZPbTi7rK9AY
135	1MgudcZEMXpB8uXUswuGHgDBTNmUZ8ZkZD
136	1PmAgUZXVvKMRcS37Hu2XVqdkovKG8ZPTk
137	1FUgt1eY69Ric3oaqtNK1xUex7dqph1eEv
138	3HB3GQhNxjfvPYKBYfUZwUVpSatqE8tHBb
139	3QqerQBe5duLc9YwqvKvDPAc3TJZxcfrsw
140	3E8yaNXEKQnnFMvnyyrwxaM9DaqNxHpFzP
141	3FeZrRq9nisxeR4RxBdj4DnhJSsABtGBAC
142	119Yw1qsUihJmBu68gcqgN36CrGy92d4aNX
143	32sVYnjTbnULtPKT8wuSNc7mzdwyuDDuAr

Accounts at Virtual Currency Exchange 2:

Defendant Property #	Account Identifier
144	13gGNrqWGPN5XxYNnceWEgGykuHuaFhPFM
145	1LuGcrfVyQ8KK1QuQysZcgoRtg7nuU55DH
146	User ID: 35764207
147	1DjYVV19zAuJPcXjn44is2CsAn4sW4it5W
148	15WrJ9vkvw46HGaD9PKpDLkGD6MCX8CEVR
149	14sXBGZZzeunJuyyA1fJY4tKyC5RM7WYTP
150	1LGcSmCwR2eMurxgwLeJtV9iRoLHCvNv3G
151	1Fyyfqjo4pvxwv6yqW5FrzrNspsYrX6ErX
152	User ID: 20920319
153	1P49duqmF5PwRSEpmL13F9QS8y3jVe4zjW
154	1BU8uxGuoFeATAey8XG91Q6Ux23tTTeYyx
155	1DPuLoyzjjTsbGFncWfu7eK52uYg1qFHtr
157	User ID: 22237397
158	1XD6XifgGCsvcGBUzXqpNNnvC5j3y8gey
159	133sCL2aCviV8N1TLngFGco7CDhHDmwChR
160	1A55bZqCNtFgASJHG4FxTNiAsU3jTt7DVo
161	1B7etAU8bG848QNXJjpe9XH9a1WrcWFm2Q

Account at Virtual Currency Exchange 3:

Defendant Property #	Account Identifier
156	34vKeiCwwu5guBZhr4J8RbnKTus8q1j7Sa

Accounts at Virtual Currency Exchange 4:

Defendant Property #	Account Identifier
162	3A2KA243cB17yFFWEcWqffTi3c9CAvq8Dh
163	3JXrtFWn7kaoz75bPqD23kPpMtKZiK3j2w

Account at Virtual Currency Exchange 5:

Defendant Property #	Account Identifier
164	35Yn5sRoasPArcXhN3Uz2HANn34rYg7ihG

Account at Virtual Currency Exchange 6:

Defendant Property #	Account Identifier
165	31mT7hQ7V6B58hfNVJchZTXP7gANpZjUjK

Account at Virtual Currency Exchange 7:

Defendant Property #	Account Identifier
166	Account at Virtual Currency 7 identified by email address

Accounts at Virtual Currency Exchange 8:

Defendant Property #	Account Identifier
167	3AwD6c5H2Hp6v73Md7Aon5n6HJU5YoBpDz
176	373k2ZQFXVsCtqdFyzRj7zmtsz1aP9dWoZ

Accounts at Virtual Currency Exchange 9:

Defendant Property #	Account Identifier
168	Account number: 11398678
169	1GgELQKEcqn572mvHKtzPBrjZ9L3bpKiLi
170	Account number: 11436806
171	1Eg7YSoJiqUV7ERsDXiGKExyJkkXR7NHr
178	1JjrTJgxSNqEPDrRBogD7odjvCwuog9Cqb

Accounts at Virtual Currency Exchange 10:

Defendant Property #	Account Identifier
172	Account number: 5806702
173	Account number: 6971221
174	3QRGcu41GN8cGYkp49xrv8VB7prLkokzLk

