

UNITED STATES DISTRICT COURT

for the

_____ District of _____

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*

)
)
)
)
)

Case No.

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

The application is based on these facts:

- Continued on the attached sheet.
- Delayed notice of _____ days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

(specify reliable electronic means).

Date: _____

Judge's signature

City and state: _____

Printed name and title

Return

Case No.:
20-sc-2077

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

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

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

Account to Be Searched

This warrant applies to information which is associated with the account identified by **maher.fakhoury@gmail.com**, which is stored at premises owned, maintained, controlled, or operated by Google, LLC, a company that accepts service in Mountain View, California.

ATTACHMENT B

Particular Things to be Seized and Procedures To Facilitate Execution of the Warrant

I. Information to be disclosed by Google LLC (“PROVIDER”) to facilitate execution of the warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of PROVIDER, including any records that have been deleted but are still available to PROVIDER, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), PROVIDER is required to disclose the following information to the government corresponding to each account or identifier (“Account”) listed in Attachment A:

a. For the time period of January 1, 2014 to present: The contents of all communications and related transactional records for all PROVIDER services used by an Account subscriber/user (such as e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services, including but not limited to incoming, outgoing, and draft e-mails, messages, calls, chats, and other electronic communications; attachments to communications (including native files); source and destination addresses and header or routing information for each communication (including originating IP addresses of e-mails); the date, size, and length of each communication; and any user or device identifiers linked to each communication

(including cookies);⁵

b. For the time period of January 1, 2014 to present: The contents of all other data and related transactional records for all of PROVIDER's services used by an Account user (such as e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services, including all services referenced in paragraph (a)), including any information generated, modified, or stored by user(s) or PROVIDER in connection with the Account (such as contacts, calendar data, images, videos, notes, documents, bookmarks, profiles, device backups, and any other saved information);

c. For the time period of January 1, 2014 to present: All PROVIDER records concerning the online search and browsing history associated with the Account or its users (such as information collected through tracking cookies);

d. For the time period of January 1, 2014 to present: All records and other

⁵ Here, PROVIDER's other services include electronic communication services such as Google Voice (voice calls, voicemail, and SMS text messaging), Hangouts (instant messaging and video chats), Google+ (social networking), Google Groups (group discussions), Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser); online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries); Pixel Phone (services which support a Google smartphone); and Google Play (which allow users to purchase and download digital content, e.g., applications).

information concerning any document, or other computer file created, stored, revised, or accessed in connection with the Account or by an Account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

e. All records regarding identification of the Account, including names, addresses, telephone numbers, alternative e-mail addresses provided during registration, means and source of payment (including any credit card or bank account number), records of session times and durations (including IP addresses, cookies, device information, and other identifiers linked to those sessions), records of account registration (including the IP address, cookies, device information, and other identifiers linked to account registration), length of service and types of services utilized, account status, methods of connecting, and server log files;

f. All records pertaining to devices associated with the Account and software used to create and access the Account, including device serial numbers, instrument numbers, model types/numbers, International Mobile Equipment Identities (“IMEI”), Mobile Equipment Identifiers (“MEID”), Global Unique Identifiers (“GUID”), Electronic Serial Numbers (“ESN”), Android Device IDs, phone numbers, Media Access Control (“MAC”) addresses, operating system information, browser information, mobile network information, information regarding cookies and similar technologies, and any other unique identifiers that would assist in identifying any such device(s) including unique

application numbers and push notification tokens associated with the Account (Cloud Messaging (“GCM”));

g. Basic subscriber records and login history (including, as described in 18 U.S.C. § 2703(c)(2), names, addresses, records of session times and durations, length of service and types of service utilized, instrument numbers or other subscriber numbers or identities, and payment information) concerning any PROVIDER account (including both current and historical accounts) ever linked to the Account by a common e-mail address (such as a common recovery e-mail address), or a common telephone number, means of payment (*e.g.*, credit card number), registration or login IP addresses (during one-week period), registration or login cookies or similar technologies, or any other unique device or user identifier;

h. All information held by PROVIDER related to the location and location history of the user(s) of the Account, including geographic locations associated with the Account (including those collected for non-PROVIDER based applications), IP addresses, Global Positioning System (“GPS”) information, and information pertaining to nearby devices, Wi-Fi access points, and cell towers;

i. For the time period of January 1, 2014 to present: All records of communications between PROVIDER and any person regarding the Account, including contacts with support services and records of actions taken;

j. Information about any complaint, alert, or other indication of malware, fraud, or terms of service violation related to the Account or associated user(s), including any memoranda, correspondence, investigation files, or records of meetings or

discussions about the Account or associated user(s) (but not including confidential communications with legal counsel); and

k. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

Within **14** days of the issuance of this warrant, PROVIDER shall deliver the information set forth above via United States mail, courier, or e-mail to the following:

AUSA Jessi Camille Brooks
c/o U.S. Attorney's Office
555 4th St., N.W
Washington, D.C. 20001
Jessica.brooks@usdoj.gov

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 1956, 1960, 1030, and 2339B, as described in the affidavit submitted in support of this Warrant, including, for each Account, information pertaining to the following matters:

- (a) Information that constitutes evidence of the identification or location of the user(s) of the Account, relating to the criminal activity under investigation;
- (b) Records and information that constitute evidence concerning persons who either
 - (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or
 - (ii) communicated with the Account about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;
- (c) Records and information that constitute evidence indicating the Account user's state of mind, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation;
- (d) Information that constitutes evidence concerning how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation;
- (e) Evidence related to virtual currency addresses and transactions, accounts and the laundering of funds (both virtual and fiat currency), relating to the criminal activity under investigation;

- (f) Evidence related to transactions at virtual currency exchanges, the transfer of virtual currency, bitcoin accounts, solicitations to download attachments containing malware, and communications with third party companies about e-mail and mass mailing services, relating to the criminal activity under investigation;
- (g) Evidence relating to the funding of terrorist organizations and the criminal activity under investigation;
- (h) Records and information pertaining to any designated foreign terrorist organization, terrorist group, or terrorist, and the criminal activity under investigation;
- (i) Records and information pertaining to travel, including tickets, reservations, and schedules, relating to the criminal activity under investigation;
- (j) Records and information relating to Islamic extremism, radicalism, and violence relating to the criminal activity under investigation;
- (k) Evidence related to anti-money laundering controls, “know your customer” policies, and/or lists, names, persons, companies, and/or FinCEN regulations and to the criminal activity under investigation;
- (l) Evidence related to operation of a money service business and the exchanging of virtual currency relating to the criminal activity under investigation;
- (m) Evidence relating to malware, VPNs, and unauthorized access of computer systems, relating to the criminal activity under investigation;
- (n) Evidence related to the transportation or transmission of funds that have been

derived from a criminal offense relating to the criminal activity under investigation;

