UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, Plaintiff, v. FACEMASKCENTER.COM - and - FOUR FACEBOOK PAGES Defendants.	Civil Action No. ____

UNITED STATES' VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

COMES NOW, Plaintiff the United States of America (the "United States"), by and through the United States Attorney for the District of Columbia, which brings this verified complaint for forfeiture in a civil action *in rem* against the defendant properties, namely: website, FaceMaskCenter.com ("Defendant Property 1") and Facebook pages, https://www.facebook.com/pg/facemaskcentertr ("Defendant Property 2"), https://www.facebook.com/toptantisort ("Defendant Property 3"), www.facebook.com/pg/toptantayttr/988930137790011 ("Defendant Property 4"), https://www.facebook.com/people/Murat-Çakar/100008437367572 ("Defendant Property 5") (collectively, the "Defendant Properties"); and alleges as follows.

NATURE OF ACTION AND THE DEFENDANT IN REM

1. This *in rem* forfeiture action arises out of an investigation by Homeland Security Investigations ("HSI"), the Internal Revenue Service, Criminal Investigations ("IRS-CI"), and the Federal Bureau of Investigation ("FBI"). Specifically, the United States is investigating the

unlawful sale of personal protection equipment ("PPE") during the national pandemic, and the related use of such proceeds to support and finance terrorism.

2. The Defendant Properties are subject to seizure and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(G)(i), as domestic and foreign assets of a designated foreign terrorist organization, the Islamic State of Iraq and the Levant ("ISIS"), which has engaged in planning and perpetrating federal crimes of terrorism as defined in 18 U.S.C. § 2332b(g)(5), against the United States, citizens or residents of the United States, and as foreign assets affording any person a source of influence over any such entity or organization.

JURISDICTION AND VENUE

3. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1345 and 1355.

4. Venue is proper pursuant to 28 U.S.C. § 1355(b)(1)(A).

FACTS GIVING RISE TO FORFEITURE

I. BACKGROUND

A. ISIS

5. On or about October 15, 2004, the U.S. Secretary of State designated al Qaeda in Iraq ("AQI"), then known as Jam'at al Tawhid wa'al-Jihad, as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act (the "INA") and as a Specially Designated Global Terrorist under section 1(b) of Executive Order 13224. On or about May 15, 2014, the Secretary of State amended the designation of AQI as an FTO under Section 219 of the INA and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224 to add the alias Islamic State of Iraq and the Levant ("ISIL") as its primary name. The Secretary also added the following aliases to the FTO listing: the Islamic State of Iraq and al-Sham (i.e., "ISIS"—which is how the FTO will be referenced herein), the Islamic State of Iraq and Syria, ad-Dawla al-Islamiyya fi al-'Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furqan

Establishment for Media Production. On September 21, 2015, the Secretary added the following aliases to the FTO listing: Islamic State, ISIL, and ISIS. To date, ISIS remains a designated FTO.

B. The Defense Production Act

6. On March 13, 2020, the President of the United States declared a national emergency due to the COVID-19 pandemic.

7. On March 25, 2020, the U.S. Department of Health and Human Services ("HHS") issued "Notice of Designation of Scarce Materials or Threatened Materials Subject to COVID-19 Hoarding Measures Under Executive Order 13910 and Section 102 of the Defense Production Act of 1950." In the notice, HHS designates the following items, among others, as scarce materials:

- N-95 Filtering Facepiece Respirators, including devices that are disposable half-face-piece non-powered air-purifying particulate respirators intended for use to cover the nose and mouth of the wearer to help reduce wearer exposure to pathogenic biological airborne particulates;
- Other Filtering Facepiece Respirators (e.g., those designated as N99, N100, R95, R99, R100, or P95, P99, P100), including single-use, disposable half-mask respiratory protective devices that cover the user's airway (nose and mouth) and offer protection from particulate materials at an N95 filtration efficiency level per 42 CFR 84.181;
- Protective devices that cover the user's airway (nose and mouth) and offer protection from particulate materials at an N95 filtration efficiency level per 42 CFR 84.181;
- Elastomeric, air-purifying respirators and appropriate particulate filters/cartridges;
- Powered Air Purifying Respirator ("PAPR");
- Portable Ventilators, including portable devices intended to mechanically control or assist patient breathing by delivering a predetermined percentage of oxygen in the breathing gas;

. . .

- Medical gowns or apparel, e.g., surgical gowns or isolation gowns;
- Personal protective equipment ("PPE") coveralls, e.g., Tyvek Suits;
- PPE face masks, including any masks that cover the user's nose and mouth and may or may not meet fluid barrier or filtration efficiency levels;
- PPE surgical masks, including masks that covers the user's nose and mouth and provides a physical barrier to fluids and particulate materials;
- PPE face shields, including those defined at 21 CFR 878.4040 and those intended for the same purpose;

. . .

- Ventilators, anesthesia gas machines modified for use as ventilators, and positive pressure breathing devices modified for use as ventilators (collectively referred to as "ventilators"), ventilator tubing connectors, and ventilator accessories as those terms are described in FDA's March 2020 Enforcement Policy for Ventilators and Accessories and Other Respiratory Devices During the Coronavirus Disease 2019 (COVID-19) Public Health Emergency located at https://www.fda.gov/media/136318/download.

C. Fraud Related to the National Pandemic

8. The Centers for Disease Control and Prevention ("CDC") recommends that people wear cloth face coverings in public settings. The CDC has further stated that it "does not recommend that the general public wear N95 respirators to protect themselves from respiratory diseases, including coronavirus (COVID-19). Those are critical supplies that must continue to be reserved for health care workers and other medical first responders, as recommended by current CDC guidance." *See* https://www.fda.gov/medical-devices/personal-protective-equipment-infection-control/n95-respirators-and-surgical-masks-face-masks.

9. In response to the current COVID-19 pandemic, N95 respirators are in high demand worldwide and designated as scarce as described above.

10. DuPont is a U.S. corporation that manufactures items in the field of industry, consumer goods, worker safety, and healthcare. DuPont manufactures a Tyvek coverall suit, which is used in hospital and hazardous material cleanups. According to the HHS, "DuPont's Tyvek is a versatile material that can provide a barrier against fine particles and chemicals. These coverall suits are part of the PPE needed for healthcare workers caring for COVID-19 patients. Other recommended PPE include a N95 respirator or surgical/face mask, a face shield or protective eyewear, and gloves." *See* https://www.hhs.gov/about/news/2020/04/08/hhs-provide-millions-tyvek-protective-suits-us-healthcare-workers.html.

11. Due to the COVID-19 pandemic, there is an acute shortage of DuPont Tyvek suits. Many resellers are out of stock or have limited offerings for sale. The U.S. government has negotiated an agreement with DuPont to deliver Tyvek Suits to the strategic national stockpile ("SNS"). The SNS is coordinating through the Federal Emergency Management Agency to deliver supplies where they are needed most for the COVID-19 response.

D. Background on Murat Cakar

12. On November 26, 2018, Zoobia Shahnaz pled guilty to providing material support to a designated foreign terrorist organization in violation of 18 U.S.C. § 2339B. Specifically, Shanaz sent more than $150,000 to shell companies, including companies in Turkey that were fronts for ISIS, and attempted to travel to Syria to join ISIS.

13. Shanaz used more than a dozen fraudulently obtained credit cards to purchase approximately $62,000 in Bitcoin, which she converted back to fiat currency to send to the shell companies.

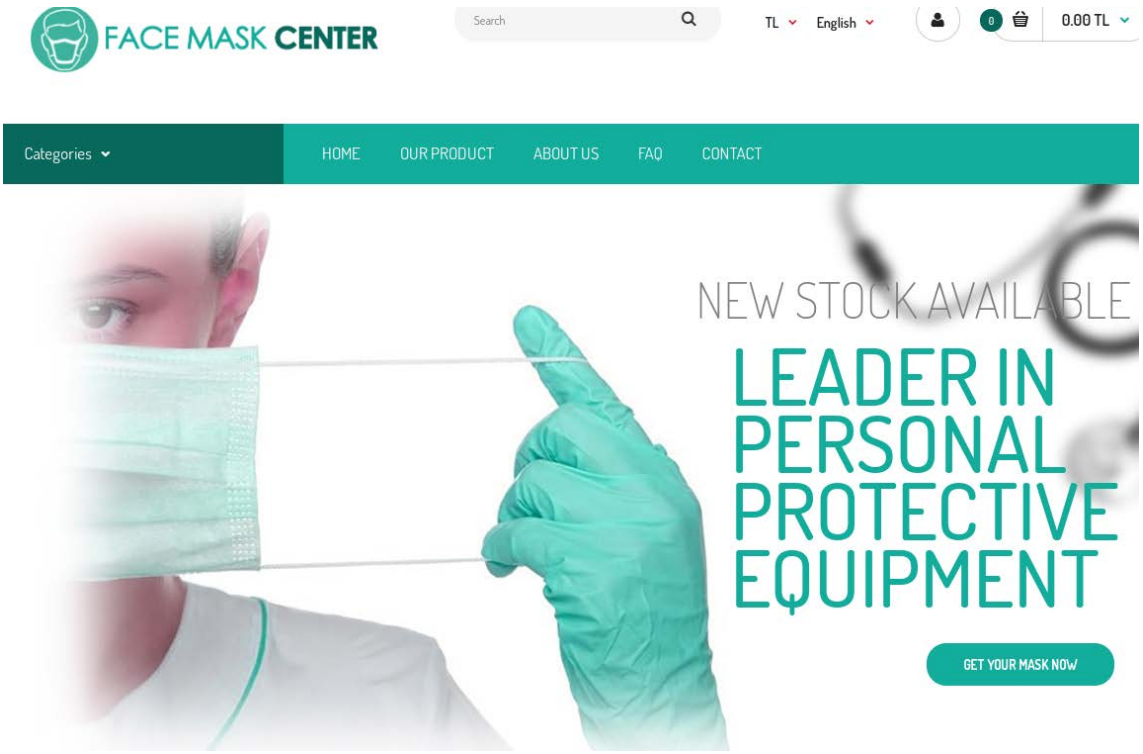
14. Financial records reveal that Zoobia Shahnaz sent approximately $100,000 to an alias of Murat Cakar. Money launderers frequently use aliases when collecting funds from different sources.