Accounts at Virtual Currency Exchange 11:

Defendant Property #	Account Identifier
175	1Mduu84x4Wm7FWm5vgaNvtk3APhEw1661t
177	1D9jDMKhss9vtmeRWeBA6tmts52JoQyezk

Accounts at Virtual Currency Exchange 12:

Defendant Property #	User ID
179	931770
180	2319627

VIRTUAL CURRENCY ADDRESSES

Defendant Property #	Virtual Currency Address
4	17QAWGVpFV4gZ25NQug46e5mBho4uDP6MD
5	1KDFQFnFfy9gJgXF18U3vpfeJQAeixPp1K
6	1HQhQfFPesW8znZdsdizHnA8ggvtc6NJ4k
7	1AW9z69zW2Wpg5i2gFs9YzkvZLjzDNx5VG
8	14EwXyqiB3yVLDJ1zVNevvEDpyyhBdnzjk
9	14S3GUHsqSY2am6yCPqEhb72sECUUbnRtE
10	14dRMzjmatz7zkc7iRYaitMvw4YPxXJYHf
11	1JJQceg2YZuCsJxUvAAVwU2YH4wDwxQoy6
12	1EQFWyM1gTus8cnuwHQErnaED3um1py2pF
13	19ncZQTCBfvfW5bsM7v3Pe7t6nzu4GZy4r

14	31hnjnw7Xe8e183u2qffHt4qpLFLfergmF
15	31idyYGpkmev8S1Kve8TvHEXydFeDM2saV
16	31iUH4sRXJt9F8MnnpVY1HAxUZ1qZQ4Z7x
17	31iZbakXU1arYMMYiCgceipKjUxCF19N5j
18	31jbxdhDYxkB6ULhsk7VMLsNB3KQgTREUZ
19	31k6eLZLTP1adv7EqZNkbn8Jm1oHnULuP
20	31mnD8FtBVyHh6CCFsUwiTFHuu6RMTCjcR
21	31mUJqqqH8HLsGaxMdARTgdPHkbWbq2yuQ
22	31n5MTyfWEFFm7pXf7e9Qt2i5Ec8jKA1py
23	31nob3VbXpByQZBuvHdFF1vcwjBoSd1xJF
24	31o5C1u66MjVZMrcJHzHYuQFk9XuDUznqX
25	31osZ4w7nPC2wbezG3fhu7fraUNBeEfdyA
26	31ot27eWxmxqVWmpisSyuakJNKqwc4uSZ
27	31otG9J9PWZ5GuUaAFVwuzP5nrAX6sVNh8
28	31p9vft5AqYgt7uPxTXCis97zHE2E8RkTG
29	31pmPV1XpevjEUzPtmr5sDXm8s4YzTyaS2
30	31pWw13YTX5h9EY6T5hjcRDT4bDF6cQMXR
31	31pYNazDxCwnhAyVCNqpELTE66qi4KcEA5
32	31qeJQa6Y6LL74HDBe5ZkuE7GxfMvUAh7t
33	31qk3S4hqj5KfedbVo45nFdvrXQ6TnYtY2
34	31qMgW6GideWcAHTdYf4GN3UEKEzVTP6jb
35	31qv732ydN8kbUyLYbv5QBNDyHRbRqL5wo
36	31rbKDq1pwA1GLHwa82cySVrkTo1R6htMK