- (o) Evidence related to the transportation, transmission, or transfer of funds that are intended to be used to promote, conceal, or support unlawful activity relating to the criminal activity under investigation;
- (p) Evidence indicating the e-mail account owner's state of mind as it relates to the criminal activities under investigation;
- (q) The identity of the person(s) who created or used the **Target Accounts** or any associated user ID, including records that help reveal the whereabouts of such person(s), relating to the criminal activity under investigation.
- (r) Identification of coconspirators, accomplices, and aiders and abettors in the commission of the above offenses under investigation; and
- (s) The identity of the person(s) who communicated with the **Target Accounts** or any associated user ID about matters relating to funding terrorist organizations or assisting or supporting terrorist organizations.

III. Government procedures for warrant execution

The United States government will conduct a search of the information produced by the PROVIDER and determine which information is within the scope of the information to be seized specified in Section II. That information that is within the scope of Section II may be copied and retained by the United States.

Law enforcement personnel will then seal any information from the PROVIDER that does not fall within the scope of Section II and will not further review the information absent an order of the Court.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by _____ (“PROVIDER”), and my _____ title is _____. I am a custodian of records for PROVIDER, and I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of PROVIDER. The attached records consist of:

[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]

I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of PROVIDER, and they were made by PROVIDER as a regular practice; and

b. such records were generated by PROVIDER’s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of PROVIDER in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by PROVIDER, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
ONE ACCOUNT STORED AT PREMISES
CONTROLLED BY GOOGLE LLC
PURSUANT TO 18 U.S.C. § 2703 FOR
INVESTIGATION OF VIOLATION OF 18
U.S.C. § 1956

SW No. 20-sc-2077

Reference: USAO Ref. # 2019R01327; Subject Account: maher.fakhoury@gmail.com.

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Samuel H. Newlin-Haus, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information which is associated with account: **maher.fakhoury@gmail.com** (“Target Account 1”), which is stored at premises controlled by Google LLC (“PROVIDER”), an electronic communications services provider and/or remote computing services provider which is located in Mountain View, California. Concurrent to this application, I am also submitting two additional applications for search warrants for information. The first is associated with account: **qalonia@yahoo.com** (“Target Account 2”), which is stored at premises controlled by Oath Holdings (formerly Yahoo Holdings, Inc.), an electronic communications services provider and/or remote computing services provider which is located in Sunnyvale, California. The second is associated with two accounts: **qalonia@live.com** (“Target Account 3”); and **qalonia@hotmail.com** (“Target Account 4”), which are stored at premises controlled by Microsoft Corporation, an electronic communications services provider and/or remote computing

services provider which is located in Redmond, Washington. These four accounts are collectively referred to as the “Target Accounts.”

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require the PROVIDER to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B, using the procedures described in Section III of Attachment

3. I am a Special Agent with the Federal Bureau of Investigation. I have been in this position since March 2016. As a special agent, I attended formal training at the Federal Bureau of Investigation (“FBI”) Academy in Quantico, Virginia, in various aspects of criminal investigations dealing specifically with criminal law, money laundering, wire fraud, and various financial investigative techniques. Upon graduating the FBI Academy, I was assigned to the White Collar / Public Corruption Squad in Los Angeles, California. While assigned, I conducted complex financial crime investigations involving wire fraud, money laundering, investment fraud, financial institution fraud, and identity theft resulting in indictments.

4. I currently am assigned to the International Terrorism Task Force at the Riverside Resident Agency of the Los Angeles Field Office. Since entering duty, I have conducted numerous investigations into terrorism-related activities, including extraterritorial investigations overseas. I have attended trainings regarding counterterrorism strategies, ideology, and

international terrorism. As a result of my experience in counterterrorism investigations, I am familiar with the strategy, tactics, methods, tradecraft and techniques of terrorists and their agents. Further, I have conducted investigations specific to terrorism financing, money laundering, tax fraud, and structuring resulting in experience with individuals who obfuscate illicit money transactions. I have received training on and have extensive experience in the search of digital devices. Recently, I have received training from the FBI specific to cryptocurrency, including the identification of methods used by criminals who wish to obfuscate their actions and frustrate law enforcement investigations. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. §§ 1956 (money laundering), 1960 (operating an unlicensed money service business), 1030 (Fraud and related activity in connection with computers); and 2339B (providing material support or resources to designated foreign terrorist organizations) will be discovered in the **Target Accounts**. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, or fruits of these crimes, further described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is a “court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

I. Background

a. Bitcoin

8. 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 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.

9. 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.

10. 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.

b. Blockchain Analysis

11. 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.

12. 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.

13. 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 Business

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).

16. I am aware that a court in this District has held that a virtual currency exchanger qualifies 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. E-Gold, Ltd.*, 550 F. Supp. 2d 82, 87-97 (D.D.C. 2008).

17. 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).

II. Current Investigation Into the al-Qassam Brigades’ Terrorist Funding

18. The Federal Bureau of Investigation (“FBI”), the Internal Revenue Service (“IRS”), and the Department of Homeland Security (“HSI”) are jointly investigating Hamas’s use of social media and BTC to finance and support its terrorist organization and operations. The investigation is focused on Hamas’s military wing, the al-Qassam Brigades, and concerns possible violations of 18 U.S.C. § 1956, and 18 U.S.C. § 2339B, among other charges.

19. 18 U.S.C. § 2339B, *Providing Material Support to Designated Foreign Terrorist Organizations*, provides, in pertinent part, that:

Whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be . . . imprisoned. . . . To violate this paragraph, a person must have knowledge that the organization is a designated terrorist

organization . . . , that the organization has engaged or engages in terrorist activity . . . , or that the organization has engaged or engages in terrorism. . .

20. Section 2339A(b)(1) defines “material support or resources,” for purposes of Section 2339B, as:

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

21. 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.

