

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

# UNITED STATES DISTRICT COURT

for the  
District of Columbia

In the Matter of the Search of

*(Briefly describe the property to be searched*

*or identify the person by name and address)*

INFORMATION ASSOCIATED WITH THREE ACCOUNTS STORED AT  
PREMISES CONTROLLED BY GOOGLE LLC PURSUANT TO 18 U.S.C.  
§ 2703 FOR INVESTIGATION OF VIOLATION OF 50 U.S.C. § § 1701-1705

Case No. 20-sc-01744

## 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)*:

See Attachment A, hereby incorporated by reference

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

See Attachment B, hereby incorporated by reference

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:

<i>Code Section</i>	<i>Offense Description</i>
50 U.S.C. §§ 1701-1705	Violations of the International Emergency Economic Powers Act

The application is based on these facts:

See Attached Affidavit

- 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*

Special Agent Joseph W. Ferrell

*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by \_\_\_\_\_ telephone *(specify reliable electronic means)*.

Date: 07/27/2020

City and state: Washington, D.C.



Deborah A. Robinson  
2020.07.27 10:48:04  
-04'00'

*Judge's signature*

U.S. Magistrate Judge Deborah A. Robinson

*Printed name and title*

UNITED STATES DISTRICT COURT

for the
District of Columbia

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
INFORMATION ASSOCIATED WITH THREE ACCOUNTS STORED AT
PREMISES CONTROLLED BY GOOGLE LLC PURSUANT TO 18 U.S.C.
§ 2703 FOR INVESTIGATION OF VIOLATION OF 50 U.S.C. §§ 1701-1705

Case No. 20-sc-01744

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure
of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

See Attachment A, hereby incorporated by reference

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B, hereby incorporated by reference.

YOU ARE COMMANDED to execute this warrant on or before August 10, 2020 (not to exceed 14 days)

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

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

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to Deborah A. Robinson
(United States Magistrate Judge)

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

for \_\_\_ days (not to exceed 30) until, the facts justifying, the later specific date of

Date and time issued: 07/27/2020



Handwritten signature of Deborah A. Robinson

Deborah A. Robinson
2020.07.27 10:47:31 -04'00'

Judge's signature

City and state: Washington, D.C.

U.S. Magistrate Judge Deborah A. Robinson

Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

**Return**

Case No.: 20-sc-01744	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**  
**Property to Be Searched**

This warrant applies to information which is associated with the Google LLC account(s) identified by [REDACTED] and [REDACTED] which is stored at premises owned, maintained, controlled, or operated by Google LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, 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 **April 1, 2018 to the Present**: The contents of all communications and related transactional records for all PROVIDER services used by an Account subscriber/user of the accounts set forth in Attachment A (hereinafter “the Accounts”), such as email 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 emails, 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 emails); the date, size, and length of each communication; and any user or device identifiers linked to each communication (including cookies);<sup>10</sup>

---

<sup>10</sup> 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

b. For the time period **April 1, 2018 to the Present**: The contents of all other data and related transactional records for all PROVIDER services used by an Account user of the Accounts, such as email 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 any information generated, modified, or stored by user(s) or PROVIDER in connection with the Accounts (such as contacts, calendar data, images, videos, notes, documents, bookmarks, profiles, device backups, and any other saved information);

c. For the time period **April 1, 2018 to the Present**: All PROVIDER records concerning the online search and browsing history associated with the Accounts or its users (such as information collected through tracking cookies), including but not limited to search and browsing history via Google Search and Google Analytics;

d. For the time period **April 1, 2018 to the Present**: All records and other information concerning any document, or other computer file created, stored, revised, or accessed in connection with the Accounts 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

---

(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).

of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

e. All records regarding identification of the Accounts, including names, addresses, telephone numbers, alternative email 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 Accounts and software used to create and access the Accounts, 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 (including Apple Push Notifications (“APN”), Google Cloud Messaging (“GCM”), Microsoft Push Notification Service (“MPNS”), Windows Push Notification Service (“WNS”), Amazon Device Messaging (“ADM”), Firebase Cloud Messaging (“FCM”), and Baidu Cloud Push);

g. Transactional logs of accounts provided access to shared media or documents and what modifications were made per user;

h. 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 any of the Accounts by a common email address (such as a common recovery email 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;

i. For the time period of **April 1, 2018 to the Present**: 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;

j. For the time period **April 1, 2018 to the Present**: All records of communications between PROVIDER and any person regarding any or all of the Accounts, including contacts with support services and records of actions taken;

k. Information about any complaint, alert, or other indication of malware, fraud, or terms of service violation related to the Accounts or associated user(s), including any memoranda, correspondence, investigation files, or records of meetings or discussions about any or all of the Accounts or associated user(s) (but not including confidential communications with legal counsel);  
and



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

**Joseph W. Ferrell**  
**Special Agent**  
**Federal Bureau of Investigation**  
**9325 Discovery Blvd**  
**Manassas, VA 20109**  
**Phone:** [REDACTED]

[REDACTED]

**II. Information to be seized by the government**

All information described above in Section I that constitutes evidence and instrumentalities of violations of 50 U.S.C. § 1701, *et seq.*, or attempting or conspiring to violate the same, as described in the affidavit submitted in support of this Warrant, including, for each Account, including information pertaining to the following matters:

- (a) Information that constitutes evidence of the identification or location of the user(s) of the Accounts;
- (b) Information that constitutes evidence concerning persons who either (i) collaborated in, conspired to commit, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the Accounts about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;
- (c) Information that constitutes evidence indicating any of the Account users' states of mind, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, related to the criminal activity under investigation;
- (d) Information that constitutes evidence concerning how and when any of the Accounts was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Account user;
- (e) Information that constitutes evidence related to the collection of money and/or transfer of money to Iran, including information related to financial institutions;
- (f) Information that constitutes evidence related to travel for the purpose of taking money to Iran;

(g) Information that constitutes evidence showing authority to collect money and/or transfer money to Iran at the behest of the Supreme Leader of Iran and/or the Government of Iran.