15. According to a confidential reliable source, Cakar is an ISIS facilitator who is responsible for managing select ISIS hacking operations, including activity involving Defendant Property 1.

E. Fraudulent sales via Defendant Property 1

16. The scarcity of the above-described PPE has led to numerous fraudulent websites claiming to sell authentic and certified PPE online.

17. Law enforcement, while in Washington, D.C., reviewed Defendant Property 1 and found that this site claims to sell multiple types of facemasks and PPE, including disposable hospital grade face masks, N95 respirator masks, washable facemasks, DuPont Tyvek coverall suits, and gloves. A recent snapshot of the site's homepage is displayed below:



18. On the "About" section of the webpage, Defendant Property 1 states:

> FaceMaskCenter is the original online personal protective equipment supplier and was the first of its kind. Owned and operated by sanitary experts, we pride ourselves on our product knowledge and quality customer service, so you can have safe and seamless online shopping experience. We have come a long way since launching our website in 1996. We started off small and grew our range to cater for everybody's health products needs. We now are serving online with our range of face masks, gloves, goggles, protective suits and thermometers.

19. The claim that the website launched in 1996 is demonstrably false. Publicly-available website registration records revealed that the website was created from an IP address in Turkey on February 26, 2020. Additionally, the site is not "owned and operated" by sanitary experts.

20. The site indicates that it accepts payment by Visa, Mastercard, and PayPal, all of which are U.S.-based financial institutions.

21. Defendant Property 1's section that sells N95 respirators states:

> **NOTE: Not all N95 masks are equal. Most are for industrial use. The N95 respirator offered by FaceMaskCenter is FDA cleared for medical use because it passed stringent fluid resistance testing. This is widely considered critical since airborne viruses transfer as fluid droplets.**
>
> - NIOSH [National Institute of Occupations Safety & Health] approved.
> - FDA cleared.
> - Meets CDC Guidelines for infection control of Flu, SARS, Corona Virus, Tuberculosis, Anthrax, Smallpox and more.
>
> . . .
>
> **This respirator has been evaluated and approved by The National Institute of Occupations Safety & Health (NIOSH) and is cleared by the U.S. Food & Drug Administration (FDA).** This product is a N95 Respirator deemed "Surgical" by the FDA. It is not a Surgical Mask. "Surgical N95 Respirators" undergo more rigorous testing and are designed to both prevent the spread of germs and protect the wearer's respiratory system.

(emphasis in original).

22. A review of the masks purportedly for sale on the site revealed that the masks are produced by a Turkish company. In spite of the Defendant Property 1's above statements, this Turkish manufacturer's respirators are not on the list of FDA/NIOSH approved N-95 respirators.

23. A customer in the United States contacted Defendant Property 1 to purchase N95 masks and other PPE for hospitals, nursing houses, and fire departments.

24. A Syrian national residing in Turkey responded to this request stating that Defendant Property 1 had such products for sale, and that they were certified.

25. The Syrian national stated that he could easily provide up to 100,000 N95 masks, which he claimed to have in his possession.

26. Defendant Property 1 also advertises the sale of DuPont Tyvek suits. Whereas other sites have severely restricted the quantity of any such items for sale (in order to prevent hoarding/price gouging on resale) or simply do not have any stock, Defendant Property 1 allows customers to place orders for any desired quantity of such items with no limits. This is inconsistent with the overall shortage of PPE, to include DuPont Tyvek suits.

F. Multiple Cakar Controlled Facebook Pages Promote Defendant Property 1

27. Defendant Property 1's related Facebook page is Defendant Property 2. Defendant Property 2's first post was on March 10, 2020, with a photo from Defendant Property 1. Defendant Property 2 posts multiple images and videos referencing Defendant Property 1 and Defendant Property 2 identifies Defendant Property 1

28. Cakar, while in Turkey, registered Defendant Property 2.

29. Cakar also created Defendant Property 3 and Defendant Property 4 which he uses to further the aforementioned PPE scheme.

30. Since 2015, Defendant Property 3 has primarily advertised the sale of t-shirts. Likewise, since 2014, Defendant Property 4 has also primarily advertised the sale of clothing products. One common method of money laundering is to claim that the funds were received through a licit business, such as clothing sales.

31. Law enforcement is aware that individuals who operate fraudulent websites often use other fraudulent companies under their control to advertise for the other sites.

32. On or about March 17, 2020, Defendant Property 3 and Defendant Property 4 posted an advertisement for Defendant Property 1. Subsequent to this post, Defendant Property 4 posted two additional advertisements for face masks.

33. Defendant Property 3 and Defendant Property 4 are linked to Defendant Property 5, which is a Facebook page in Cakar's name.

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

34. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 33 above as if fully set forth herein.

35. ISIS is a designated foreign terrorist organization.

36. The Defendant Properties are associated with ISIS.

37. As such, 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.

* * *

PRAYER FOR RELIEF

WHEREFORE, the United States 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 judgment be entered declaring that the Defendant Properties be forfeited to the United States for disposition according to law; and that the United States be granted such other relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Dated: July 31, 2020
Washington, D.C.

Respectfully submitted,

MICHAEL R. SHERWIN,
N.Y. Bar Number 4444188
ACTING UNITED STATES ATTORNEY

By: */s/ Zia Faruqui*
ZIA M. FARUQUI, D.C. Bar No. 494990
JESSICA BROOKS
Assistant United States Attorneys
Fourth Street, NW
Washington, DC 20530
(202) 252-7566 (main line)

and

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)

Attorneys for the United States of America

VERIFICATION

I, Joseph Consavage, a Special Agent with the Homeland Security Investigation, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *In Rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 31st day of July, 2020.

/s/ Joseph Consavage
Special Agent Joseph Consavage,
Homeland Security Investigation

I, Christopher Janczewski, a Special Agent with the Internal Revenue Service-Criminal Investigations, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *In Rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 31st day of July, 2020.

/s/ Chris Janczewski
Special Agent Chris Janczewski, IRS-CI

I, Nicholas Rivers, a Special Agent with the Federal Bureau of Investigation, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *In Rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 31st day of July, 2020.

/s/ Nicholas Rivers
Special Agent Nicholas Rivers
FBI

CIVIL COVER SHEET

JS-44 (Rev. 5/12 DC

I. (a) PLAINTIFFS

United States of America
c/o U.S. Attorney's Office
555 Fourth Street, N.W.
Washington, D.C. 20530

b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF _____
(EXCEPT IN U.S. PLAINTIFF CASES)

DEFENDANTS

FACEMASKCENTER.COM and
FOUR FACEBOOK PAGES

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT _____
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

c) ATTORNEYS (FIRM NAME, ADDRESS, AND TELEPHONE NUMBER)

Zia M. Faruqui (202) 252-7117
Assistant United States Attorney
555 4th Street, N.W.,
Washington, DC 20530

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION
(PLACE AN x IN ONE BOX ONLY)

- (●) 1 U.S. Government Plaintiff
- ( ) 3 Federal Question (U.S. Government Not a Party)
- ( ) 2 U.S. Government Defendant
- ( ) 4 Diversity (Indicate Citizenship of Parties in item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (PLACE AN x IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT) **FOR DIVERSITY CASES ONLY!**

	PTF	DFT		PTF	DFT
Citizen of this State	( ) 1	(●) 1	Incorporated or Principal Place of Business in This State	(●) 4	( ) 4
Citizen of Another State	( ) 2	(●) 2	Incorporated and Principal Place of Business in This State	( ) 5	(●) 5
Citizen or Subject of a Foreign Country	( ) 3	(●) 3	Foreign Nation	( ) 6	( ) 6

IV. CASE ASSIGNMENT AND NATURE OF SUIT

(Place an X in one category, A-N, that best represents your Cause of Action and one in a corresponding Nature of Suit)

( ) A. *Antitrust*

- [ ] 410 Antirust

( ) B. *Personal Injury/ Malpractice*

- [ ] 310 Airplane
- [ ] 315 Airplane Product Liability
- [ ] 320 Assault, Libel & Slander
- [ ] 330 Federal Employers Liability
- [ ] 340 Marine
- [ ] 345 Marine Product Liability
- [ ] 350 Motor Vehicle
- [ ] 355 Motor Vehicle Product Liability
- [ ] 360 Other Personal Injury
- [ ] 362 Medical Malpractice
- [ ] 365 Product Liability
- [ ] 367 Health Care/Pharmaceutical Personal Injury Product Liability
- [ ] 368 Asbestos Product Liability

( ) C. *Administrative Agency Review*

- [ ] 151 Medicare Act

Social Security
- [ ] 861 HIA (1395ff)
- [ ] 862 Black Lung (923)
- [ ] 863 DIWC/DIWW (405(g))
- [ ] 864 SSID Title XVI
- [ ] 865 RSI (405(g))

Other Statutes
- [ ] 891 Agricultural Acts
- [ ] 893 Environmental Matters
- [ ] 890 Other Statutory Actions (If Administrative Agency is Involved)

( ) D. *Temporary Restraining Order/Preliminary Injunction*

Any nature of suit from any category may be selected for this category of case assignment.