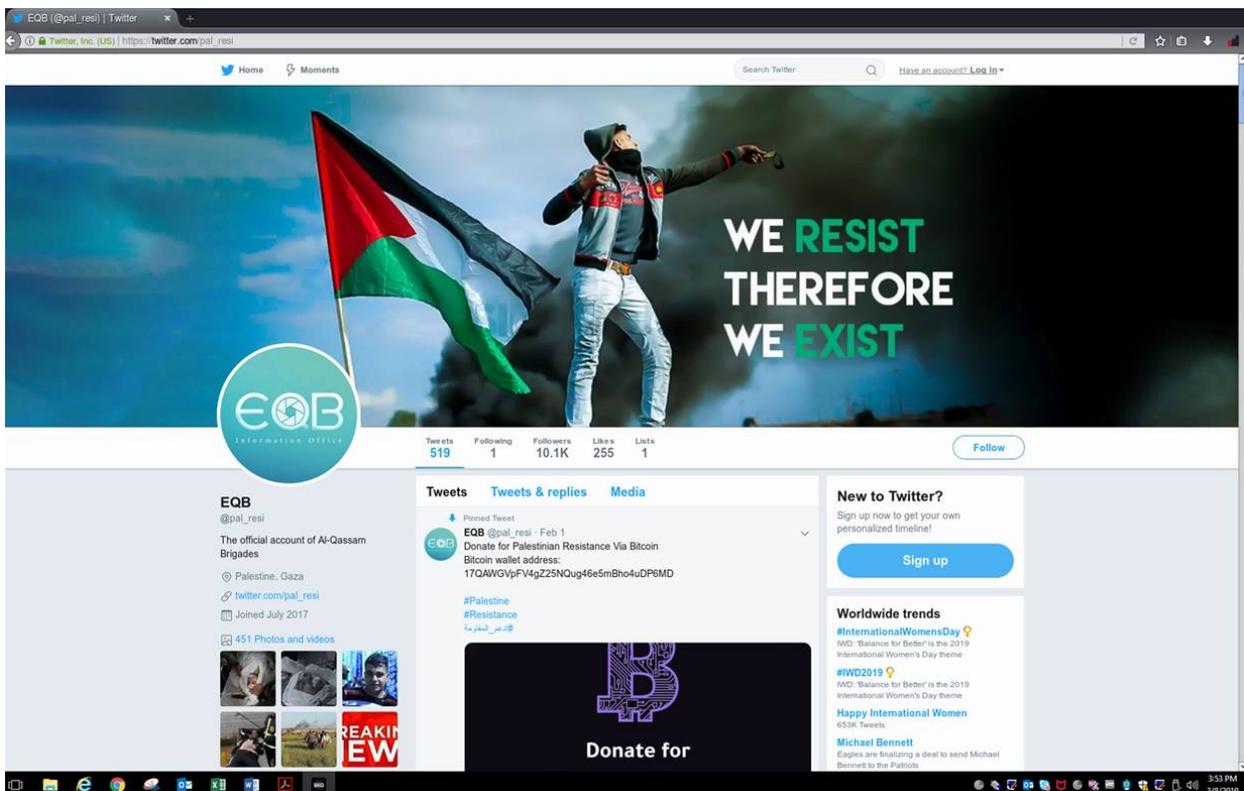
22. The Office of Foreign Assets Control (“OFAC”) has also targeted Hamas with three sanctions programs, codified at 31 C.F.R. Part 594, 31 C.F.R. Part 595, and 31 C.F.R. Part 597.

23. The State Department’s most recent annual Country Report on Terrorism from 2018 noted that the al-Qassam Brigade branch of Hamas, had conducted numerous attacks,

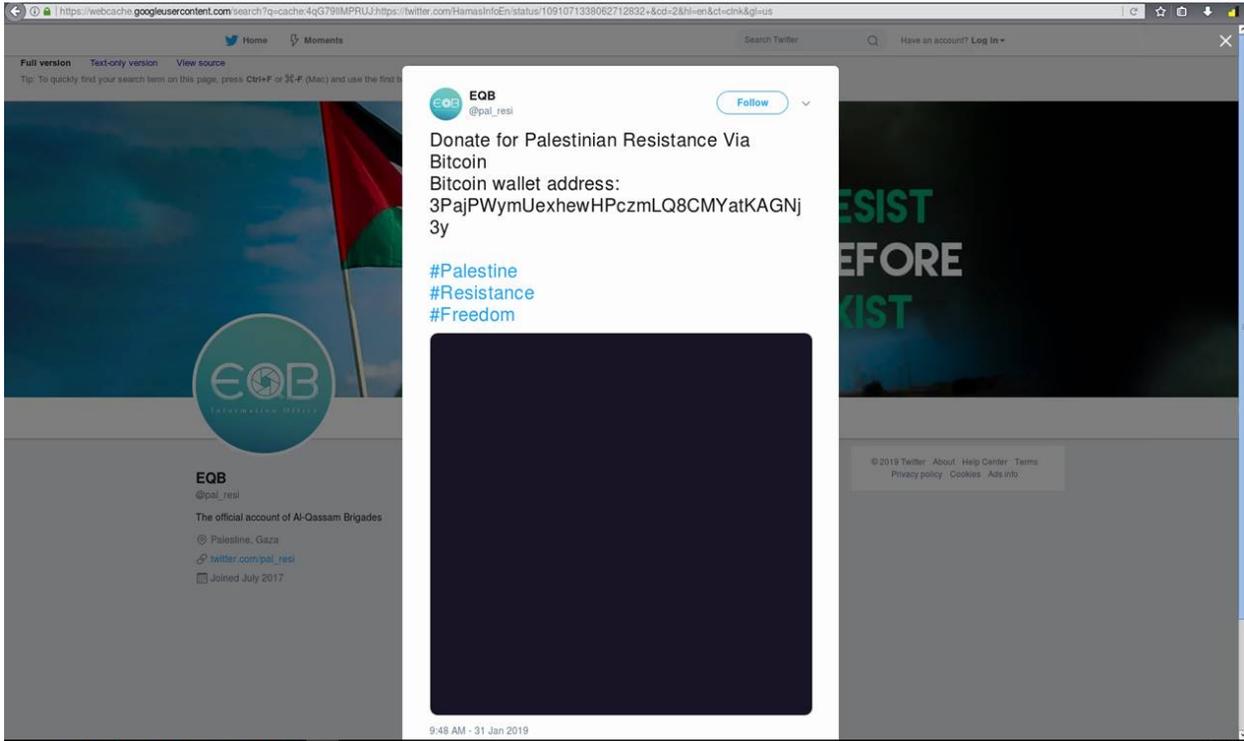
including large-scale suicide bombings against civilian targets in Israel. This annual reporting also explains that Hamas and its components, including the al-Qassam Brigade, rely heavily on donations from Palestinian expatriates around the world, including in North America.