(h) Evidence constituting knowledge of export-control laws, money laundering, the Iran sanctions, structuring monetary transactions, and cash reporting requirements for overseas travel.

### **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. Such sealed information may include retaining a digital copy of all information received pursuant to the warrant to be used for authentication at trial, as needed.

**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  
THREE ACCOUNTS STORED AT  
PREMISES CONTROLLED BY  
GOOGLE LLC PURSUANT TO 18 U.S.C.  
2703 FOR INVESTIGATION OF  
VIOLATION OF 50 U.S.C. §§ 1701-1705

SC No. 20-sc-1744

Filed Under Seal

Reference: USAO Ref. [REDACTED] Subject Account(s): [REDACTED]  
[REDACTED]

AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT

I, Joseph W. Ferrell, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of applications for search warrants for information associated with four electronic accounts, [REDACTED] (“TARGET ACCOUNT 1”), [REDACTED] (“TARGET ACCOUNT 2”), and [REDACTED] (“TARGET ACCOUNT 3”), which are stored at premises controlled by Google LLC (“Google”), an electronic communications services provider and/or remote computing services provider which is headquartered at and accepts service at 1600 Amphitheatre Parkway, Mountain View, California, and [REDACTED] (“MICROSOFT TARGET ACCOUNT”), which is stored at premises maintained by Microsoft Corp. (“Microsoft”), an electronic communications

services provider and/or remote computing services provider which is headquartered and accepts services at 1 Microsoft Way, Redmond, Washington, collectively the “**TARGET ACCOUNTS.**”<sup>1</sup>

2. The information to be searched is described in the following paragraphs and in Attachment A for each provider. 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 Google and/or Microsoft to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B for each provider. 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 B.

3. I am a Special Agent with the Federal Bureau of Investigation (“FBI”). I have been in this position since May 12, 2019. Prior to joining the FBI, I served four and a half years in the United States Army, most recently as a Squad Leader in the 82nd Airborne Division, to include a ten month deployment to Afghanistan. After completing my enlistment with the Army, I was a Management Analyst on an Internal Performance Audit team with the National Science Foundation, working on an audit of government accountability for equipment purchased on multi-million dollar grants. Since joining the FBI, I have been assigned to an extraterritorial terrorism squad primarily investigating terrorism financing operations.

4. 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

---

<sup>1</sup> Your affiant is submitting separate search warrants for Microsoft and Google contemporaneously. The probable cause section of each affidavit is identical.

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.

5. 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 the International Economic Emergency Powers Act (IEEPA), Title 50, United States Code, Sections 1701-1705, have been committed by Muzzamil ZAIDI and others. There is also probable cause to search the information described in Attachment A for evidence and instrumentalities of these crimes as further described in Attachment B.

### **JURISDICTION**

6. 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). As discussed more fully below, acts or omissions in furtherance of the offenses under investigation occurred within Washington, DC. *See* 18 U.S.C. § 3237.

### **BACKGROUND**

#### **Islamic Republic of Iran**

7. Iran is an Islamic theocracy. The Supreme Leader—Ayatollah Ali Hosseini Khamenei—is the head of state and ultimate political and religious authority responsible for Iran’s domestic and foreign policies. Under Iran’s constitution, its president and executive branch are subservient to the Supreme Leader. Among other things, the Supreme Leader serves as the commander-in-chief of Iran’s armed forces and controls its intelligence and security operations.

Under the system of Veleyat-e-Faqih, Twelver Shiism considers the Government of Iran the official Islamic State and the Supreme Leader the leader of all Shi'a Muslims.

8. The United States and Iran have had no formal diplomatic relations since 1980, following the Islamic Revolution. The U.S. Secretary of State has named Iran a state sponsor of terrorism each year since 1984.

#### **Al-Mustafa International University**

9. An organization of seminaries for foreign students was established in Iran in 1979 to export Iran's revolutionary ideology abroad. In or around 1993, Khamenei took control of the institution, separating it into the Global Center for Islamic Sciences, dedicated to foreigners in Iran; and a Seminaries Abroad section, devoted to ideological training outside Iran. They were later merged into a unified Al-Mustafa International University. Al-Mustafa International University's main campus is in Qom, Iran. Funded and controlled by the Iranian government, the university trains foreign Shia clerics, religious scholars, and missionaries. It is estimated that more than 45,000 foreign clerics and scholars have graduated from the university since its inception. As discussed herein, ZAIDI started attending the university in late 2014.

#### **Khums**

10. Khums, which means "one-fifth" in Arabic, is a religious tax imposed as a jurisprudential tenant of Islam. Within Shia Islam, individuals are required to pay twenty percent of their remaining annual income to the Imam, the head of the Islamic State, through his surrogates, who are known as maraji al-taqlid (literally "sources of emulation"). As of 2017, there were 86 maraji (sing. marja) worldwide, with Khamenei being among the most prominent. Sayyid Ali al-



Husayni al-Sistani is another prominent Iranian marja, living in Iraq. Sistani is considered the leading spiritual leader of Iraqi Shia Muslims, and one of the most senior clerics in Shia Islam.

11. Khums are paid to a marja through his designated representatives, who are authorized in writing to collect on his behalf. Representatives provide official receipts as proof of payment. Without a receipt, a person's religious obligation to pay khums has not been relieved. According to a fatwa by Sistani's office, "for those who pay their religious dues that their fulfillment is not complete by just delivering their dues to an authorized agent/Wakeel, rather they are obligated to ask him for a receipt which is issued by us (our offices). Otherwise, the payer's obligation is not considered fulfilled without an official receipt even though the cause may be due to forgetfulness, inadvertent mistake, or otherwise."<sup>2</sup>

12. After collection, khums are distributed under the supervision of the marja to causes supporting and promoting Islam and to individuals in need. As the Supreme Leader of Iran, Khamenei determines how khums are used in Iran.