37	31rhvmw3BPW9bYXvV6RJ4ZuwgUP2QbN6Wp
38	31rQoLSQkVa2SQhgRByhrM5e69KaKPntpp
39	31rZQb9DM2Fz5Yqi47UTsZ3FttETRAvbeu
40	31s1NZm8S16JsedBDJcSX815ikhNCkro28
41	31spTrrz7g2nCtf7JPVFrSawiQi6SGJyGU
42	31tKBTcV4bWYLEXzSwByPuJWmEnWkNUNs
43	32LjBurh7tKVpxmhhEhfPUnKYzV7jxzane
44	33mskKAPj8RVaFcSaCDtWtpCQYNCP4dFLw
45	344Aycb4ZzEZXEf26qgbGrfYjFEqMJbN6F
46	38vt9RRxHJboCyFbTieWT1sFKxbacKeBgg
47	3AHkpUF4zgvxVxRPKNrTQyo4NrZ1PH8x5Z
48	3CafimPzKw8ZhXQyQjojD2GDNpwsaQb12J
49	3DTLocTRA6s4LyZGnSN5g4aRfLd8FVaxHh
50	3Ea4umPPeQGELifMTXWmkJAZCzijBuYtVm
51	3EaD7SfNXda1LujuB1fyi8mzuA1qmrsUAq
52	3EaGnTmpjGYRSV2KAkrp6zg2uhPHAw15o
53	3EaKhQrXE2oZ6b74H7ML2SipNU7cdXhqDz
54	3EaPVCEnRRWZ96qJR8p6JgvgeTmGshvZRy
55	3EbyqWHMMzE96mMmB6bASnXsaGinwq7now
56	3EciaU3UgTycJvmd2KC4YG4NBoh6fqpZFU
57	3EcQ7XQXQiSS27LgV3hrvsXFntN7GxAxzf
58	3EdXMhAWLKg7PJfLbEKRCMm8Ldm6dsZDzT
59	3EeAr4pt2n9wjeFWY5XXTK1AGcmfTLG2hB

60	3Eein3xzdKxrvKQQJp5Y5H8cbqrhoEKW1N
61	3EekremuSe1bnR43w9nZMG2W7YMkvbvgPEa
62	3EemNUbRZoov3jp38BZuAJhSXxnSKQRN9F
63	3EeNxvKupEyoZjPEvoccaZBQN2TVTgndgP
64	3EeqqFMzUEPMpB4PZeDe1yHBmLVSiQ6QdX
65	3EeyeaD1YXwrkQGeYgo7QsoJi9tL9CZrxw
66	3EfH1Jk9JBqu6cHqXWUysRiM16HS5bjeK6
67	3EfKyF6eCRVTmvoMXPk8jUgDWfMXXAhhVq
68	3EfUV43ULkkxsezDDbfh9acBWhCNXQw3p
69	3EfYuiuGvoU6quCSD7RNHBQAngqkfjtu75
70	3EfzSMen4ds6HXTWP4FZeVZynJTSvvtUgN
71	3EgLDToL4NS51KC7LzY8rw6CsLeaoUVzzz
72	3EgnlPtQuctJViaK5E9gn2BYUZ9vkoyhQY
73	3Egrrh9KggYYnwoTic2mGrNNqUg7H2xMzt
74	3EguPmkenPJJa5ezKgRi41nnnz7JwUvexfy
75	3EWxNDQg52QH7ZXrAfxU22T5XyKCtxUG8Q
76	3EX4bu9vjudVXnFEXJq7pRW7qboPLPcCpU
77	3EX9MLM6pTK6nvajFj4woTx2nT7NXBxrLZ
78	3EXBCqAR9jW2XJsGK6pAifLhZrg76vDJxF
79	3EXUxdgs5JjmBTvhpCCtyYXveHXW9Ykxmc
80	3EXzujBDN5cVDeRgysMpQjyK8AZ3eZ7m5L
81	3EY8Ln5c51jwY4x7pKroCETEAK6Ch4EDVu
82	3EYc9agtyf5xjdX6gjXNXQVvxUb3UNtTzc