(If Antitrust, then A governs)

(●) E. *General Civil (Other)* OR **( ) F. *Pro Se General Civil***

Real Property
- [ ] 210 Land Condemnation
- [ ] 220 Foreclosure
- [ ] 230 Rent, Lease & Ejectment
- [ ] 240 Torts to Land
- [ ] 245 Tort Product Liability
- [ ] 290 All Other Real Property

Personal Property
- [ ] 370 Other Fraud
- [ ] 371 Truth in Lending
- [ ] 380 Other Personal Property Damage
- [ ] 385 Property Damage Product Liability

Bankruptcy
- [ ] 422 Appeal 27 USC 158
- [ ] 423 Withdrawal 28 USC 157

Prisoner Petitions
- [ ] 535 Death Penalty
- [ ] 540 Mandamus & Other
- [ ] 550 Civil Rights
- [ ] 555 Prison Conditions
- [ ] 560 Civil Detainee – Conditions of Confinement

Property Rights
- [ ] 820 Copyrights
- [ ] 830 Patent
- [ ] 840 Trademark

Federal Tax Suits
- [ ] 870 Taxes (US plaintiff or defendant)
- [ ] 871 IRS-Third Party 26 USC 7609

Forfeiture/Penalty
- [ ] 625 Drug Related Seizure of Property 21 USC 881
- [x] 690 Other

Other Statutes
- [ ] 375 False Claims Act
- [ ] 400 State Reapportionment
- [ ] 430 Banks & Banking
- [ ] 450 Commerce/ICC Rates/etc.
- [ ] 460 Deportation
- [ ] 462 Naturalization Application
- [ ] 465 Other Immigration Actions
- [ ] 470 Racketeer Influenced & Corrupt Organization

- [ ] 480 Consumer Credit
- [ ] 490 Cable/Satellite TV
- [ ] 850 Securities/Commodities/ Exchange
- [ ] 896 Arbitration
- [ ] 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- [ ] 950 Constitutionality of State Statutes
- [ ] 890 Other Statutory Actions (if not administrative agency review or Privacy Act)

○ **G. *Habeas Corpus/ 2255***	○ **H. *Employment Discrimination***	○ **I. *FOIA/Privacy Act***	○ **J. *Student Loan***
☐ 530 Habeas Corpus – General ☐ 510 Motion/Vacate Sentence ☐ 463 Habeas Corpus – Alien Detainee	☐ 442 Civil Rights – Employment (criteria: race, gender/sex, national origin, discrimination, disability, age, religion, retaliation) *(If pro se, select this deck	☐ 895 Freedom of Information Act ☐ 890 Other Statutory Actions (if Privacy Act) *(If pro se, select this deck	☐ 152 Recovery of Defaulted Student Loan (excluding veterans)
○ **K. *Labor/ERISA (non-employment)***	○ **L. *Other Civil Rights (non-employment)***	○ **M. *Contract***	○ **N. *Three-Judge Court***
☐ 710 Fair Labor Standards Act ☐ 720 Labor/Mgmt. Relations ☐ 740 Labor Railway Act ☐ 751 Family and Medical Leave Act ☐ 790 Other Labor Litigation ☐ 791 Empl. Ret. Inc. Security Act	☐ 441 Voting (if not Voting Rights Act) ☐ 443 Housing/Accommodations ☐ 440 Other Civil Rights ☐ 445 Americans w/Disabilities – Employment ☐ 446 Americans w/Disabilities – Other ☐ 448 Education	☐ 110 Insurance ☐ 120 Marine ☐ 130 Miller Act ☐ 140 Negotiable Instrument ☐ 150 Recovery of Overpayment & Enforcement of Judgment ☐ 153 Recovery of Overpayment of Veteran's Benefits ☐ 160 Stockholder's Suits ☐ 190 Other Contracts ☐ 195 Contract Product Liability ☐ 196 Franchise	☐ 441 Civil Rights – Voting (if Voting Rights Act)

V. ORIGIN

● 1 Original Proceeding ○ 2 Remand from State Court ○ 3 Remanded from Appellate Court ○ 4 Reinstated or Reopened ○ 5 Transferred from another district (specify ○ 6 Multi-district Litigation ○ 7 Appeal to District Judge from Mag. Judge

VI. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE.)

IEEPA 50 U.S.C. § 1701, conspiracy statute 18 U.S.C. § 371, money laundering 18 U.S.C. § 1956(a)(2)(A), (h)

VII. REQUESTED IN COMPLAINT CHECK IF THIS IS A **CLASS ACTION** UNDER F.R.C.P. 23 **DEMAND $** **JURY DEMAND:** Check YES only if demanded in complaint YES ☐ NO ☒

VIII. RELATED CASE(S) IF ANY (See instruction) YES ☐ NO ☒ If yes, please complete related case form

DATE: 07/31/2020 **SIGNATURE OF ATTORNEY OF RECORD** /s/ Zia M. Faruqui

INSTRUCTIONS FOR COMPLETING CIVIL COVER SHEET JS-44
Authority for Civil Cover Sheet

The JS-44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and services of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. Listed below are tips for completing the civil cover sheet. These tips coincide with the Roman Numerals on the cover sheet.

I. COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF/DEFENDANT (b) County of residence: Use 11001 to indicate plaintiff if resident of Washington, DC, 88888 if plaintiff is resident of United States but not Washington, DC, and 99999 if plaintiff is outside the United States.

III. CITIZENSHIP OF PRINCIPAL PARTIES: This section is completed only if diversity of citizenship was selected as the Basis of Jurisdiction under Section II.

IV. CASE ASSIGNMENT AND NATURE OF SUIT: The assignment of a judge to your case will depend on the category you select that best represents the primary cause of action found in your complaint. You may select only one category. You must also select one corresponding nature of suit found under the category of the case.

VI. CAUSE OF ACTION: Cite the U.S. Civil Statute under which you are filing and write a brief statement of the primary cause.

VIII. RELATED CASE(S), IF ANY: If you indicated that there is a related case, you must complete a related case form, which may be obtained from the Clerk's Office.

Because of the need for accurate and complete information, you should endure the accuracy of the information provided prior to signing the form.

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,	)	**Civil Action No. 20-cv-2227**
THE ALQASSAM.NET DOMAIN,	)	
THE ALQASSAM.PS DOMAIN,	)	
-- and –	)	
THE QASSAM.PS DOMAIN	)	
Defendants.	)	

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

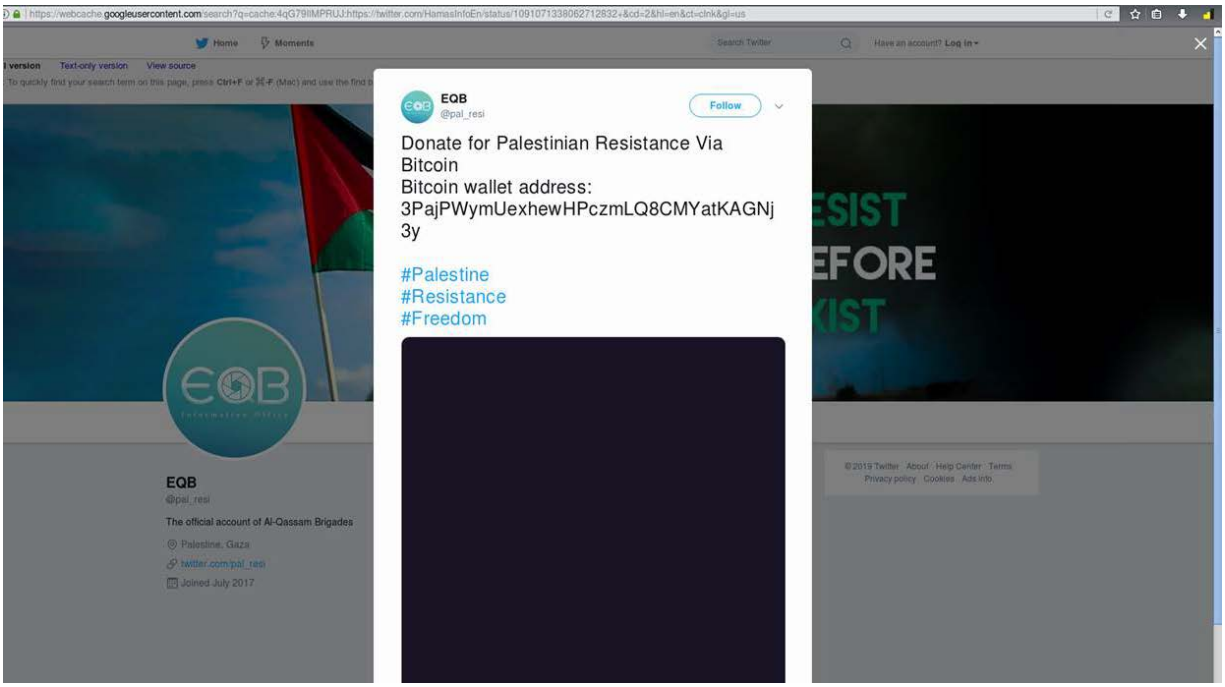
23. Stage one involved the following **Defendant Properties**, as described below:

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

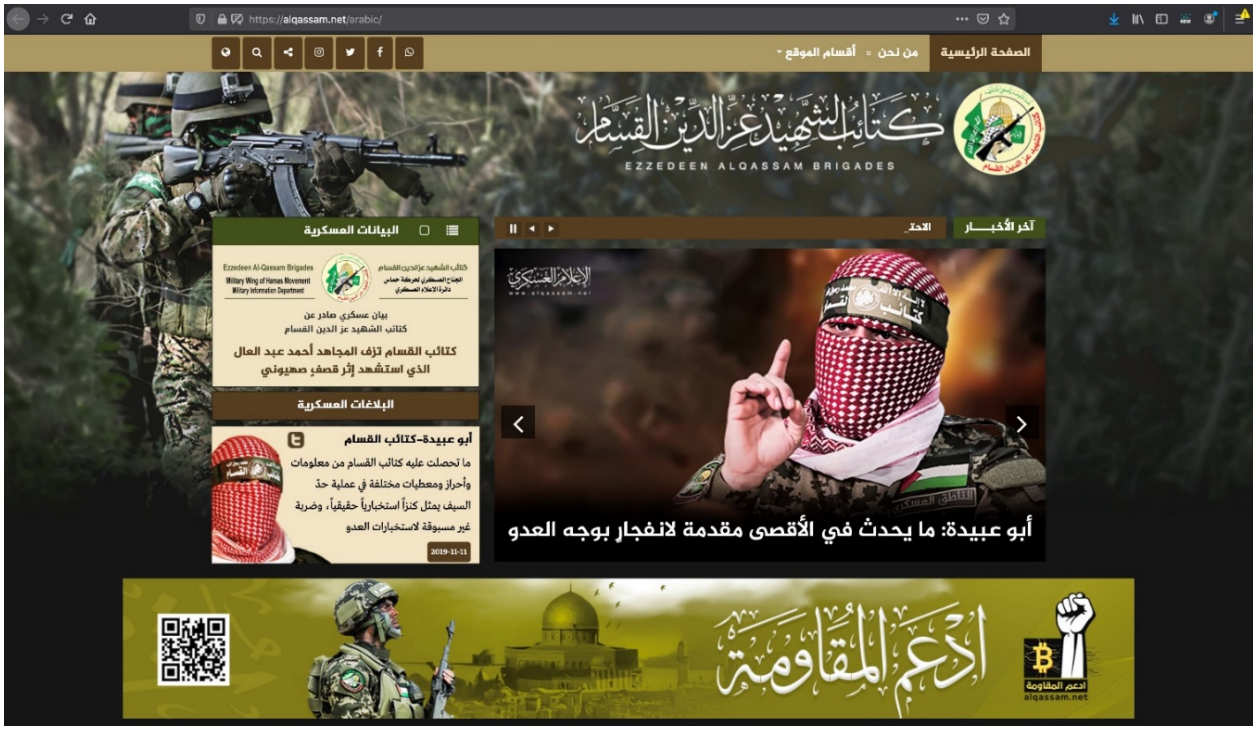
35. The first two stages relied on static BTC addresses, *i.e.*, a single fixed account number that could receive donations from anyone. Virtual currency exchanges could easily monitor the single static address on the Blockchain and evaluate their exposure to this terrorist funding campaign, and subsequently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