#### Yemen Civil War

13. Since approximately 2015, two factions have been fighting for control of Yemen: the current government of Yemen and the Houthi armed movement. According to a U.S. Department of State report on terrorism, Iran is engaged in a military campaign in Yemen to support the Houthi rebels, who share Iran's Shia ideology. Saudi Arabia—Iran's key ideological and geopolitical adversary in the region—has been backing the current Yemeni government. The United States has been providing assistance to Saudi Arabia.

---

<sup>2</sup> A fatwa is a ruling or legal opinion under Islamic law.

Islamic Pulse

14. Islamic Pulse (<http://islamicpulse.tv>) is a publicly available multimedia website that hosts images, videos, and articles about Shia Islam and Iranian culture from the perspective of the Government of Iran. It is purportedly staffed by Shia seminary students in Qom, Iran, to include ZAIDI and Ali Chawla, who is also known as “Ali Ali,” (CHAWLA). The Islamic website provides **TARGET ACCOUNT 3** to the public for all inquiries. As discussed below, CHAWLA is the subscriber of **TARGET ACCOUNT 3** (in addition to **TARGET ACCOUNT 2**).

15. Among other things, on July 6, 2019, Islamic Pulse published an approximately five-minute long, English-narrated video titled “Islamic Pulse Funds Yemen (Campaign),” (hereafter referred to as the “IP Yemen Video”). The video was uploaded to Islamic Pulse’s YouTube page around the same time. The email address associated with the YouTube page and used to upload videos to it was **TARGET ACCOUNT 3**.

16. The IP Yemen Video implores viewers to give khums or donations to Islamic Pulse’s representatives, purportedly to help victims of the Yemeni civil war. The video claims that the campaign has collected close to \$90,000 USD and that donations were coming from multiple countries, including the United States. The video further states that the campaign has received permission to collect khums on behalf of Ayatollah Khamenei, Ayatollah Sistani, and Ayatollah Makarem, and it depicts a letter written in Farsi authorizing [the campaign to collect khums; translation @ time stamp 3:49]. Finally, the video instructs viewers to send an email to **TARGET ACCOUNT 1** with the following information: 1) name; 2) city of residence; 3) state/province; 4) country; 5) amount; 6) donation or khums; and 7) name of marja, if khums. And, it explains that the campaign “will try our best to arrange a pickup of these funds through one of our representatives in your vicinity.” The Islamic Pulse YouTube page hosting the video also

contained the hashtag, “#IPfundsYemen,” which matches the username for **TARGET ACCOUNT 1**.

**RELEVANT LAW**

17. The International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701-1705, granted the President of the United States the authority to deal with unusual and extraordinary threats to the national security, foreign policy or economy of the United States. Pursuant to that authority, the President may declare a national emergency through Executive Orders that have the full force and effect of law. Among other things, IEEPA empowers the President to impose economic sanctions on a foreign country.

18. On March 15, 1995, the President issued Executive Order 12,957, which found that the actions and policies of the Government of Iran constituted an unusual and extraordinary threat and declared a national emergency under IEEPA to deal with that threat. 60 Fed. Reg. 14,615 (Mar. 17, 1995). In two subsequent Executive Orders in 1995 and 1997, the President imposed comprehensive sanctions on Iran and clarified the original declaration of a national emergency. *See* Exec. Order No. 13,059, 62 Fed. Reg. 44,531 (Aug. 21, 1997); Exec. Order No. 12,959, 60 Fed. Reg. 24,757 (May 9, 1995). Since 1997, the President has continued the national emergency with respect to Iran and the 1995 and 1997 Executive Orders.

19. To implement the sanctions, the Secretary of the Treasury, through the Office of Foreign Assets Control (OFAC), which is located in Washington, D.C., promulgated the Iranian Transactions and Sanctions Regulations (ITSR), 31 C.F.R. Part 560.

20. Absent permission from OFAC in the form of a license, the ITSR prohibits, among other things, the export, re-export, or supply, directly or indirectly, from the United States, or by a U.S. person, wherever located, of any goods or services, including financial services, to Iran or the

Government of Iran. 31 C.F.R. § 560.204. This prohibition applies to (1) the transfer of funds, directly or indirectly, from the United States or by a U.S. person, wherever located, to Iran or the Government of Iran, and (2) the provision of money remittance services, directly or indirectly, to Iran or the Government of Iran. 31 C.F.R. § 560.427.

21. The term “Government of Iran,” as used in the ITSR, includes, among other things, the state and Government of Iran, as well as any political subdivision, agency, or instrumentality thereof; and any person to the extent that such person is, or has been, acting or purporting to act, directly or indirectly, for or on behalf of the foregoing. 31 C.F.R. § 560.340. This definition includes the Supreme Leader of Iran and the Supreme Leader’s Office.

22. The ITSR further prohibits transactions or dealings within the United States or by any United States person with individuals or entities that have been placed on OFAC’s Specially Designated Nationals (SDN) List. 31 C.F.R. § 560.211. Among other things, the ITSR specifically prohibits the making of any contribution or provision of funds to, or for the benefit of, any person on the SDN List. 31 C.F.R. § 560.211(b).

23. On June 24, 2019, the President imposed sanctions on the Supreme Leader and the Supreme Leader’s Office.<sup>3</sup> Exec. Order No. 13,876; 84 Fed. Reg. 30,573 (Jun. 26, 2019). These additional steps were taken in response to “the actions of the Government of Iran and Iranian-backed proxies, particularly those taken to destabilize the Middle East [and] promote international terrorism.” Concurrently, under this new authority, OFAC added Khamenei and others to the Specially Designated National (SDN) List. Thus, as of June 24, 2019, the ITSR further prohibits

---

<sup>3</sup> The Executive Order specifically prohibits the making of donations of food, clothing, and medicine to, or for the benefit, of the Supreme Leader and his office, finding that such donations would “seriously impair . . . the ability to deal with the national emergency.”

the provision of funds to, or for the benefit of, Khamenei and his office, in addition to the prohibitions involving Iran and the Government of Iran that are described above.