24. On or about January 31, 2019, a user with the registered name, “alqassam brigades” opened an account with a BTC deposit address starting with 3Paj (“Hamas Account 1”) at a U.S. based BTC exchange (U.S. Exchange 1). As is the case with opening a bank account, a customer must provide identifying information in order to open an account at U.S. Exchange 1. Subpoena returns from U.S. Exchange 1 revealed that user of Hamas Account 1 provided an e-mail address to register the account and accessed U.S. Exchange 1’s platform from an IP address located within Gaza in the Palestinian territories.

25. Also on or about January 31, 2019, the al-Qassam Brigades began a public fundraising campaign, soliciting BTC donations on Twitter. The post (displayed below) called upon supporters to “Donate for Palestinian Resistance via Bitcoin.”



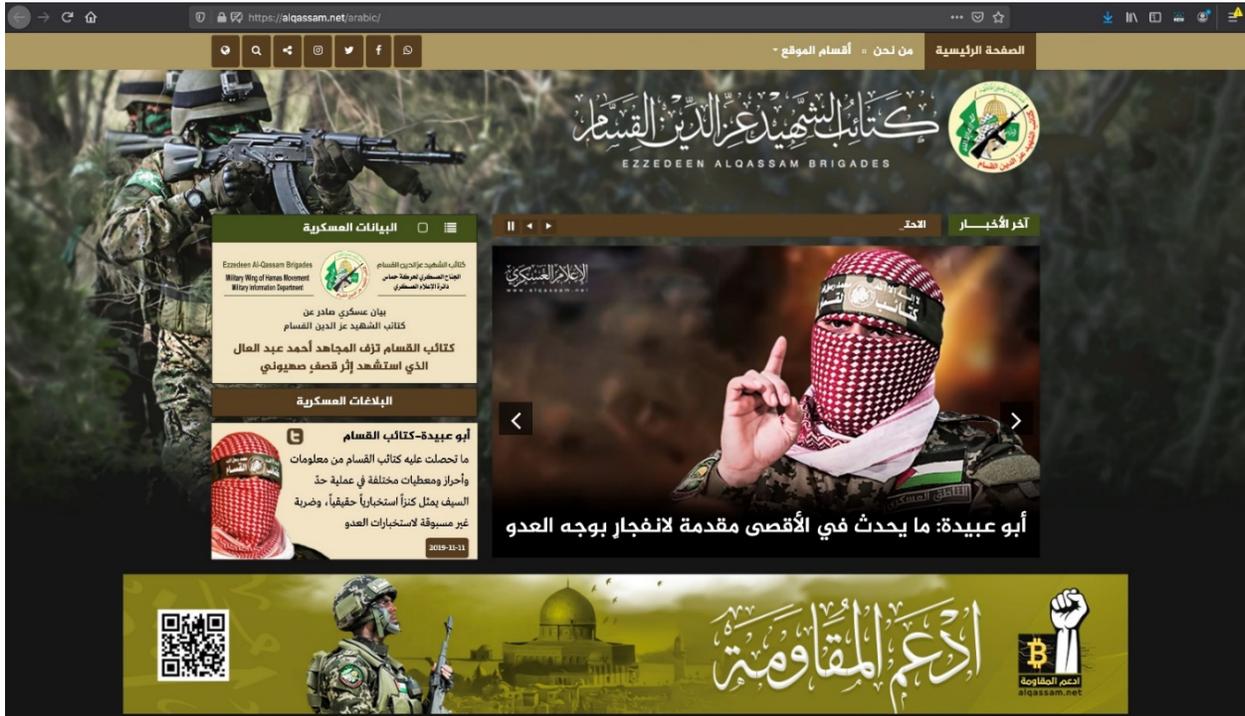
26. Clicking on the post causes another window to pop up, which provides Hamas Account 1 (i.e., a BTC deposit address starting with 3Paj) as the BTC deposit address to which donors could send their funds to the al-Qassam Brigades.



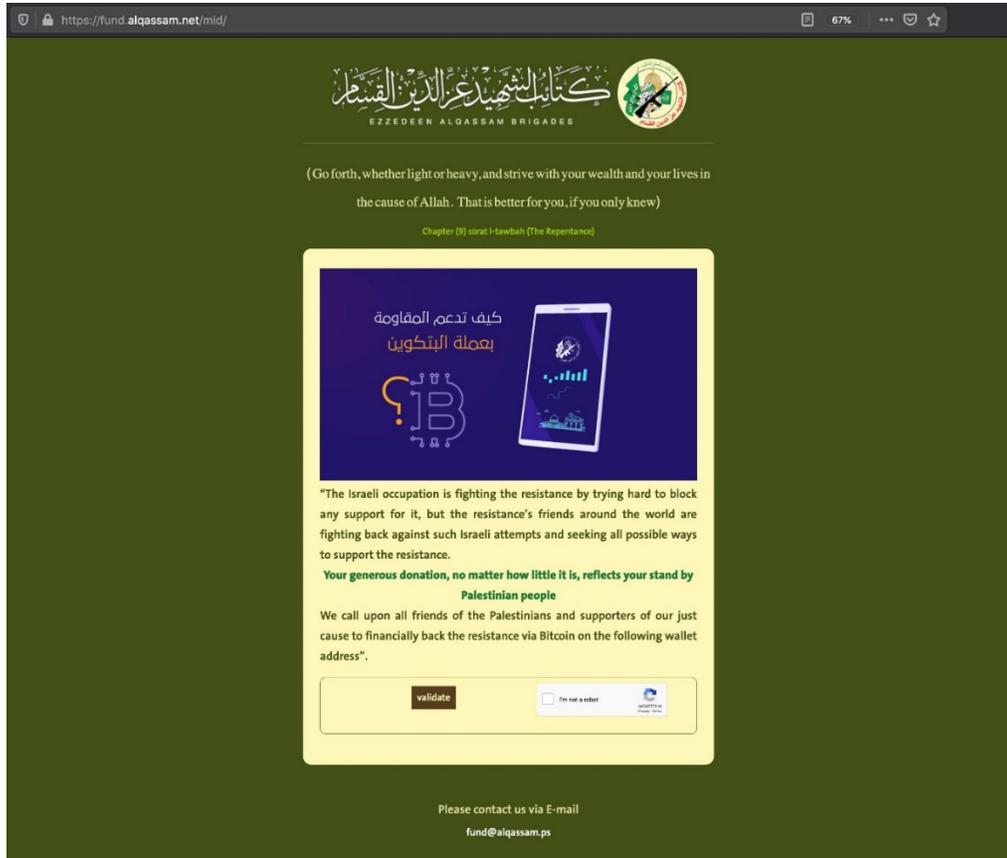
27. On or about February 1, 2019, Hamas continued its social media fundraising campaign, seeking additional BTC donations to be sent to another BTC deposit address, starting with 17QAW (“Hamas Account 2”). Using commercially-available reliable third-party Blockchain analytics software, law enforcement learned that Hamas Account 2 has been clustered (the process of which is described above) with ten other BTC deposit addresses. These ten BTC addresses comprise Hamas Account 2, because the clustering together of BTC addresses reflects common ownership/control.