83	3EYwWQxei7iFcZcr99LcJAa5pFtFdyQrYX
84	3EZ6VeppfgZc3bGuefA7V5g17i9BnnNVWD
85	3EZetpgN7K5jow7sv9dKQZ2tL6JfNJU4Hy
86	3EZf21ULWjqpLDtzJU1qbfqXgHqaPDpdUD
87	3EZfMVxWBNBUm23HUvvaQXcET3WbkR34oS
88	3EZG4CNSAiDchj5mU5NehxtqVZgJqj3tuN
89	3EZQYLt6XAaWgwqm6PUHAKPGcfNtt3oY6T
90	3EZvc5LA6WjchP7VWY3BohXZ6u73xo3WcE
91	3EZx1DuWqwuRhErsoZJva2ibp8FUuYjBvC
92	3Fq8LkKoJU61MVqL7HJiPR3ecEpxEmqKkU
93	3FqsDefk77P9jQKbnM9qyQiyF13JFYcHTR
94	3FqsDefk77P9jQKbnM9qyQiyF13JFYcHTR
95	3FqV49yKKscsMV3JLmEX6NBm92bdZB83SZ
96	3FqV49yKKscsMV3JLmEX6NBm92bdZB83SZ
97	3Fr2ejXvkk7ccWx4of2TTBkkN4Z8PhmBkW
98	3Fr2ejXvkk7ccWx4of2TTBkkN4Z8PhmBkW
99	3Fr4DFkumQffMD9crpSxSP4oQ2dQRA75Ev
100	3Fr4DFkumQffMD9crpSxSP4oQ2dQRA75Ev
101	3Fr9hEMfYCnRoNyd9wEBJPMVgSEgVRxFXT
102	3FraSMiSHqntVAxiAiaPaD2z2K1YMvmSu9
103	3Freatgh7mpUhSjvrzUvDR4kR23ERYu3Gz
104	3FrfgNJ6cMoLt4DvSokLRWJYhs3iR58uG6
105	3FrGKydhTg1mgrwzaBdCF2TLq6dne7sQW

106	3FrgLnW4DQWJQXkaHQm1rvH4GFk7MPpRzy
107	3Frh4A8Teb1YFsf9T64TCvE6XCqv17Mse
108	3FricPpCwRFkL7zvYBKNEYMGUQp5F7Qj47
109	3FrP22X7MGdQZX66FHDPsrMvGoxFzFxxSD
110	3FrPk5dAyaqSpvs1bM43hRFHwHVmnosHw3B
111	3FrRV3hZKuBJmd9oEHuwPbq4Dq1f49yzus
112	3FrS1Vm2Vha1JrMTrGiyCxpwjvEx27cfS8
113	3FrSvZWjvDSGrRDPG6fdwEEEsUkrY65ZU7
114	3FrTayH9wkCnNkTTkfuqx7SVQQzzCQd5Cp
115	3FrUtZ3dXoGNDWejDbXanYefZR56JyiLsT
116	3FrVsAxKhtau1kcjVY8iXQNo2i1uZD6orS
117	3FrZphLBUTm9aTiXhnZTA3piVJ4oTxjpBU
118	3FtDtZdVMY53Jjk8fCPxydXb633jFdj3wo
119	3FtHfUNd2zgSY8FNW4Aq2f88wwSYiyVacg
120	3Ftpn5gXf79Zurdf7PYGfQZiipgVqEiUkg
121	3FvrNAv5KaEWVA7o8JJKFqeCfCP28JqRDt
122	3FvV3xyheg6BWAjX8Yy6dcENRfmhMnAZ6a
123	3Fw3NTwtmk8zQuwg6s2FPniXWPKirfqAgP
124	3FWSkG5NmyXF3rqMav7piXiJUDYzKpgFRT
125	3JaDQWNPpysYRcNNQxgkwSUpApXvn3XkbW
126	3La8eKaybxVeBLDxGNSyydVRoX9ZxjrDCW
127	3LhP8JYJ77cj2eVXBasY92Z6omTyRbUdbh
128	3Ngo99WAQieMEJGf5WJz2ycH1reFkj6yg

129	3QGyLXfEdN1iPt21toAf4qhM4zQ8zsDMMY
130	3Qms9Dk4ViL2LNfup8J5fYLXYCWsXj43Qa

ACCOUNTS AT FINANCIAL INSTITUTION 1

Defendant Property #	Account Ending	Email Address
181	40816	Hamas Email 1
182	17365	Hamas Email 1 Hamas Email 2
183	01709	Hamas Email 2 Hamas Email 3
184	08539	Hamas Email 4
185	52104	Hamas Email 4

DOMAIN NAMES

Defendant Property #	Account Ending
186	alqassam.net
187	alqassam.ps
188	qassam.ps