24. While the ITSR authorizes the transfer of funds involving noncommercial, personal remittance to Iran or for or on behalf of an individual in Iran, it specifically prohibits such transfers individuals on the SDN List and transfers to, by, or through the Government of Iran. 31 C.F.R. § 560.550(a). Moreover, transfers that are authorized must be processed by a U.S. depository or registered securities broker or dealer and cannot involve debiting or crediting of an Iranian account. 31 C.F.R. § 560.550(a). Additionally, while a U.S. person is authorized to carry funds as a noncommercial, personal remittance to an individual in Iran, he or she is not authorized to carry such funds to, or on behalf of, individuals on the SDN List. 31 C.F.R. § 560.550(d). Moreover, U.S. persons are only authorized to carry such funds on their own behalf, and not on behalf of another person. 31 C.F.R. § 560.550(d).

25. Charitable donations of funds to Iran require a specific license from OFAC.<sup>4</sup> Noncommercial, personal remittances do not include charitable donations to or for the benefit of an entity or transfers of funds for use in supporting or operating a business, including a family-owned enterprise. 31 C.F.R. § 560.550(b).

---

<sup>4</sup> OFAC has issued a general license authorizing nongovernmental organizations (NGOs) to export or re-export services to, or related to, Iran in support of certain not-for-profit activities designed to directly benefit the Iranian people. See [https://www.treasury.gov/resource-center/sanctions/Programs/Documents/iran\\_gle.pdf](https://www.treasury.gov/resource-center/sanctions/Programs/Documents/iran_gle.pdf). The license further authorizes NGOs to transfer up to \$500,000 per year in support of such activities. The license does not, however, authorize U.S. persons to transfer financial donations directly to Iran or NGOs in Iran. Furthermore, the license does not authorize the export or re-export of services to sanctioned individuals, including, as of June 24, 2019, the Supreme Leader of Iran.

26. The ITSR further prohibits any transaction by any U.S. person or within the United States that evades or avoids, or has the purpose of evading or avoiding, or attempts to violate, any of the prohibitions contained in the ITSR. 31 C.F.R. § 560.203.

27. Under IEEPA, it is a crime to willfully violate, attempt to violate, conspire to violate, or cause a violation of any order, license, regulation, or prohibition issued by statute, including the ITSR. 50 U.S.C. § 1705(a).

#### PROBABLE CAUSE

28. The FBI is investigating Muzzamil ZAIDI and others (collectively “the subjects”) for, *inter alia*, IEEPA violations. As detailed herein, by December 5, 2018, the subjects had obtained authority to collect funds on behalf of the Supreme Leader of Iran, Khamenei. Using that authority, they produced an online video to solicit money from individuals in the United States and elsewhere and directed those individuals to make financial pledges by emailing **TARGET ACCOUNT 1**. **TARGET ACCOUNT 1** was then used to track pledges and contributions, including through a Google Document titled “Track.”

29. As explained below, there is probable cause to believe that, beginning at least as early as a 2018, ZAIDI and others conspired to and did collect and organize the collection of funds in the United States and arranged to have the funds transported to Iran and to Khamenei and his associates, knowing that it was unlawful to do so without a license. In an effort to secretly move the money from the United States to Iran and to avoid law enforcement detection, ZAIDI arranged for others who were traveling to Iran or Iraq to carry the money for him in amounts less than \$10,000; money that was sent to Iraq was planned to be carried into Iran.

30. This affidavit first sets forth the probable cause to believe that ZAIDI is involved in a conspiracy to violate IEEPA by: collecting money in the United States on behalf of the

Supreme Leader; unlawfully transferring that money from the United States to Iran and the Government of Iran without a license; unlawfully transferring that money to, and on behalf of, the Supreme Leader of Iran and the Supreme Leader's Office; and engaging in a series of transactions intended to evade the ITSR prohibitions. It then sets forth the probable cause to believe that evidence of that conspiracy will be found within each of the **TARGET ACCOUNTS**.

#### **Background**

31. ZAIDI was born in Pakistan in December 1984 and became a naturalized U.S. citizen in January 2005. His family has primarily resided in the Houston, Texas, area since their arrival to the United States in October 1999. ZAIDI has several siblings, including [REDACTED] [REDACTED] who is the subscriber of [REDACTED] as discussed below.

32. In or around August 2014, ZAIDI traveled from the United States to Qom, Iran, to attend Al-Mustafa International University. Since that time, he has primarily resided in Qom, occasionally returning to the United States. His brother [REDACTED] also resides in Qom and attends Al-Mustafa International University.

33. According to a court-authorized search of a Yahoo account attributed to ZAIDI ("ZAIDI's Yahoo Account"), on July 28, 2015, ZAIDI emailed [REDACTED] which is the email address for the Supreme Leader's public website. ZAIDI wrote, in English, that he was living in Qom and that he wanted to serve and strengthen the Islamic movement. He described himself as an American with advanced educational degrees and expressed an interest in serving the Islamic Republic in the "socio-political arena or in another field."

#### **ZAIDI's Authority to Collect Khums**

34. During a court-authorized search of ZAIDI's Google Account, the FBI seized an audio recording. The recording, which is primarily in English, is dated December 5, 2018, and

appears intended for a group audience. In the recording, ZAIDI states that it is publicly known that he is collecting khums on behalf of Khamenei.<sup>5</sup> He further states that, when he receives official authorization from Khamenei within the next several hours, he will send that information to the group. Additionally, ZAIDI mentions that he is collecting khums for Sistani and that Sistani's representative has promised him that fifty percent of the khums collected will be used to support the cause in Yemen. ZAIDI further states that, while he does not yet have absolute permission from Sistani, he will issue receipts for contributions and the office (likely referring to Sistani's office) will acknowledge the amount. Based on my training and experience and the nature of this recording and the letter described in the following paragraph, I believe that that the conspiracy and conduct at issue, including the effort to obtain authority to collect on behalf of Khamenei, began some number of months prior to December 2018, at least as early as April 2018.