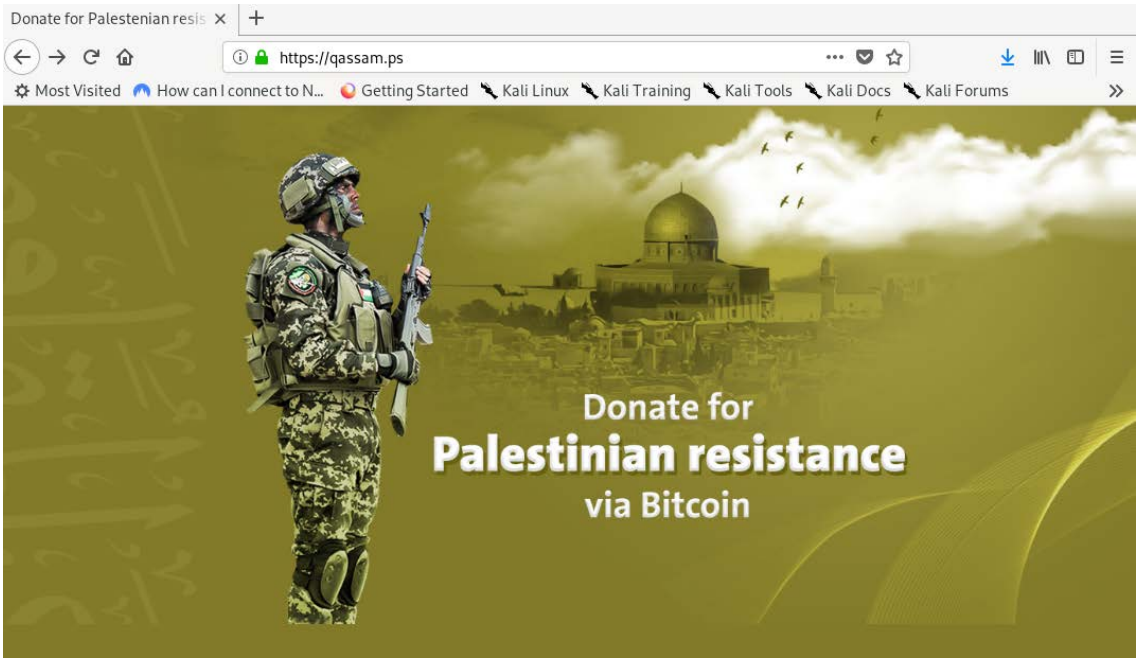
37. The al-Qassam Brigades' website included a reCAPTCHA human verification system provided by Google so that BTC addresses could not be harvested automatically. The al-Qassam Brigades also created two additional official sites located on the Palestinian domain to raise BTC for the campaign, **Defendant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

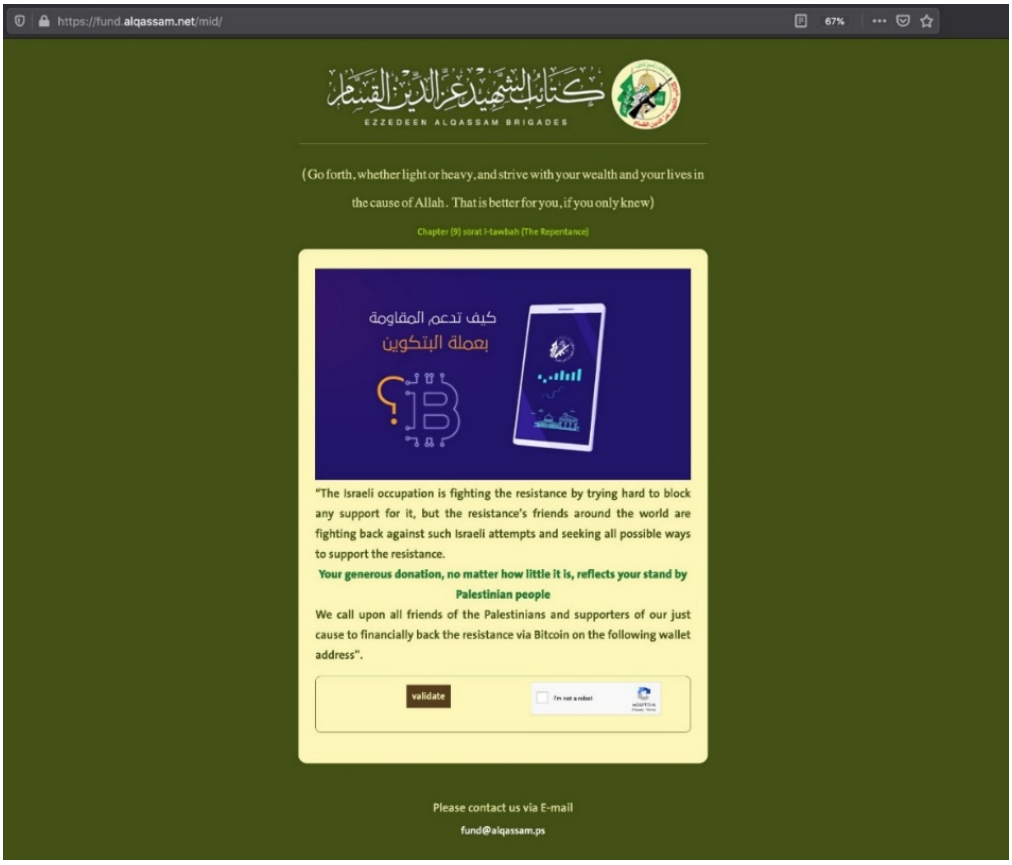
38. One of the Palestinian domain sites, **Defendant Property 187** appears identical to **Defendant Property 186**, providing the exact same information and instructions for contacting and donating to the organization.



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	31jbxdhDYxkB6ULhsk7VMLsNB3KQgTREUZ
19	31k6eLZLTP1adv7EqZNkbnd8Jm1oHnULuP
20	31mnD8FtBVyHh6CCFsUwiTFHuu6RMTCjcR
21	31mUJqpqH8HLsGaxMdARTgdPHkbWbq2yuQ
22	31n5MTyfWEFFm7pXf7e9Qt2i5Ec8jKA1py
23	31nob3VbXpByQZBuvHdFF1vcwjBoSd1xJF
24	31o5C1u66MjVZMrcJHzHYuQFk9XuDUznqX
25	31osZ4w7nPC2wbezG3fhu7fraUNBeEfdyA
26	31ot27eWxmxbQtVWmpiSyuakJNKqwc4uSZ
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	3EaGnTmpjGYRSV2KAkrgP6zg2uhPHAw15o
53	3EaKhQrXE2oZ6b74H7ML2SipNU7cdXhqDz
54	3EaPVCEnRRWZ96qJR8p6JgvgeTmGshvZRy

55	3EbyqWHMMzE96mMmB6bASnXsaGinwq7now
56	3EciaU3UgTycJvmD2KC4YG4NBoh6fqpZFU
57	3EcQ7XQXQiSS27LgV3hrvsXFntN7GxAxzf
58	3EdXMhAWLKg7PJfLbEKRCMm8Ldm6dsZDzT
59	3EeAr4pt2n9wjeFWY5XXTK1AGcmfTLG2hB
60	3Eein3xzdKxrvKQQJp5Y5H8cbqrhoEKW1N
61	3EekremuSe1bnR43w9nZMG2W7YMkbvgPEa
62	3EemNUbRZoov3jp38BZuAJhSXxnSKQRN9F
63	3EeNxvKupEyozjPEvoccaZBQN2TVTgndgP
64	3EeqkFMzUEPMpB4PZeDe1yHBmLVSiQ6QdX
65	3EeyeaD1YXwrkQGeYgo7QsoJi9tL9CZrxw
66	3EfH1Jk9JBqu6cHqXWUysRiM16HS5bjeK6
67	3EfKyF6eCRVTmvoMXPk8jUgDWfMXXAhhVq
68	3EfUV43ULkkxsezDDbfnh9acBWhCNXQw3p
69	3EfYuiuGvoU6quCSD7RNHBQAngqkfjtu75
70	3EfzSMeN4ds6HXTWP4FZeVZynJTSvvtUgN
71	3EgLDToL4NS51KC7LzY8rw6CsLeaoUVzzz
72	3Egn1PtQuctJViaK5E9gn2BYUZ9vkoyhQY
73	3Egrrh9KgqYYnwoTic2mGrNNqUg7H2xMzt
74	3EguPmkenPJa5ezKgRi41nnnz7JwUvexfy
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	3FrGKydHtTg1mgrwzaBdCF2TLq6dne7sQW
106	3FrgLnW4DQWJQXkaHQm1rvH4GFk7MPpRzy
107	3Frh4A8Tecb1YFsf9T64TCvE6XCqv17Mse
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.