28. Hamas subsequently began seeking donations to its BTC addresses on its website, alqassam.net (displayed below), which law enforcement accessed while in Washington, D.C.

Hamas also created a second official site, alqassam.ps, located on the Palestinian domain. Notably, the two websites appear to be identical, providing the same information and instructions for contacting and donating to the organization.



29. Clicking on the BTC symbol at the bottom right corner of the homepage led to the following BTC donation page on alqassam.net:



30. In total, the al-Qassam Brigades' fundraising campaign on Twitter and on the organization's two websites, Hamas Account 1 and Hamas Account 2 received more than 75 transactions of BTC totaling approximately \$6,000 worth of virtual currency donations, at the time of donations. Many of these donations were sent from U.S. and international exchanges.

31. Following the start of al-Qassam Brigades' fundraising efforts, U.S.-based exchanges subsequently began to freeze transactions to BTC addresses associated with Hamas Account 1 and Hamas Account 2 after flagging the accounts for suspected ties to terrorism finance.

32. In response to these account freezes, Hamas shifted its BTC fundraising tactics.

a. Hamas Account 1 was a static BTC address, *i.e.*, a single fixed account number that would receive donations from anyone. Exchanges could easily find the single static address.

b. Following the account freezes, Hamas changed to providing donors on its official website a dynamic BTC address system, wherein the website created a new BTC address for each individual wishing to fund Hamas. Like an e-mail address, it is typically free to create a new BTC address. There are hundreds of millions of BTC addresses currently in use.

c. Law enforcement is aware from prior investigations that the creation of unique BTC addresses is a common tactic used by websites to conceal the users laundering funds. This is in contrast to the tactic of pooling all the funds into a static BTC address that can easily be identified by law enforcement.

33. Following Hamas's shifting of tactics, reliable third-party BTC analytics software "clustered" approximately 77 BTC addresses (collectively referred to as "Hamas Account 3") connected to the Hamas website that received approximately 80 donations totaling 2.00629847 BTC (\$10,835.73 at the time of transaction). One of the 77 BTC addresses was used by a defendant already charged in the District of New Jersey for providing material support to Hamas.

34. Additionally, in response to the terrorism detection efforts by U.S.-based exchanges, Hamas published a video on its website educating donors on how to launder BTC to the new dynamic addresses. Among other tactics, the video suggests donors create BTC wallets at three trusted BTC wallet websites and then fund the trusted wallet at an exchange. This way,

the donor is not sending BTC directly from an exchange and is creating a layer between Hamas and the exchanges to help avoid detection.

35. Numerous transactions, initiated at a variety of U.S. and international exchanges by different accounts and clusters, continued from January to at least October 2019, largely laundering BTC to Hamas Account 3.

III. FAKHOURY and the Al-Qassam Brigades' BTC Fundraising Campaign **Information from SOURCE 1 Regarding FAKHOURY's Ideology**

36. In 2016, a Confidential Human Source (“SOURCE 1¹”) provided information on a conversation with FAKHOURY. SOURCE 1 identified FAKHOURY as suspicious, stating he had a lot of money and frequently traveled to Turkey and Jordan. FAKHOURY expressed support for ISIS² beginning in 2014, thinking they were the “righteous team,” saying “they’ll fight like lions.” FAKHOURY also voiced his support for Hamas.

¹ SOURCE 1 has worked with the FBI since June, 2016 and has been consistently open and forthright with all information and has provided reliable information consistent with the facts uncovered in other facets of this investigation.

² On 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 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. In an audio recording publicly released on June 29, 2014, ISIS announced a formal change of its name to the Islamic State. 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.

37. In 2017, SOURCE 1 provided additional information regarding FAKHOURY. SOURCE 1 said FAKHOURY trusted ISIS but was not directly aware of FAKHOURY providing material support to ISIS. FAKHOURY made statements indicating he believed Palestinians would be “ready” for the Israelis during their next major conflict.

Bitcoin Transactions

38. On or about February 20, 2019 and March 12, 2019, an account (“17PK”) at a U.S.-based exchange (“U.S. Exchange 2”) sent BTC to an intermediary BTC cluster totaling approximately 0.03164932 BTC. In turn, on March 24, 2019, this intermediary BTC cluster sent approximately 0.025 BTC to Hamas Account 3. The intermediary BTC cluster had no other transactions, meaning the accounts were used for the sole purpose of receiving funds from 17PK and then sending these funds to Hamas Account 3. The sending of funds in such a manner is consistent with an intermediary account appearing to act as a middleman that transfers the funds onto the intended recipient, thereby obscuring the origin of the funds. Notably, this obstruction technique is consistent with the methodology taught in the Hamas video referenced above.