35. During a court-authorized search of ZAIDI's Google Account, the FBI located a letter, hand-written in Farsi, dated December 5, 2018, giving permission to spend khums money on the people of Yemen. The letter appeared to bear the signature and stamp of Ayatollah Mohsen Araki. Ayatollah Araki is based in Tehran, Iran. He is an Iranian scholar, cleric, university lecturer and politician. Araki is a member of the Assembly of Experts in Iran, the deliberative body empowered to designate and dismiss the Supreme Leader of Iran. Members of the Assembly of Experts must be approved by the Supreme Leader of Iran before gaining membership. Araki was formerly the personal representative of Ayatollah Ali Khamenei.

---

<sup>5</sup> Although ZAIDI does not identify himself in this particular recording, your affiant submits that there is probable cause to believe that the voice is his because it was seized from his account. Moreover, FBI linguists have listened to numerous recordings in which ZAIDI does identify himself, and based on my conversations with those linguists, they believe this recording to also be ZAIDI's voice.



36. During a court-authorized search of ZAIDI's Google Account, the FBI located a second letter bearing the stamp of Ayatollah Mohsen Araki and issued on February 28, 2019. The letter was from Araki declaring that based on religious permissions by Ayatollah Khamenei and Ayatollah Sistani and in reference to a letter by Araki on December 5, 2018, that it is permissible to spend half of the khums money on the people of Yemen.

37. During a court-authorized search of ZAIDI's Google Account, the FBI seized a photograph of a khums receipt. The receipt, which is in Farsi and Arabic, is dated December 26, 2018. The receipt shows that ZAIDI received khums in the amount of 600,000 Tomans (approx. \$180 United States Dollars ("USD")) from an individual your affiant believes to be ZAIDI's brother.<sup>6</sup> A green stamp that includes the word "Khamenei" in Arabic is affixed to the receipt. Based on my training and experience, and in the context of this investigation, I believe that ZAIDI's brother paid khums to Khamenei through ZAIDI and that ZAIDI, who was in Iran at the time, sent his brother a photograph of the official receipt issued from Khamenei's office.

38. According to a court-authorized search of ZAIDI's Google Account, on February 20, 2019, CHAWLA (using **TARGET ACCOUNT 2**) sent an invitation to the following seven individuals to view and edit a spreadsheet titled "Track" in Google Docs: ZAIDI, [REDACTED] using [REDACTED], CHAWLA (using **TARGET ACCOUNT 3**), [REDACTED]

[REDACTED] Based on the evidence, I believe this spreadsheet was an initial attempt to keep track of contributions to the Campaign to Save Yemen. As discussed below, a second "Track" document was then used for the same purpose once **TARGET ACCOUNT 1** was created.

---

<sup>6</sup> [REDACTED] Tomans are a unit of the official currency of Iran.

**ZAIDI's Collection of Khums in the United States**

39. As discussed below in paragraph 71, according to Google subscriber records, **TARGET ACCOUNT 1** was created on June 4, 2019.

40. According to U.S. Customs and Border Protection (CBP) records, ZAIDI returned to the United States on June 9, 2019, arriving in Houston.

41. As previously discussed, the President imposed sanctions on Khamenei and his office on June 24, 2019. According to court-authorized surveillance, on June 25, 2019, ZAIDI and another individual discussed the new sanctions. Specifically, ZAIDI said that “they have placed sanctions on our father.” ZAIDI stated that they should seek legal advice, because, “if the khums are being collected in the name of that person [father], anything that has to do with them would be flagged.” Based on my knowledge and experience, including the timing of the statement relative to the imposition of the sanctions, ZAIDI was referring to the Supreme Leader as “father.” According to a court-authorized search of a Google account attributed to ZAIDI, on July 7, 2019, ZAIDI searched Google for “ofac countries” and then visited the U.S. Treasury Department’s publicly available website that provides information about OFAC and its sanctions programs, including sanctions against Iran and Khamenei.<sup>7</sup>

42. As described in paragraph 15 and 16, the IP Yemen Video was published on July 6, 2019, and **TARGET ACCOUNT 3** was used to upload the video to Islamic Pulse’s YouTube page. ZAIDI appears to have been involved in producing the video. According to a court-authorized search of ZAIDI’s Google Account, on June 1, 2019, an individual sent a near-verbatim

---

<sup>7</sup> Additionally, on March 4, 2019, ZAIDI searched Google for “is carrying money from america to iran for an american citizen illegal.” On or about the same day, he visited a publicly available online travel forum on the topic of “U.S. Customs Restrictions for Americans Visiting Iran.”

transcript of the IP Yemen Video to ZAIDI. The individual wrote, in part, “The length of the script may be too long . . . . But I’ll leave that editing side to you. . . . If you want me to remove something/add something then let me know.”

43. According to a court-authorized search of ZAIDI’s Google Account, on July 9, 2019, **TARGET ACCOUNT 1** emailed ZAIDI an invitation to view and edit a spreadsheet labeled “Track” in Google Docs. Based on my training and experience, and in the context of this investigation, to include the importance of tracking *khums* information and receipts as laid out above, I believe that ZAIDI was given access to a document stored in **TARGET ACCOUNT 1** that was created to keep track of information related to the collection of khums and donations, such as the amount a person paid, the person’s location, and the name of the marja who will receive the money.