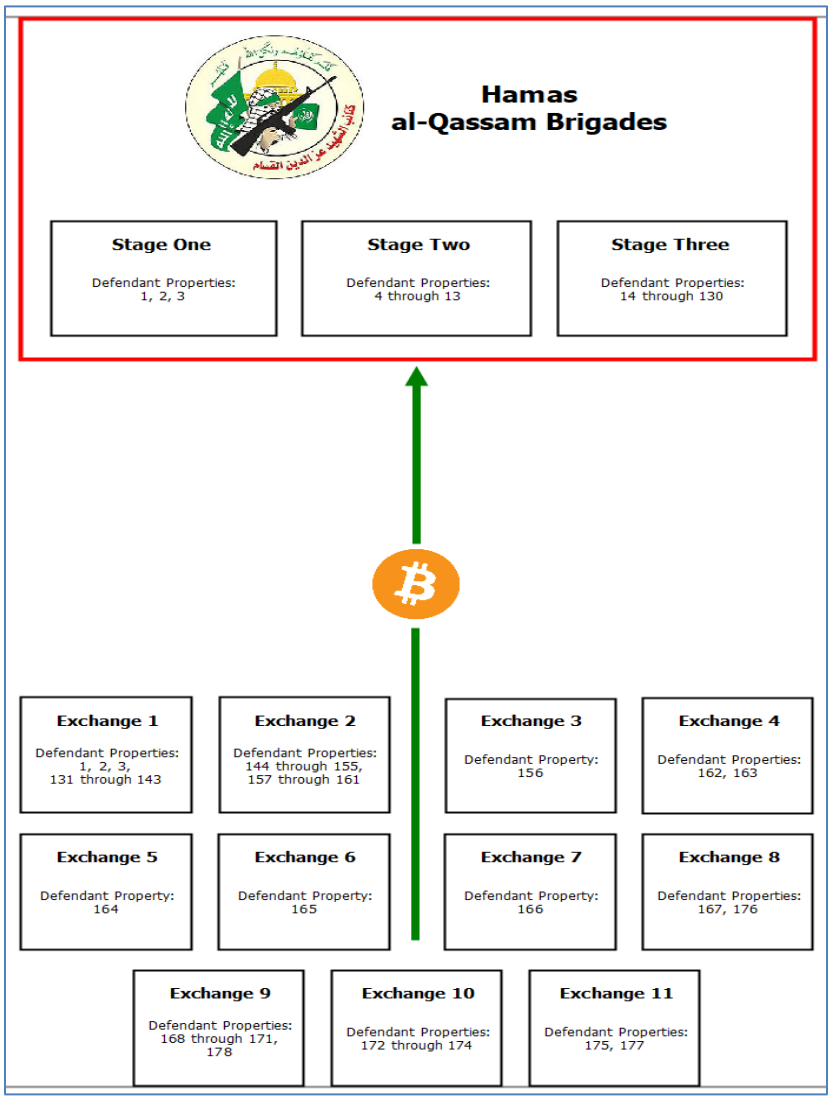
c. On or about March 24, 2014, **Defendant Property 183** was registered with Financial Institution 1 with Hamas Email 2. On or about June 22, 2014 and June 25, 2014, **Defendant Property 183** was used in an attempt to pay for website hosting services relative to the al-Qassam Brigades' Websites.

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. **<u>Virtual Currency Exchange 1</u>**:

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

Defendant Property #	Account Identifier
131	17cZ7CBhSPHn2gDkfNgrwNmHFDDHX7zC6q
132	1J6665h8Njpva6crm1VSFwW8BToNFxaPxz
133	1GeLggwn8GqtTW6CYFUwerybHkzcNqPqaX

134	1Jp1Kwn43qzHWt7bGMdgZS9ZPbTi7rK9AY
135	1MgudcZEMXpB8uXUswuGHgDBTNmUZ8ZkZD
136	1PmAgUZXVvKMRcS37Hu2XVqdkovKG8ZPTk
137	1FUgt1eY69Ric3oaqtNK1xUex7dqph1eEv
138	3HB3GQhNxjfvPYKBYfUZwUVpSatqE8tHBb
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	1Fyyfqjo4pvxwv6yqW5FrzrNspsYrX6ErX
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	1Eg7YSoJiqUV7ERsDXiGKExtyJkkXR7NHr

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)

VERIFICATION

I, Christopher Janczewski, a Special Agent with the Internal Revenue Service-Criminal Investigations, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *In Rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 13th day of August, 2020.

/s/ Chris Janczewski
Special Agent Chris Janczewski, IRS-CI

I, William Capra, a Special Agent with the Homeland Security Investigation, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *In Rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 13th day of August, 2020.

/s/ William Capra
Special Agent William Capra,
Homeland Security Investigation

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	1J6665h8Njpva6crm1VSFwW8BToNFxaPxz
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	1Eg7YSoJiqUV7ERsDXiGKExtyJkkXR7NHr
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	31k6eLZLTP1adv7EqZNkbnd8Jm1oHnULuP
20	31mnD8FtBVyHh6CCFsUwiTFHuu6RMTCjcR
21	31mUJqpqH8HLsGaxMdARTgdPHkbWbq2yuQ
22	31n5MTyfWEFFm7pXf7e9Qt2i5Ec8jKA1py
23	31nob3VbXpByQZBuvHdFF1vcwjBoSd1xJF
24	31o5C1u66MjVZMrcJHzHYuQFk9XuDUznqX
25	31osZ4w7nPC2wbezG3fhu7fraUNBeEfdyA
26	31ot27eWxmxbQtVWmpiSyuakJNKqwc4uSZ
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	3EaGnTmpjGYRSV2KAkrgP6zg2uhPHAw15o
53	3EaKhQrXE2oZ6b74H7ML2SipNU7cdXhqDz
54	3EaPVCEnRRWZ96qJR8p6JgvgeTmGshvZRy
55	3EbyqWHMMzE96mMmB6bASnXsaGinwq7now
56	3EciaU3UgTycJvmD2KC4YG4NBoh6fqpZFU
57	3EcQ7XQXQiSS27LgV3hrvsXFntN7GxAxzf
58	3EdXMhAWLKg7PJfLbEKRCMm8Ldm6dsZDzT
59	3EeAr4pt2n9wjeFWY5XXTK1AGcmfTLG2hB

60	3Eein3xzdKxrvKQQJp5Y5H8cbqrhoEKW1N
61	3EekremuSe1bnR43w9nZMG2W7YMkbvgPEa
62	3EemNUbRZoov3jp38BZuAJhSXxnSKQRN9F
63	3EeNxvKupEyozjPEvoccaZBQN2TVTgndgP
64	3EeqkFMzUEPMpB4PZeDe1yHBmLVSiQ6QdX
65	3EeyeaD1YXwrkQGeYgo7QsoJi9tL9CZrxw
66	3EfH1Jk9JBqu6cHqXWUysRiM16HS5bjeK6
67	3EfKyF6eCRVTmvoMXPk8jUgDWfMXXAhhVq
68	3EfUV43ULkkxsezDDbfnh9acBWhCNXQw3p
69	3EfYuiuGvoU6quCSD7RNHBQAngqkfjtu75
70	3EfzSMeN4ds6HXTWP4FZeVZynJTSvvtUgN
71	3EgLDToL4NS51KC7LzY8rw6CsLeaoUVzzz
72	3Egn1PtQuctJViaK5E9gn2BYUZ9vkoyhQY
73	3Egrrh9KgqYYnwoTic2mGrNNqUg7H2xMzt
74	3EguPmkenPJa5ezKgRi41nnnz7JwUvexfy
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	3FrGKydHtTg1mgrwzaBdCF2TLq6dne7sQW

106	3FrgLnW4DQWJQXkaHQm1rvH4GFk7MPpRzy
107	3Frh4A8Tecb1YFsf9T64TCvE6XCqv17Mse
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

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

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, Plaintiff, v. 155 VIRTUAL CURRENCY ASSETS Defendants.	Civil Action No. 20-cv-2228

UNITED STATES' VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

COMES NOW, Plaintiff the United States of America, by and through the Acting United States Attorney for the District of Columbia, and brings this Verified Complaint for Forfeiture *in Rem* against the defendant properties, namely: 155 virtual currency accounts (the "Defendant Properties"), which are further described 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 DEFENDANT 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"), Federal Bureau of Investigation ("FBI"), and Homeland Security Investigations ("HSI"). Specifically, the United States is investigating the unlawful use of the cryptocurrency to support and finance terrorism.

2. The Defendant Properties are subject to seizure and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(G)(i), as foreign assets of designated foreign terrorist organizations based in Syria that are linked to al-Qaeda, including the Al-Nusrah Front ("ANF") and Hay'at Tahrir al-Sham ("HTS"), which have engaged in planning and perpetrating federal crimes of terrorism as defined

in 18 U.S.C. § 2332b(g)(5), against the United States, citizens or residents of the United States, and as foreign assets affording any person a source of influence over any such entity or organization.

JURISDICTION AND VENUE

3. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1345 and 1355.

4. Venue is proper pursuant to 28 U.S.C. § 1355(b)(2).

FACTS GIVING RISE TO FORFEITURE

I. BACKGROUND

A. al-Qaeda and Affiliated Foreign Terrorist Organizations

5. On October 8, 1999, the United States Secretary of State designated al-Qaeda as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist ("SDGT") under section 1(b) of Executive Order 13224. The Secretary of State also added the following aliases to the FTO listing: "the Base," the Islamic Army, the World Islamic Front for Jihad Against Jews and Crusaders, the Islamic Army for the Liberation of the Holy Places, the Usama Bin Laden Network, the Usama Bin Laden Organization, Islamic Salvation Foundation, and The Group for the Preservation of the Holy Sites. To date, AQ remains a designated FTO.

6. Al Qaeda's designation as an FTO and SDGT has been renewed on multiple occasions since 1999, and al-Qaeda remains a designated FTO and SDGT today.

7. On October 15, 2004, the Secretary of State designated Jam'at al Tawhid wa'al-Jihad as an FTO under Section 219 of the Immigration and Nationality Act and as a SDGT under section 1(b) of Executive Order 13224.

8. On December 15, 2004, the Deputy Secretary of State added numerous aliases to the Jam'at al Tawhid wa'al-Jihad FTO designation including the alias al-Qaida in Iraq ("AQI").

9. On December 11, 2012, the Secretary of State amended the FTO and SDGT designations of Jam'at al Tawhid wa'al-Jihad to include the following aliases: al-Nusrah Front ("ANF"), Jabhat al-Nusrah, Jabhet al-Nusra, The Victory Front, and Al-Nusrah Front for the People of the Levant.