39. Subpoena returns from U.S. Exchange 2 revealed 17PK was linked to Maher Fakhoury (“FAKHOURY”). The account information included an image of FAKHOURY’s driver’s license, a second photo of FAKHOURY, an address of 34675 Chinaberry Dr., Winchester, CA 92596 (“FAKHOURY’s ADDRESS”), which matched that on his driver’s license, and listed **Target Account 1** as the email address.

IV. Probable Cause Specific to Each Target Account

Target Account 1 – maher.fakhoury@gmail.com

40. 2703(d) returns from Google for **Target Account 1** showed a creation date of July 19, 2005. The account information listed the recovery email as **Target Account 3** and an “alternate” email as **Target Account 2**. The records further listed the nickname for **Target Account 1** as “qalonia.” Based on my training and experience, I know that “Qalunya” is a small Palestinian village that was destroyed during a prior armed conflict and would be used as a symbol of the Palestinian resistance.

41. A general review of **Target Account 1** header information between 2015 and 2019 revealed approximately 27 emails exchanges between **Target Accounts**. Records showed 8 emails between **Target Account 1** and **Target Account 2**, 17 emails between **Target Account 1** and **Target Account 3**, and 2 emails between **Target Account 1** and **Target Account 4**. Based on my training and experience, I know that criminals who communicate via e-mail, typically employ multiple fake identities to avoid easy detection. These fake identities are fostered through the creation and use of multiple free e-mail accounts, linked in a variety of ways.

42. Further, when criminal actors are conducting illegal activity, such as laundering proceeds for terrorists, they prefer to distance the activity from themselves as much as possible. To do so, they often create new emails to obstruct their activity and link to the criminal behavior. Each email is then utilized for a singular purpose in the overall scheme, thereby, providing an additional layer of protection between the actor and the crime. This tactic is particularly useful in schemes involving online platforms, such as virtual currency exchanges. This is because the

exchanges require, and rely on, email addresses as unique identifiers for each account. Therefore, if a criminal actor wanted to create multiple accounts at an exchange, so as not to connect illicit funds with their own, they could utilize a different email address.

43. In order to manage this number of accounts, criminal actors often have to link the accounts in some manner. Linking allows a single user the ability to access as well as reset passwords for the multiple linked accounts. The tracking and detection of linked accounts is one way by which a person and/or co-conspirators can be identified. Moreover, the linking of an account can further demonstrate who has access and/or control of an account.

44. According to 2703(d) returns, **Target Account 1** received two (2) emails on March 2, 2019 and March 12, 2019 from U.S. Exchange 2, referencing a wallet hosted at U.S. Exchange 2. Based on my training and experience, I know that private keys used to access BTC are stored in wallets at virtual currency exchanges. These two emails referencing a wallet at U.S. Exchange 2 support that FAKHOURY transacted at this exchange from 17PK, relying on said wallet. Importantly, the second email is the same date as the transaction of BTC from 17PK to the intermediary account.

45. **Target Account 1** also contained over 100 emails between 2018 and 2019 from cryptocurrency related items, such as virtual currency exchanges, and traditional money service businesses. Notably, within one day of the transactions from 17PK, on February 19, February 20, March 12, and March 13, 2019, header information from 2703(d) records showed that **Target Account 1** received approximately ten (10) emails that were apparently related to virtual currency exchanges and money service businesses.

46. A further review of header information from 2703(d) returns revealed four (4) emails sent from **Target Account 2** to **Target Account 1**, one (1) on the same date of the February 20, 2019 BTC transaction and three (3) one day earlier on February 19, 2019.

Target Account 2 – qalonia@yahoo.com

47. Information from 2703(d) returns of **Target Account 2** revealed the account was created on December 30, 2009. The records list the name associated with the account as “maher fakhoury” and the “Alternate Email Address(es)” as **Target Account 1** and **Target Account 3**.

48. A review of header information from the 2703(d) returns of **Target Account 2** starting in 2015 revealed the following information:

a. **Target Account 2** received approximately 340 emails from uspsinformeddelivery@usps.gov. Based upon a review of the public website <https://informeddelivery.usps.com/>, “informed delivery” relates to digital previews of mail and the tracking of packages. Based upon my training and experience, I know individuals who wish to obfuscate financial transactions will often utilize the mail to send or transfer cash as this makes it much more difficult for law enforcement to track.

b. **Target Account 2** engaged in approximately 30 email exchanges with **Target Account 3**. Notably, two (2) emails were sent from **Target Account 2** to **Target Account 3** on February 20, 2019 (the date 17PK sent BTC to the intermediary account) and five (5) emails were exchanged between **Target Account 3** and **Target Account 2** on February 21, 2019. Importantly, on March

24, 2019, **Target Account 3** sent an email to **Target Account 2**, which is the same date the intermediary account transferred BTC to Hamas Account 3.

c. **Target Account 2** sent four emails to **Target Account 1**, one (1) sent the same day of the February 20, 2019 BTC transaction and three (3) sent one day earlier on February 19, 2019.

d. Between 2016 and 2018, **Target Account 2** sent three emails to **Target Account 4**.

e. Since December 2018, **Target Account 2** has received approximately 19 emails from support@expressvpn.com. I know from my training and experience that ExpressVPN is a popular Virtual Private Network (“VPN”), which is frequently used by individuals who wish to hide their online activity from law enforcement.

f. Since 2018, **Target Account 2** has received approximately 69 emails with money service businesses, including Venmo, PayPal, and Ria Money Transfer, as well as with cyber security software Bitdefender. I know from my training and experience that individuals frequently use money service businesses to send cash overseas and other locations in an effort to avoid electronic bank transfers and the establishment of bank accounts. Further, money service businesses allow the transfer of money to public terminals as opposed to specific bank accounts attributed to a specific individual. Additionally, based upon my review of the website www.bitdefender.com, I know Bitdefender offers VPN

services as well as other cybersecurity features, which as explained above is frequently used by actors wishing to hide their activity from law enforcement.

49. Additional subpoena records show FAKHOURY opened an account at Venmo, a money service business, where he listed **Target Account 2** as his registered email address.

Target Account 3 – qalonia@live.com

50. Information from 2703(d) returns revealed **Target Account 3** was created on June 17, 2010. The records list the name associated with the account as “maher fakhoury” and the “Alternate Email” as **Target Account 4**.