44. Between approximately June 2019 and at least October 2019, ZAIDI collected khums and donations from individuals in the United States. For example, according to court-authorized surveillance, on August 27, 2019, ZAIDI engaged in a conversation via text message, with a woman in the United States. In that conversation, ZAIDI informed the woman that he was told to reach out to her by the Islamic Pulse team, and he referenced the IP Funds Yemen video. ZAIDI agreed to call her, and the text conversation later reflects that she agreed to make a donation of “800.” She asked whether to send “them” an email to say how much money was sent. Based on my training and experience, and in the context of this investigation, I submit that there is probable cause to believe that ZAIDI was attempting to collect a donation from an individual who had emailed **TARGET ACCOUNT 1** in response to the IP Yemen Video. Further, I believe that ZAIDI was directing the individual to email **TARGET ACCOUNT 1** in order to receive a receipt for the donation.

45. As another example, according to court-authorized surveillance, on September 17, 2019, a U.S.-based person told ZAIDI that someone was paying “three” but that “he has not received the email from us.” ZAIDI responded that he would inform “Brother Ali Ali.” Based on my training and experience, and in the context of this investigation, I believe that ZAIDI was being informed that someone was paying \$3,000 to Islamic Pulse’s Yemen campaign and that the person had not yet received a receipt or some other communication from **TARGET ACCOUNT 1**. Further, ZAIDI was going to inform the administrator of Islamic Pulse, “Ali Ali,” of the failure to issue a receipt. I submit that there is probable cause to believe that “Ali Ali” is CHAWLA, based on the information in paragraphs 72 and 73 below.

*Collection of Funds for ZAIDI*

46. According to court-authorized surveillance, on August 9, 2019, [REDACTED] [REDACTED] called ZAIDI to discuss money he collected to send to ZAIDI. [REDACTED] was with [REDACTED], who was dispatched by ZAIDI to collect the funds. [REDACTED] informed ZAIDI that there was an issue as “all the cash he had [was] in his bank account and his ATM had a cash withdrawal limit.” The cash withdrawal limit was \$700.00. [REDACTED] acknowledged that [REDACTED] would “return next week and by that time he [REDACTED] will withdraw all of it.” [REDACTED] opined that by “that time there might be more collection added to it since there were two to three donors more who were out of town and they are in his friends circle.” [REDACTED] asked ZAIDI if he was fine with that plan and ZAIDI said “that is fine.”

47. [REDACTED] According to information provided by [REDACTED] a U.S.-based company that allows people to send funds to each other electronically, [REDACTED] maintains a [REDACTED] account tied to the phone number he used to communicate with Zaidi, [REDACTED] 0746, and the email account [REDACTED] [REDACTED] statement contained at least three entries on or around August 2, 2019, August 10, 2019 and August 17, 2019 identified as “Islamic Pulse funds Yemen,”

“Yemen,” and “Yemen funds.” I understand that [REDACTED] often sends an email with transaction details to a user’s registered email account when that user completes a transaction.

48. [REDACTED] According to records obtained from [REDACTED] where [REDACTED] maintains a bank account, on August 9, 2019 an entry was identified as an ATM withdrawal of \$700.00. This withdrawal is consistent with the aforementioned conversation [REDACTED] had with ZAIDI on the same day. Approximately eight days later, on or around August 15, 2019, an entry in th [REDACTED] records for [REDACTED] account shows a teller cash withdrawal of \$4,900.00.

#### **Movement of Money to Iran**

49. ZAIDI enlisted others to transport the money collected in the United States to Iran on at least four occasions. ZAIDI intentionally caused each person to carry less than \$10,000 out of the United States, to avoid CBP reporting requirements. Specifically, as discussed below, ZAIDI sent money on August 23, 2019, with an individual named [REDACTED]; on September 5, 2019, with his [REDACTED]; on October 9, 2019, with an individual named [REDACTED] and on October 12 and 13, 2019, with multiple individuals who were traveling to Iraq for a religious pilgrimage. [REDACTED] also personally traveled to Iraq on October 16, 2019, and then from Iraq to Iran, before returning to the United States on October 27, 2019.

---

[REDACTED] *Travel to Iran*

50. According to court-authorized surveillance, on August 13, 2019, ZAIDI told an individual (hereafter "INDIVIDUAL #1") that he (ZAIDI) can send money with [REDACTED] who is leaving soon. I submit that there is probable cause to believe that [REDACTED] is a U.S. person named [REDACTED] based in part on court-authorized surveillance that captured a telephone call between ZAIDI and [REDACTED] on August 21, 2019, where they discuss how much [REDACTED] will take for ZAIDI. ZAIDI told [REDACTED] that his contact in Iran, [REDACTED], would take [REDACTED] to the Islamic Pulse studio for a tour and introduce [REDACTED] to [REDACTED] (appeared in and narrated the IP Funds Yemen video). Moreover, according to CBP records, an individual named [REDACTED] traveled from Houston to Iran on August 23, 2019, and returned on September 6, 2019. In a conversation with one of his [REDACTED] on September 5, 2019, which is discussed below, ZAIDI stated that he had sent [REDACTED] fully packed."

*ZAIDI's* [REDACTED] *Travel to Iran*

51. According to court-authorized surveillance, on September 4, 2019, ZAIDI told an individual that his family was leaving in case the individual wanted to send money. After ZAIDI mocked the individual for only giving "\$50 per month," the individual agreed to give "\$500" per month.

52. According to court-authorized surveillance, on September 5, 2019, ZAIDI and an individual believed to be one of his [REDACTED] had a conversation about khums and sending money to Iran. Specifically, ZAIDI asked [REDACTED] how much money he was sending with their [REDACTED] [REDACTED] replied "around five or six." ZAIDI then asked [REDACTED] if his [ZAIDI's] [REDACTED] could carry ten or if their [REDACTED] five would be part of the ten. [REDACTED] responded that it should be separate since their tickets were separate and that they can say that the [REDACTED] is not part of the family since

her ticket was booked separately. Based on my training and experience, and in the context of this investigation, I believe that ZAIDI and his [REDACTED] were discussing how to maximize the amount of money that ZAIDI's [REDACTED] could each carry to avoid CBP's \$10,000 reporting requirement for households traveling together.