10. On May 15, 2014, the Secretary of State, in response to the evolving nature of the relationships between ANF and AQI, amended the FTO and SDGT designations of AQI to remove all aliases associated with ANF. Separately, the Secretary of State then designated al-Nusrah Front (ANF), also known as Jabhat al-Nusrah, also known as Jabhet al-Nusra, also known as The Victory Front, also known as Al-Nusrah Front for the People of the Levant, also known as Al-Nusrah Front in Lebanon, also known as Support Front for the People of the Levant, and also known as Jabaht al-Nusra li-Ahl al-Sham min Mujahedi al-Sham fi Sahat al-Jihadb as an FTO under Section 219 of the Immigration and Nationality Act and as a SDGT under section 1(b) of Executive Order 13224.

11. On October 19, 2016, the Secretary of State amended the FTO and SDGT designations of ANF to include the following new aliases: Jabhat Fath al Sham, also known as Jabhat Fath al-Sham, also known as Jabhat Fatah al-Sham, also known as Jabhat Fateh al-Sham, also known as Fatah al-Sham Front, also known as Fateh Al-Sham Front, also known as Conquest of the Levant Front, also known as The Front for liberation of al Sham, also known as Front for the Conquest of Syria/the Levant, also known as Front for the Liberation of the Levant, also known as Front for the Conquest of Syria.

12. On May 17, 2018, the Secretary of State amended the FTO and SDGT designations of ANF to include the following aliases: Hay'at Tahrir al-Sham, also known as Hay'et Tahrir al-Sham, also known as Hayat Tahrir al-Sham, also known as HTS, also known as Assembly for the Liberation of Syria, also known as Assembly for Liberation of the Levant, also known as

Liberation of al-Sham Commission, also known as Liberation of the Levant Organisation, also known as Tahrir al-Sham, also known as Tahrir al-Sham Hay'at.

13. To date, ANF and HTS remain designated FTOs.

B. Bitcoin

14. 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 does not identify the individuals involved in the transaction. This feature makes BTC pseudonymous; 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.

15. 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 public transactions can sometimes lead to identifying both the owner of a BTC address and any other accounts that the person or entity owns and controls.

16. BTC is often transacted using a virtual-currency exchange, which is a virtual-currency trading platform and bank. It typically allows 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.

B. Blockchain Analysis

17. 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.

18. 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.

19. 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.

II. AL-QAEDA BTC TERROR FINANCE CAMPAIGN

20. In April 2019, the administrator of the Telegram group "Tawheed & Jihad Media," which is now defunct, provided a Bitcoin address starting with 37yrx7 ("**Defendant Property AQ1"**) as a repository for pro-al-Qaeda donations.

21. Posts on the Tawheed & Jihad Media Telegram group during that same time frame advertised fundraising campaigns to raise money for fighters. For example, on or about May 25, 2019, a user posted an image with the text: "FUNDRAISING CAMPAIGN" and "FINANCE BULLETS AND ROCKETS FOR THE MUJAHIDEEN." Muhajideen in this context refers to al Qaeda fighters or soldiers. The post accompanying the image stated, "For Donations and more details: Please message: @TawheedJihadMedia."

22. The media content of the Tawheed & Jihad Media Telegram group included watermarked images of both Ansar al-Tawheed, a jihadist group that was created in or about March 2018, and the Syria-based pro-al-Qaeda collective Wa Haredh al-Moemeneen ("Incite the Faithful"), of which Ansar al-Tawheed is a member. The collective Wa Haredh al-Moemeneen was formed in approximately the fall of 2018 to oppose negotiations with the Syrian regime and, as of May 2019, when the Telegram group administrator solicited donations to **Defendant Property AQ1**, was fighting against Syrian government forces and their allies in northern Syria.

23. On or about May 5, 2019, **Defendant Property AQ1** sent its entire balance of BTC, approximately 0.14610741 BTC, to a cluster of BTC addresses, containing the root address starting with 3LcrD ("**Defendant Property AQ2**").

24. Al-Qaeda and affiliated terrorist groups have been operating a BTC money laundering network using Telegram channels and other social media platforms to solicit BTC donations to further their terrorist goals. As described below, al-Qaeda and affiliated terrorist groups operate a number of Telegram channels and purport to act as charities when, in fact, they are soliciting funds for the mujahedeen. Al-Qaeda and the affiliated terrorist groups are connected and use multi-layered transactions to obfuscate the movement of BTC.

25. **Defendant Property AQ2** is a central hub used to collect funds and then redistribute the funds within this money laundering network. From on or about February 25, 2019 through on or about February 5, 2020, **Defendant Property AQ2** received approximately 15.27050803 BTC via 187 transactions.

26. Between February 25 through on or about July 29, 2019, **Defendant Property AQ2** sent approximately 9.10918723 BTC via 38 transactions to an account at a virtual currency exchange (**Defendant Property 1**).

27. Funds received by **Defendant Property 1** were in turn sent to various online gift

card exchanges ("GCE") that facilitate the sale of various gift cards in exchange for cryptocurrency. This is a common method of money laundering known to law enforcement.

28. On or about May 21, 2019, a BTC address starting with 3KhAH (**Defendant Property 2)** sent approximately 0.02825625 BTC to **Defendant Property AQ2**.

29. On or about May 29 and 30, 2019, **Defendant Property 2** sent a total of approximately 0.07640859 BTC to a BTC address starting with 3LZg4 **(Defendant Property 3)**. Within hours, **Defendant Property 3** sent BTC to **Defendant Property AQ2**. This is a common method of money laundering known to law enforcement as layering.

Leave an Impact Before Departure

30. A Syria-based organization that translates to "Leave an Impact Before Departure," has conducted donation campaigns asking people to send support via BTC. As of July 30, 2020, Leave an Impact Before Departure publicly claimed that it was a charity conducting humanitarian work. However, this group has posted images on its Telegram channel regarding the prices of military equipment needed to support the fighters inside of Syria.

31. For example:

32. As demonstrated above, these posts are seeking funds for military equipment.

33. Leave an Impact Before Departure advertised an account at a virtual currency exchange (**Defendant Property 4**) in the Telegram channel as its deposit address to which donors could send BTC.

34. **Defendant Property 4** received approximately 14.58133728 BTC via 65 transactions for the period on or about March 10 to on or about December 11, 2019. This includes seven transactions totaling approximately 0.73060999 BTC from **Defendant Property AQ2**.

35. A cluster of approximately 29 BTC addresses with a root address starting with 1JtyZ received (**Defendant Property 5 - Defendant Property 33**) approximately 0.29328346 BTC via six transactions from **Defendant Property AQ2**. Cluster 1JtyZ sent:

a. 0.76916964 BTC via three transactions to **Defendant Property 1**; and

b. 0.2270076 BTC via two transactions to **Defendant Property 4**.

Al Ikhwa

36. The Telegram channel for @Al_ikhwa_official appeared online in or around June 2018. The administrator of the group is listed as "@AL_ikhwa." The group's profile describes them as an "independent charity on the ground in Syria" and that they "do not support any acts of terrorism;" however, blockchain analysis and a review of related social media posting demonstrates otherwise.

37. Many of Al Ikhwa's posts on Telegram solicit donations through PayPal, Western Union and "anonymous payment" with BTC. Their first post stated, in part:

> …supporting the brothers in Syria, Wives of [martyrs] and their families…[and] We help those who defend the Muslims in [Syria].

38. The Al Ikhwa administrator posted 11 BTC addresses for potential donors to fund ("**Al Ikhwa Cluster**"). These 11 BTC addresses represent **Defendant Property 34** through **Defendant Property 44.**

39. Blockchain analysis revealed the **Al Ikhwa Cluster** has received approximately 0.43820188 BTC via 18 transactions for the period October 15, 2018 to September 3, 2019.

40. Approximately half of the BTC received by this cluster, 0.22524884 BTC, was sent via four transfers to **Defendant Property AQ2**.

41. Shortly thereafter **Defendant Property AQ2** received BTC from the **Al Ikhwa Cluster**, the proceeds of which were sent to **Defendant Property 1**.

42. **Al Ikhwa** also operated a Facebook account which had posted four BTC addresses for donations. Two of these BTC addresses are part of the **Al Ikhwa Cluster** and the other two are part of a cluster of six BTC addresses ("**Al Ikhwa Facebook Cluster**"). These six BTC addresses represent **Defendant Property 45** through **Defendant Property 50**. **Al Ikhwa**

Facebook Cluster sent approximately 0.09413247 BTC during April and May 2020, via three transfers to the **Al Ikhwa Cluster**.

43. The documented practice of layering BTC transfers is observed herein, where Al Ikhwa is attempting to obfuscate the source of BTC and conceal the identity of the owner.

44. The Al Ikhwa administrator stated on Telegram:

> Yeah, bitcoin makes a new one [i.e. address] every transaction so it's good, it always looks like it's going to a different place..if you ever get [a] police visit and they want to trap you to say you sent [donations] to Syria.. say they are liars..because one person told me maybe they can't track the bitcoin but they can see IP address...But our Syria IP addresses are Turkish because our Internet comes from Turkey. So if they try to trap someone and say you sent money here by showing IP address, you say they are liars and you did business in Turkey.. cause the IP address is Turkish.

45. The Al Ikhwa money laundering network conducted layered transactions including as follows:

a. **Al Ikhwa Cluster** sent 0.09019068 BTC to cluster 3HvtR on or about January 20, 2019, and then five days later this cluster sent 0.3372531 BTC to **Defendant Property 1**.

b. **Al Ikhwa Cluster** sent 0.05927279 BTC to address 36A2P on or about April 2, 2019.

i. That same day, address 36A2P sent 0.041 BTC to **Defendant Property 4**;

ii. A few days later, address 36A2P sent 0.01953034 BTC to **Defendant Property 1**;

c. **Al Ikhwa Cluster** sent a total of 0.00016023 BTC via two transactions to cluster 12Btp on or about October 19, 2018, and on or about March 2, 2019. On or about July 16, 2019, cluster 12Btp sent 0.00651841 BTC to **Defendant Property AQ2**.

Malhama Tactical

46. Open source reporting has linked Al Ikhwa to Malhama Tactical, a jihadist military company that trains HTS fighters and has solicited BTC to finance HTS operations in Syria.

47. Malhama Tactical is described in open source materials as a "jihadist private military company." It is comprised of fighters from Uzbekistan and the Russian Caucuses.