51. A review of header information beginning in 2015 showed 102 emails between **Target Account 3** and **Target Account 2**, 41 emails between **Target Account 3** and **Target Account 1**, and 18 emails between **Target Account 3** and **Target Account 4**. Of note, 6 emails were sent between **Target Accounts** within one (1) day of the bitcoin transactions mentioned previously, including two emails from **Target Account 2** to **Target Account 3** on February 20, 2019 (the date BTC was sent from 17PK to the intermediary account), two emails from **Target Account 2** to **Target Account 3** on February 21, 2019, one email from **Target Account 2** to **Target Account 3** and **Target Account 2** on February 21, 2019, and one email from **Target Account 3** to **Target Account 2** on March 24, 2019 (the date BTC was transferred to Hamas Account 3).

52. Information from the 2703(d) return for **Target Account 3** identified several additional email addresses of note, including:

a. Hundreds of messages with email addresses relating to money transfer services, including PayPal, Western Union, MoneyGram, and Venmo, since 2016.

b. Approximately 19 cryptocurrency and virtual exchange related email addresses since December 2018, including email addresses referencing the “blockchain” and “cryptopay.”

c. Approximately 44 messages since 2017 with email addresses relating to overseas banking, including Bank of Jordan and Bank of Melbourne (Australia). Based upon my training and experience, I know individuals who wish to hide income and obfuscate monetary transactions will often set up accounts in other countries, commonly referred to as “offshore accounts.”

d. Approximately 12 emails between 2017 and 2018 involving “maher@yolopay.io,” which upon reviewing the header information showed the associated name to be “maher fakhoury.” A review of the website www.angel.co/company/yololite showed Yolopay created a product called Yololite, which the website described as a digital banking service that came with Visa prepaid cards.

e. An email from support@expressvpn.com received in April 2019, which as explained earlier, is a popular Virtual Private Network company used to hide internet activity.

f. Approximately 5 emails since 2019 with the domain “xnspy.com,” “flexispy,” and “mobilespyfaq.” I reviewed the websites www.xnspy.com,

www.flexispy.com, and www.mobilespy.com and discovered these companies provide monitoring software for phones and computers. I know from my training and experience that individuals involved in organizations conducting illicit activity often maintain a level of suspicion of those around them. Individuals use programs that record activity on phones and computers, as well as other forms of surveillance, to track activity and monitor whether information is provided to law enforcement or other investigative authorities.

53. Subpoena records from OfferUp, an online marketplace used to sell items, showed registered email addresses for an account attributed to FAKHOURY as **Target Account 3** and **Target Account 4**.

Target Account 4 – qalonia@hotmail.com

54. Information from 2703(d) returns revealed **Target Account 4** was created on April 27, 2003. The records list a name associated with the account as “maher fakhoury,” the “Alias Name” as “qalonia,” and the “billing email” as **Target Account 2**.

55. Header information obtained from the 2703(d) returns between 2015 and 2019 showed two (2) emails between **Target Account 4** and **Target Account 1**, 19 emails between **Target Account 4** and **Target Account 2**, and 9 emails between **Target Account 4** and **Target Account 3**.

56. A review of 2703(d) returns identified a message with the email address “qalonia@strimail.com,” which was on the “to” line along with **Target Account 4** and **Target Account 3** and sent from **Target Account 2** in August 2015. Header information showed the name associated with the email address to be “Maher Fakhoury.”

57. The 2703(d) returns for **Target Account 4** also revealed an email sent to “sales@alliedwallet.com” in June 2017. A review of the website www.alliedwallet.com described AlliedWallet as a merchant account provider focusing on e-commerce payment processing. According to a press release from the Federal Trade Commission in May 2019, AlliedWallet, among other actions, knowingly processed payments for merchants engaged in fraud and created fake foreign shell companies to open accounts in their names. According to information from the DEA, as referenced below, FAKHOURY and associates operated an illegal drug trafficking and money laundering organization under the façade of a legitimate business. Based upon my training and experience, businesses engaged in illegal activity and money laundering attempt to locate merchant account providers who ignore or help facilitate the illicit activity.

58. As noted above, Subpoena records from OfferUp, an online marketplace used to sell items, showed registered email addresses for an account attributed to FAKHOURY as **Target Account 3** and **Target Account 4**.

59. Apple records provided pursuant to a subpoena, also showed an account there connected to FAKHOURY, listing FAKHOURY’s ADDRESS, **Target Account 4**, and multiple registered Apple iPhones.

V. FAKHOURY’s Indictment and Arrest on Drug and Money Laundering Related Charges

60. According to the Drug Enforcement Agency (“DEA”), FAKHOURY was indicted on May 8, 2019 and arrested on May 14, 2019 for: Count 1: 21 U.S.C. §§ 802(32)(A), 813, 841(a)(1) and (b)(1)(C) and 846, Conspiracy to Distribute Controlled Substances and Controlled Substance Analogues Resulting in Death; Count 2: 21 U.S.C. §§ 802(32)(A), 813, 841(a)(1) and

(b)(1)(C) and 846, Conspiracy to Distribute Controlled Substances and Controlled Substance Analogues Resulting in Serious Bodily Injury; Count 3: 21 U.S.C. §§ 802(32)(A), 813, 841(a)(1) and (b)(1)(C) and 846, Conspiracy to Possess With Intent to Distribute Controlled Substance Analogues; and Count 4: 18 U.S.C. § 1956 (h), Conspiracy to Commit Money Laundering. Following the arrest, a superseding indictment was issued on December 18, 2019 for: Count 1: 21 U.S.C. §§ 802(32)(A), 813, 841(a)(1) and (b)(1)(C) and 846, Conspiracy to Distribute Controlled Substances and Controlled Substance Analogues Resulting in Death; Count 2: 21 U.S.C. §§ 802(32)(A), 813, 841(a)(1) and (b)(1)(C) and 846, Conspiracy to Distribute Controlled Substances and Controlled Substance Analogues Resulting in Serious Bodily Injury; Count 3: 21 U.S.C. §§ 802(32)(A), 813, 841(a)(1) and (b)(1)(C) and 846, Conspiracy to Possess With Intent to Distribute Controlled Substance Analogues; Count 4: 18 U.S.C. § 1956 (h), Conspiracy to Commit Money Laundering. *See* 19-cr-1169-AM (W.D. Tx.). The case against FAKHOURY in the Western District of Texas is ongoing.