53. In the same conversation [REDACTED] told ZAIDI that he has to give ZAIDI khums in the amount of "\$6,200." [REDACTED] then mentioned to ZAIDI that [REDACTED] had just traveled "there," which your affiant submits there is probable cause to believe is a reference to [REDACTED] [REDACTED] travel to Iran on August 23, 2019. ZAIDI acknowledged [REDACTED] travel and told [REDACTED] that he had sent him "fully packed," which your affiant believes is a reference to [REDACTED] carrying up to \$10,000 for ZAIDI. Per the aforementioned conversation with ZAIDI, [REDACTED] agreed to carry \$9500; \$3000 of his own money and \$6500 for ZAIDI. ZAIDI further told [REDACTED] that it is not just [REDACTED] money that needs to be sent, which your affiant believes is a reference to ZAIDI's collection of khums from others in the United States.

54. According to CBP records, ZAIDI's [REDACTED] traveled to Iran on September 5, 2019. During their departure, CBP referred them to secondary inspection where they were questioned. During the interview, ZAIDI's [REDACTED] stated that her [REDACTED] resided in a different household. When asked, ZAIDI's [REDACTED] stated that she was traveling with \$6,500 USD; CBP verified the exact amount to be \$6,582. ZAIDI's [REDACTED] stated that she was traveling with \$6,000; CBP verified the exact amount to be \$6,578. ZAIDI's [REDACTED] told CBP that ZAIDI had given her the money. ZAIDI's mother claimed that her son, ZAIDI's [REDACTED] provided her the money.

55. According to court-authorized surveillance, at some point prior to or during the secondary inspection, ZAIDI's [REDACTED] called ZAIDI. She asked him whether she should take out the money from the orange envelope to show CBP or if she can show them the envelope, which

had a name written on it. At first, ZAIDI directed his [REDACTED] not to show CBP the envelope; after she told him that the name is of the “maulana” (a title of respect for Muslim religious scholars), he told her to show the money to CBP with the envelope, since “it was merely the name of the maulana.” During the conversation, ZAIDI also directed his [REDACTED] to tell CBP that she is traveling separately.

56. ZAIDI's [REDACTED] returned to the United States on October 29, 2019. CBP referred ZAIDI's [REDACTED] to secondary inspection where she was questioned. ZAIDI's [REDACTED] initially claimed, contrary to her prior statement to CBP, that she had left the United States with \$1,000 to \$1,500 of her own personal money. Almost immediately, she remembered that ZAIDI had given money to his [REDACTED] who then split the amount, giving her \$6,578. When asked what she did with the money in Iran, ZAIDI's [REDACTED] appeared confused and had difficulty responding. Eventually, she stated that she returned the money to ZAIDI's [REDACTED] who handed the money to ZAIDI. ZAIDI's [REDACTED] further stated ZAIDI's [REDACTED] did not carry the entire sum, because she knew that the limit was \$10,000 per person. She also explained that the money came from friends, associates, and family who trusted ZAIDI with the money to distribute to needy people. When asked where the money would go, she replied that she overheard her male [REDACTED] including ZAIDI, discuss the money going to Yemen, Iran, and other countries. She further stated that each time money was taken out of the U.S. it was in increments of \$8,000 to \$10,000. As noted above, when questioned while leaving the United States, ZAIDI's [REDACTED] originally told CBP that her son had provided her money to cover her expenses traveling to Pakistan. However, upon her return to the United States, ZAIDI's [REDACTED] admitted that the entire amount was provided by ZAIDI and split between herself and ZAIDI's [REDACTED] to evade reporting requirements.



57. ZAIDI's mother also told CBP officers that another one of her sons, [REDACTED] lived in Qom, Iran pursuing religious studies. [REDACTED] was also involved in collecting money. ZAIDI's mother affirmed that "[REDACTED] and Muzzamil [ZAIDI] have different people that take money outside of the U.S."

*[REDACTED] Travel to Iran with money for ZAIDI*

58. According to court-authorized surveillance, on September 26, 2019, [REDACTED] informed ZAIDI that he was traveling to Iran on October 9, 2019, and from there to Iraq on October 11, 2019. Based on telephone records reviewed by the FBI, ZAIDI and [REDACTED] appear to be friends. ZAIDI asked [REDACTED] if he could carry money for him. [REDACTED] responded that he could take up to \$5,000. When ZAIDI asked [REDACTED] for his account number, he told ZAIDI that he was in Washington, DC. ZAIDI then said that he would give the money to [REDACTED] to give to [REDACTED]

59. According to CBP records, on October 9, 2019, [REDACTED] traveled from the Washington, DC area to Iran. CBP referred [REDACTED] to secondary inspection, where he was questioned. During the interview he stated that he was carrying \$3,000 of his own money and \$5,000 for someone else; CBP verified that the actual amounts were \$3,000 and \$4,000. [REDACTED] claimed that his brother-in-law, [REDACTED] gave him the money to give to an unknown person in Iran for an unknown purpose.

*Individuals Traveling to Iraq for Religious Pilgrimage*

60. [REDACTED] Arba'een is an Islamic religious pilgrimage that takes place yearly in Karbala, Iraq. In 2019, Arba'een took place in late October. The Arba'een Pilgrimage is held at the end of the 40-day mourning period following Ashura, the religious ritual for the commemoration of martyrdom of the grandson of Prophet Mohammad and the third Shia Imam, Husayn ibn Ali. On

the routes of the pilgrimage, food, accommodation and other services are provided for free by volunteers.