48. The Twitter page of Malhama Tactical's founding leader, Abu Salman Belarus, describes him as the "Commander of Malhama Tactical, we are the military instructors, we've been teaching rebels how to fight and provide emergency aid on battlefield since 2013." In a published interview in February 2019, Abu Salman Belarus stated that Malhama Tactical worked with and trained HTS fighters. Moreover, in around July 2019, Malhama Tactical fundraised for drones to be used for "artillery adjustment and reconnaissance." In releasing an intelligence report about that fundraising effort, the SITE Intelligence Group described Malhama Tactical as an HTS Special Forces training group.

49. Notably, an April 2020 online video from a news media outlet showed interviews with members of Malhama Tactical about certain military tactics they used after recent battles in Idlib, Syria. In a published video interview on or about June 11, 2020, a Malhama Tactical leader named Ali al-Shishani described Malhama Tactical as a group of professional instructors who trained members of the Syrian resistance and stated that HTS was one of the groups with whom Malhama Tactical worked.

50. The Twitter account of Malhama Tactical's founder, Abu Salman Belarus, tweeted two BTC addresses when soliciting donations. His tweets stated, "You can support and help us anonymously and safely with Bitcoin wallet: 1J5x4," and "Bitcoin wallet for support instructor team of [MT]: 1LVwt."

51. These two Malhama Tactical addresses are part of a cluster of 23 addresses ("**MT cluster**") that received approximately 0.19501359 BTC via 15 transactions for the period July 13 to November 22, 2019. These 23 BTC addresses represent **Defendant Property 51** through **Defendant Property 73.**

52. On or about October 9, 2018, **MT cluster** sent approximately 0.03839 BTC to cluster 3Jb1M which has sent BTC to **Defendant Property AQ2** on multiple occasions.

Reminders From Syria

53. The Al Ikhwa Telegram channel forwarded several posts from the "@RemindersFromSyria" ("RFS") channel, and the RFS channel has similarly forwarded Al Ikhwa's posts, many of which contained Al Ikhwa's BTC addresses.

54. RFS's channel falsely states that they are "not affiliated with any fighting groups in Syria" and they "do not promote any acts of violence and terrorism." In fact, they have posted numerous donation requests to support foreign fighters, threats to the United States, and radical extremists abroad.

55. For example, one post showed a photograph of a machine gun with a military-style vest holding numerous additional magazines of bullets. Another post stated:

56. On or about July 16, 2020, an HSI agent acting in an undercover capacity ("UCA") messaged the administrator of the RFS Telegram channel asking to donate BTC. The administrator provided a BTC address starting with 1CoEM (**Defendant Property 74**). Subsequently, **Defendant Property 74** clustered with **Defendant Property 75** and **Defendant Property 76 ("RFS Cluster")**.

57. The administrator stated that he hoped for the destruction of the United States and warned the UCA to be careful of possible criminal consequences from carrying out a jihad in the United States.

58. After these illicit conversations, the administrator shared his "own wallet" BTC address starting with 1Q4xw (**Defendant Property 77**), which could be used for "jihad."

59. The administrator complained about U.S. drones and subsequently stated that "Bullets and bombs is all affordable, but the drone stuff, its very hard to unless u have like anti aircraft stuff which is like millions of dollars. Here they shoot it with a ground to air missile.. its possible to hit them but hard. Or a 23mm machine gun. U know those big guns attached to a car.."

60. **RFS Cluster** and **Defendant Property 77** are further linked because they both, in separate transitions, sent approximately 0.003769 BTC and 0.00235163 BTC respectively, at the same time on or about July 23, 2020 to a cluster of BTC addresses with the main address starting with 3QkrD.

61. A majority of the BTC received by cluster 3QkrD is sent to a BTC address starting with 1Kszb (**Defendant Property 78**), which is hosted at the same virtual currency exchange as (**Defendant Property 1**).

62. **RFS Cluster** also sent BTC to a cluster of BTC addresses with the main address starting with 3KKa3. Like cluster 3QkrD, cluster 3KKa3 sent BTC to **Defendant Property 78** multiple times.

Al Sadaqah

63. Al Sadaqah ("charity" in Arabic) is a Syrian organization that operates social media accounts on multiple platforms which seek to finance terrorism via BTC solicitations. They described themselves as "an independent charity organization that is benefiting and providing the Mujahidin in Syria with weapons, finical [sic] aid and other projects relating to the jihad. You can donate safely and securely with Bitcoin."

64. On its Telegram channel, Al Sadaqah openly solicited donations via BTC to an address starting with 15K9Z (**Defendant Property 79**, which clustered with **Defendant Property 80**).

65. In one such post (depicted below), they directed people to "Donate anonymously with Cryptocurrency" to **Defendant Property 79**, to support "the mujahidin in Syria with weapons, financial aid, and other projects assisting the jihad."

66. Example posts are shown here:

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

67. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 66 above as if fully set forth herein.

68. Al-Qaeda, HTS, and ANF are designated foreign terrorist organizations.

69. The above described scheme involves these designated foreign terrorist organizations' campaigns to finance terrorism via BTC solicitations involving the Defendant Properties.

70. 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.

PRAYER FOR RELIEF

WHEREFORE, the United States 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 judgment be entered declaring that the Defendant Properties be forfeited to the United States for disposition according to law; and that the United States 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
Washington, D.C.

Respectfully submitted,

MICHAEL R. SHERWIN,
N.Y. Bar Number 4444188
ACTING UNITED STATES ATTORNEY

By: */s/ Zia Faruqui*
ZIA M. FARUQUI, D.C. Bar No. 494990
JESSICA BROOKS
Assistant United States Attorneys
Fourth Street, NW
Washington, DC 20530
(202) 252-7566 (main line)

and

ALEX HUGHES
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)

Attorneys for the United States of America

VERIFICATION

I, Christopher Janczewski, a Special Agent with the Internal Revenue Service-Criminal Investigations, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *In Rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 13th day of August, 2020.

/s/ Chris Janczewski
Special Agent Chris Janczewski
IRS-CI

I, Joseph Consavage, a Special Agent with the Homeland Security Investigation, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *In Rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 13th day of August, 2020.

/s/ Joseph Consavage
Special Agent Joseph Consavage,
Homeland Security Investigation

ATTACHMENT A:

Defendant Property	BTC Address
1	1421chCK32pV32Tw5MQbiUiKWKvnmj7d91
2	3KhAHDfTuVnHUfRgQfVP4LcV8SHXpN51u7
3	3LZg4hHfbpLrJBagQqXp2agGbwrz9XpXai
4	163oWqgPk8fKhUqmHpNnoQhikfFjHyD3Pr
5	1JtyZYT4CKeKNyxMzbCpC9VJT6KTmeAKFN
6	3Bp2Eb87ApoMAsKPSQB2SAqLmRymjeLmtv
7	3HUhCkt44P3izoLZkK3rcx8NsZXKJdksh5
8	3Q4Nb6jUWAJQLq5NS7S92YPPCTcTyuSPhK
9	3Bo3cPpPjFzt6YHFfRoX6ufY1b2zzVf8mT
10	3HSK6MbuoewuttVBuYepEA4fyyPxHzZ6pB
11	1Awi7RLBGdT9qCo5SCB5y6Xea7MTb1F5Xc
12	33uWGWsWSTBw1KLM4UFPvxYvDJ5Xfo9s63
13	3G68RkhEDjwhajkDN83Z1611ZGnUZmvrUD
14	3QabnGEAWXrc7rvo1JcJBzUMhcifT7m6gd
15	32ZiFK53wYe5TL8zmcy7zaAvQnSd67fcA2
16	1sQ1oXjay4KwkEuVdFf7yveQFytH1ES7g
17	3PrThrqU4fhNG4LJzVT5nMDs41S7yh75Vu
18	1DnGvHRkXC7hTXuTDDxqNEwUYyhgR1nSDn
19	3J9DbduuLLU4o65Hfw29zMVoxdjkZ9CJHo
20	3MLnjFfp9VeFVQroAbENXrDyGgioT1TZJQ
21	14mNSNTp8N9ATPoyfYQCfnm8B43YjLNbwG
22	12jUCD1da5EzutFg1zWq9fhmE1dAkB5MxF
23	3Gv56YFJ5Zaue6RCDzBNFbUE7EharKXenE
24	3DJqv8q3bxSizdc47UfuGoCkAzq7QxotEV
25	35NdXGaaMV19T6yiRpNaZTN5jQiJR5F95z
26	3KiHfB5FfsEVhRowBwMDsxzT1KT9kFEsqx
27	3GfghFZjkLncctgUDdQpuZTjFHjLhH7Hn6
28	1JnweKtFaSVYZtrNs633MyAQfxv3zWybdZ
29	1PCsivNdLzKNArTewBQeXztncMRgay9A8H
30	3PZqkm88UAeYQvfgE6HnTMPgSawaLS3PCN
31	3HMhnidbjj7pRc6KrxhRv9dxsGQhfA1Mae
32	39yTYpsCpfqBmpmQgZpoE4epgr7ppSDJmK
33	31xjhbbEAsC85QynVmRRnQbL5K2UgtXXhW
34	1M34CzVZEhGfLxocxFXyNSJcrxPgoEzcHH
35	1DnKvXkfAKnBnp8WzfwCFSLakoYv9y6p6S
36	1Wdq3SJiAwcW1V7wPJWvfLF9ZcARXzXyz
37	161rhMMWhtFw4zSLgmubAfx9DkAnQxXLRs