BACKGROUND CONCERNING PROVIDER ACCOUNT

61. PROVIDER is the provider of the internet-based account identified as **Target Account 1**, or maher.fakhoury@gmail.com.

62. The PROVIDER provides their subscribers internet-based accounts that allow them to send, receive, and store e-mails online. The PROVIDER's accounts are typically identified by a single username, which serves as the subscriber's default e-mail address, but which can also function as a subscriber's username for the PROVIDER's other services, such as instant messages and remote photo or file storage.

63. Based on my training and experience, I know that the PROVIDER allows subscribers to obtain accounts by registering on the PROVIDER's website. During the registration process, the PROVIDER asks subscribers to create a username and password, and to provide basic personal information such as a name, an alternate e-mail address for backup purposes, a phone number, and in some cases a means of payment. The PROVIDER typically does not verify subscriber names. However, the PROVIDER does verify the e-mail address or phone number provided.

64. Once a subscriber has registered an account, the PROVIDER provide e-mail services that typically include folders such as an "inbox" and a "sent mail" folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber's username. The PROVIDER's subscribers can also use that same username or account in connection with other services provided by the PROVIDER³.

65. In general, user-generated content (such as e-mail) that is written using, stored on, sent from, or sent to the PROVIDER's account can be permanently stored in connection with that account, unless the subscriber deletes the material. For example, if the subscriber does not

³ Here, PROVIDER's (Google's) other services include electronic communication services such as Google Voice (voice calls, voicemail, and SMS text messaging), Hangouts (instant messaging and video chats), Google+ (social networking), Google Groups (group discussions), Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser); online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries); Pixel Phone (services which support a Google smartphone);

delete an e-mail, the e-mail can remain on the PROVIDER's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to exist on the PROVIDER's servers for a certain period of time.

66. Thus, a subscriber's PROVIDER account can be used not only for e-mail but also for other types of electronic communication, including instant messaging and photo and video sharing; voice calls, video chats, SMS text messaging; and social networking. Depending on user settings, user-generated content derived from many of these services is normally stored on the PROVIDER's servers until deleted by the subscriber. Similar to e-mails, such user-generated content can remain on the PROVIDER's servers indefinitely if not deleted by the subscriber, and even after being deleted, it may continue to be available on the PROVIDER's servers for a certain period of time. Furthermore, a PROVIDER subscriber can store contacts, calendar data, images, videos, notes, documents, bookmarks, web searches, browsing history, and various other types of information on the PROVIDER's servers. Based on my training and experience, I know that evidence of who controlled, used, and/or created a PROVIDER account may be found within such computer files and other information created or stored by the PROVIDER subscriber. Based on my training and experience, I know that the types of data discussed above can include records and communications that constitute evidence of criminal activity.

67. Based on my training and experience, I know that providers such as the PROVIDER also collect and maintain information about their subscribers, including information about their use of the PROVIDER's services. This information can include the date on which

and Google Play (which allow users to purchase and download digital content, e.g., applications).

the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. Providers such as the PROVIDER also commonly have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with other logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as the PROVIDER typically collect and maintain location data related to subscriber's use of PROVIDER's services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.

68. Based on my training and experience, I know that providers such as the PROVIDER also collect information relating to the devices used to access a subscriber's account – such as laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or "hardware," some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are actually assigned by the PROVIDER in order to track what devices are using the PROVIDER's accounts and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier ("GUID"), device serial number, mobile network information, telephone number, Media Access Control ("MAC") address, and International Mobile Equipment Identity ("IMEI"). Based on my

training and experience, I know that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other PROVIDER accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during course of the investigation was used to access the PROVIDER account.

69. Based on my training and experience, I know that providers such as the PROVIDER use cookies and similar technologies to track users visiting the PROVIDER's webpages and using its products and services. Basically, a "cookie" is a small file containing a string of characters that a website attempts to place onto a user's computer. When that computer visits again, the website will recognize the cookie and thereby identify the same user who visited before. This sort of technology can be used to track users across multiple websites and online services belonging to the PROVIDER. More sophisticated cookie technology can be used to identify users across devices and web browsers. From training and experience, I know that cookies and similar technology used by providers such as the PROVIDER may constitute evidence of the criminal activity under investigation. By linking various accounts, devices, and online activity to the same user or users, cookies and linked information can help identify who was using a PROVIDER account and determine the scope of criminal activity.

70. Based on my training and experience, I know that the PROVIDER maintains records that can link different PROVIDER accounts to one another, by virtue of common identifiers, such as common e-mail addresses, common telephone numbers, common device identifiers, common computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple PROVIDER accounts. Based on my training

and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular PROVIDER account.

71. Based on my training and experience, I know that subscribers can communicate directly with the PROVIDER about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as the PROVIDER typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

72. In summary, based on my training and experience in this context, I believe that the computers of the PROVIDER are likely to contain user-generated content such as stored electronic communications (including retrieved and un-retrieved email for the PROVIDER's subscribers), as well as PROVIDER-generated information about its subscribers and their use of the PROVIDER's services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide the PROVIDER with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

73. As explained above, information stored in connection with a PROVIDER account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal

conduct under investigation, thus enabling the United States to establish and prove each element of the offense, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with a PROVIDER account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the PROVIDER can show how and when the account was accessed or used. For example, providers such as the PROVIDER typically log the IP addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the PROVIDER account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculpate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via e-mail). Finally, stored electronic data may provide relevant insight into the user’s state of mind as it relates to the offense under investigation. For example, information in the PROVIDER account may indicate its user’s motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).⁴

⁴ At times, internet services providers such as PROVIDER can and do change the details and

**REQUEST TO SUBMIT WARRANT BY TELEPHONE
OR OTHER RELIABLE ELECTRONIC MEANS**

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

CONCLUSION

75. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on PROVIDER, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,



Samuel H. Newlin-Haus
Special Agent
Federal Bureau of Investigation

functionality of the services they offer. While the information in this section is true and accurate to the best of my knowledge and belief, I have not specifically reviewed every detail of PROVIDER's services in connection with submitting this application for a search warrant. Instead, I rely upon my training and experience, and the training and experience of others, to set forth the foregoing description for the Court.

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on this 12th day of August, 2020.

THE HONORABLE G. MICHAEL HARVEY
UNITED STATES MAGISTRATE JUDGE