38	1PQwHVZvEQM2A3vVQdsGy1PpR47fD25CBV
39	1A4kjy59YcYJNThyEX9nGgj7615qnXVgea
40	1iL6WtDdonsgVsPquHDKZXScyZCWTqFnQ
41	17J9tFkU7Z5tjotQJBdsUWVxfP2WWBquyb
42	1NqrxD6SatMMu2m4vEkxfYp9UQbwrEAU5j
43	1NbsPXpCa1adNNi9fKjvTsMEWUJGWodeKc
44	1UHVEwmzVn4x6gusr9G2K6UkPN8nX8ELo
45	18HxszY7vsYMvFMRNsbjZRQrS3A4r3YVS7
46	1MdYecvNGSwu7rTz3ACY9vdmxyQwkpVX14
47	1NhpCGz48W7T2umxZsz2XWwr8LvUEC1Rab
48	1JRXEW4qnbSbdmMq8efykq7tPaF9EH9AsJ
49	18woRRJNizuSjATH6mRwEuXChrQeJ9hzkj
50	1KPsvnx53VpJixUrdjaZtMouC7HK11qkV5
51	1LVwtwghTiorsXKtozvHHQCME3qRcse3DP
52	17qRPuXAu2yJd31e3Fdd8rWuiKUxsC85Nu
53	1JUmgvW6A1AP2j4FG6eMgfeQi8436G9Njd
54	1BdVWKUaUkH33oB6fYs5rN6zYj4HAv9xDe
55	1Nn2jNEpE55nq66fHxbqByRnoyWgqHuF2r
56	1NR1po4isKDrTBoV2SWPt3ibNbt4kryuju
57	1Bjd913RMgMxJyqp84Uopx5GtDUYJXbcBB
58	1PYiZensBzM7Jd3YEiDYyAxagrf8EFRaf8
59	1McrLZDNUEnB1i6qn25v7icCGSWi2ynamw
60	16xYb8rkWA4aaPpaqg8jsHreW64DHXUvW8
61	15kV9USE7keMUy4GBuBDXow7mydZ25RncJ
62	185i3gHsTe2kfzG6iQZGoyJX1bK4QhKHxu
63	1CxR1hxQYw953sy9nXhFKX3vQxKX2XuQNE
64	1NootiBHcBb1SrBp89uD1vV28r2bY1zjeB
65	1G3VhaP8E5CLrh1PXmbCwNgdWnYvVpSFzh
66	1B71wHvBgFqXzc3H9uxf3V1q8LB7XrdgDk
67	1CcEbXYSNwvN8T4e7rjgURATqgQEWRqq2J
68	1BeTdU7ymcSTHfJhYKaMhJjzeJMJWHEnCY
69	1BVjLitLbaHGZrfU7Xuj8js9fEPrtUGxut
70	1NjpNMuJ9BSocgibU1gCVJd3SHokSoi3sS
71	1J5x4is2cqHZFYDeaef2bih5WVWuvEcLdA
72	12eyVkVExHiBLyxojCZfYFfo9VE5aLY1p6
73	15WezvMKGdnBjEMYjCSa3r69ZudGzGp66t
74	1CoEM6LVSxdBUiyudqLXSSuwiy79j6Yb2X
75	1BpGu5BFS3uw8J81KCfvudQcHWnn95cRhQ
76	1FQkGKvP5FmYTvKP1qGG98SNVohxzzeZpQ
77	1Q4xwkF6mUGQHBUaWy2PusTJMCFZbXmwfc

78		1KszbucM4mBc6sQz4sGR2tRwc8Qn8VkCMS
79		15K9Zj1AU2hjT3ebZMtWqDsMv3fFxTNwpf
80		1BQAPyku1ZibWGAgd8QePpW1vAKHowqLez
81	AQ1	37yrx7sTX3VP2BC4eKbmvZiCyH15Wavx1S
82	AQ2	3LcrDjD1AJXUk2DKshRpo7CCjMmdsWQS1R
83	AQ2	372RABNMMfY6rKEHL7k4zbGS1gdQD8fN6y
84	AQ2	37CsFAjLo4ZKdUPmj2F7TYZQFnKmQG87HS
85	AQ2	3B5p2LERKDQrBjWqaEXDXcxuXUveqRAcWd
86	AQ2	3QadnFouUe4iDiCyC4ETjFawf7ec6XeT4S
87	AQ2	bc1q84ue52z2p6mxz7080f5wcfr4hfmdscvng8kydr
88	AQ2	36g1AzDkxFfmUBtBvShW9BE4qoCYwttYHE
89	AQ2	3DaEFm23S1scNf63xYJGmhNLHs9nnGNAQp
90	AQ2	331AkqgXeLxAZ9WcmEha3hBbFcJduTeqPf
91	AQ2	bc1qtpdhcm5rxf8e58aj6les0e2aqfqddtf7s2zyfl
92	AQ2	3MCa9HSAKNDJm7VToyvxmjR7nE9XEbj5W9
93	AQ2	1AyBtxgmP1MWxMSokB36t6BvAScRQWPfUY
94	AQ2	1C7rUNar8G8v5vWAqg1FkidJAj9PdAaqNq
95	AQ2	34JUtDmLkd1LkZ1eSKJ2KpRqMhSt4fNAXA
96	AQ2	3EbW7JkomWTuhMtMAv4i7bNSCEoRPktGd7
97	AQ2	3EYRY54QutwDZcUANB3RiUD1vpFYAY43Qx
98	AQ2	3FQgB6DMBeWZ7wgJCJ8NLBh7rWs4QLPPYX
99	AQ2	3LbjnkMzHBrhyn5UX6vUVzqqCbZMqhipcA
100	AQ2	1L9H7gdwyCsUk1hG2QPA2KyPKD6BWXmzXh
101	AQ2	1DzHmgAJawvA8ZawUmsxKfN1qcDHvC8JGU
102	AQ2	3L6h9mKJcmd4hn4NpZi1RdKCrs7q2AFQct
103	AQ2	3GVbjrZD8mAmH71QqPuKimPaBnNTopQv9M
104	AQ2	1NbvLuxxBtM6M21i3pNNwjtE669s1kFaPv
105	AQ2	33yRKW3uquTTiveVb9EGb7sywXD8yiEXVj
106	AQ2	35Y4ET8Lp4G4MCefPhpRTJKACe15TvEsJo
107	AQ2	3Ln5VWAfn5VfyLLhgaz7QtFPRsaz71CaJY
108	AQ2	3ErJ9qAxB6zz3wuowu9K2bdRS6ZjkE7cC8
109	AQ2	1HMDogpJTdJNKwEwnBtrP9NEQduZ351CNK
110	AQ2	3GbTitJyBLgo7oVkA6NCKa5aq7xZBNMCvG
111	AQ2	1CwVW45KkWjFeBoP1LZSESNnh8vQR2g7bG
112	AQ2	1EPnWUooTb4Cz9WpnxidRotevaZFUFfiVG
113	AQ2	1NTdgFn7q1mAtpGWzunaYgoMRriNdupfmm
114	AQ2	1KY3mPxaB4KYKhiGoJsDXYtgkQPouVn8kr
115	AQ2	18Woupz3chLHCDbjXeJWXEi7FJpYLGtpFh
116	AQ2	3DFgq7WR8ng4mQx4kTqNm1YcMokmz5H71P
117	AQ2	391TpBcg9SzwUHWK8cSAXoaMi1kKvxri3F

118	AQ2	1FbxH4UnNXXx2yMrDH9JM1nTK2uRK7tbbm
119	AQ2	1tKfLT8tL8APBDk4cS929EZ7ZnKLgYF2R
120	AQ2	34FTVSKVhTs5nnbgMyCPpdUXAA2tMnTiHZ
121	AQ2	1Pe3Emzjrhoqz5odkZRFU1Zf6qPiDaQgxP
122	AQ2	3FtCpM8a2bpTziAozbC1wHyJJ8Mf8vhHCf
123	AQ2	33868RXegKD9KJwWGNjDGhpve3SZCWtvFK
124	AQ2	3HaZrRZsepCeSWHpVkywT5ZxTuj3rgq6vb
125	AQ2	36nvxwHtFEfETZN61z7FxM7rmaXTSohrK3
126	AQ2	3FLvM3FLahm1Cg44beb1UeLxD1a8RZDzT5
127	AQ2	3MyxLuH79hFjJv5txfZky2m1QUXnyKedfP
128	AQ2	3CKqK7TaY11Hvo7JfnPMhAXGVj9hZnmYjw
129	AQ2	3JAzu5syB4JbkpC3s5gykNeRY21rChPp14
130	AQ2	35bTbKarTJoXX2N3qjz9WpECGzJG23gBsV
131	AQ2	33z7aAa52fvwNxEi3MJ2kCSytipC7nwrRj
132	AQ2	3LMnbGBJe6ZUtCArGgRhKuAXmiVkYf6WZj
133	AQ2	3M3QCf2euKqJhPEbni5bXh675pUkU3x4zC
134	AQ2	3KSuGp6RQbrFAugje78qiqkUZ4rSFoUTvK
135	AQ2	3Fij9xVYCdn9h8CdjaJBzdW7dmU8aHzWLf
136	AQ2	3N9vcfrAohotVCNJzQx2srHf69viMHhrqX
137	AQ2	3G7CuBeXcFrSyB2fkx2GvfBDYoUD2oghxR
138	AQ2	3LpaQzZUPFeR2LF55sumb9kZk4j5HdMUaC
139	AQ2	3FDNrcgT6hV8swepYLPFCALy4oZMqyxKFU
140	AQ2	3F4GniWYtwU6W1bMV432DE1Q1P9qcDHCf1
141	AQ2	3Md8xo8ug4Rm1WSLWjK3NUDaFBpyHm4hEp
142	AQ2	35tGYGmcq7Hj2M6GTDXbCYaK1Dw98xBRST
143	AQ2	3Dbv6vnbRsF9Kiqc8er2ykmSwd2g828D6F
144	AQ2	36o6t4aXtjGV8hx1Qwg6XAQ1jeUYFxUGuz
145	AQ2	3ErTJgH6QnYeUcbVq79gTmYsepapbRxiAE
146	AQ2	33VPbqSAH86mMzz8UpjZ5cJBCpMB3iCwSs
147	AQ2	3DQu9fGbsbyH5f5FeY4YmtsMHqWU7EJWGZ
148	AQ2	36DfazzthtbdpWg23bKTDh54vapjYN5ACM
149	AQ2	32nDFPvVHU3gYaB7JzduMjLGb4Vxw9JeEY
150	AQ2	3Qep64j3PbVow66j4KzB5KhwKXGmkLTc7Z
151	AQ2	395JzR5iGTFq9Qrw4iDrECtrHXGcz2wqQv
152	AQ2	1LAS42uBuCD7tpUR9RPyM61TnMee5y7aYw
153	AQ2	37qXWELabpGQZ7pich2qxZNveEMT7iYxNf
154	AQ2	1AmYvWtDbxgU2eYxEfdQRicj4hBr3k4wtv
155	AQ2	1DTzYoa85xFfKcYK4iqSfbkFHhaeZhXpA3