61. According to court-authorized surveillance, on September 24, 2019, ZAIDI asked his [REDACTED] [REDACTED] whether [REDACTED] spoken to someone “about bringing money as there will be people coming from Iraq and they will be able to take it back with them.” During the conversation, ZAIDI confirmed that there were people coming to Iran from Iraq. Based on my training and experience, and in the context of this investigation, I submit that there is probable cause to believe that ZAIDI was arranging for individuals to transport money to Iraq and then for others to transport the money from Iraq to Iran.

62. According to court-authorized surveillance, on October 12, 2019, ZAIDI asked an individual identified as [REDACTED] to take “\$7,000” of ZAIDI’s money. [REDACTED] agreed and further informed ZAIDI that [REDACTED] would be traveling on the same flight. Your affiant believes that [REDACTED] is [REDACTED] as discussed below.

63. According to CBP records, on or about October 12, 2019, a group of approximately 25 individuals traveled from Houston to Iraq for pilgrimage. [REDACTED] was part of the group. On October 13, 2019, [REDACTED] and [REDACTED] also traveled from Houston to Iraq for pilgrimage. During their departures, CBP referred the three men to secondary inspection where they were each questioned. During [REDACTED] interview, he stated that he was traveling with \$4,000; CBP verified the amount. During [REDACTED] interview, he stated that he was traveling with about \$7,900 and that the money was his; CBP did not document whether the amount was verified or not. During [REDACTED] interview, he stated that he was traveling with \$7,000 and that the money was his; CBP verified the amount.

64. According to court-authorized surveillance, on October 13, 2019, [REDACTED] told ZAIDI that he was leaving for Iraq and was purchasing his ticket that same day. ZAIDI informed [REDACTED] that he would be taking "\$7,000."

65. According to court-authorized surveillance, on October 13, 2019, ZAIDI told INDIVIDUAL #1 that "they" took pictures of "the currency." He further stated that "he does not want to say that it is nothing." INDIVIDUAL #1 responded that "it cannot be ignored but it cannot also be blown out of proportion." Based on my training and experience, and in the context of this investigation, I believe that ZAIDI and INDIVIDUAL #1 were discussing CBP's secondary inspections of [REDACTED] and others and were surmising that it was possible that law enforcement had learned about ZAIDI's scheme.

66. According to court-authorized surveillance, on or about October 15, 2019, ZAIDI told INDIVIDUAL #1 that he was picking up money from [REDACTED] whom your affiant believes to be [REDACTED]. According to ZAIDI, [REDACTED] did not travel to Iraq as planned.

67. During the same conversation, ZAIDI further stated that he "hates accounting and calculations" and that "he spent two to three hours figuring things out." Additionally, he told the person he was speaking to ("INDIVIDUAL #1") that "he thought he had sent 49 but had actually given 45." Based on my training and experience, and in the context of this investigation, I believe ZAIDI was explaining to INDIVIDUAL #1 that he had sent \$45,000 to Iran with the group who had traveled to Iraq.

68. According to court-authorized surveillance, on October 16, 2019, ZAIDI and a different individual ("INDIVIDUAL #2") discussed how CBP had stopped the group that was traveling to Iraq. INDIVIDUAL #2 was angry with ZAIDI for asking "[REDACTED] to call him [INDIVIDUAL #2] to say "farewell." ZAIDI responded that his only intention was to check on

“ [REDACTED] safety” and that “all of these guys have left safely.” Later in the conversation, the individual reminded ZAIDI that [REDACTED] had been stopped and that “everything was accounted for,” including “the receipts.” ZAIDI responded that he would never put INDIVIDUAL #2 in harm’s way. Based on my training and experience, and in the context of this investigation, I believe that ZAIDI and the individual were discussing how CBP had stopped [REDACTED] and the others who were transporting money out of the United States for ZAIDI.

ZAIDI’s Travel to Iraq and Iran

69. According to CBP records, on October 16, 2019, ZAIDI traveled from the United States to Iraq before returning to the United States from Iran on October 27, 2019. During his departure, CBP referred him to secondary inspection, where he was questioned. During his interview, ZAIDI stated that he was traveling to Iraq for pilgrimage and that he was meeting his family and friends there. He also stated that during his trip to Iraq he was planning to visit Iran for five days to see his wife and children. He declared that he was traveling with around \$1,900; CBP verified the amount was \$1,885.

70. During a Court-authorized search of ZAIDI’s Google Account, the FBI found an audio recording dated October 22, 2019. In that recording, ZAIDI was asked by INDIVIDUAL #3 “if it is confirmed that people from Iran are going to Iraq.” INDIVIDUAL #3 stated that he had heard that those people are unable to obtain visas and that “he wants to confirm because he is about to send the money with someone.” INDIVIDUAL #3 further stated that “if people are coming to Arba’in [the pilgrimage in Iraq] than he can give it to them there.” Based on my training and experience, and in the context of this investigation, I believe that ZAIDI and the individual were discussing how to move money from Iraq to Iran.

**Connection of TARGET ACCOUNTS to ZAIDI's Scheme**

71. According to records obtained from Google, **TARGET ACCOUNT 1** was created on June 4, 2019, by an individual identified as [REDACTED]. The narrator of the IP Yemen Video is believed to be a British national named [REDACTED] who shares the same surname as the listed subscriber. In addition, as described above, the IP Yemen Video instructs viewers to send an email to **TARGET ACCOUNT 1** with the following information: 1) name; 2) city of residence; 3) state/province; 4) country; 5) amount; 6) donation or khums; and 7) name of marja, if khums. And, it explains that the campaign “will try our best to arrange a pickup of these funds through one of our representatives in your vicinity.” The Islamic Pulse YouTube page hosting the video also contained the hashtag, “#IPfundsYemen,” which matches the username for **TARGET ACCOUNT 1**.

72. On February 21, 2020, a preservation letter was served on Google, pursuant to 18 U.S.C. § 2703(f), for **TARGET ACCOUNT 1**. A second preservation letter was served on May 25, 2020.

73. Islamic Pulse uploaded the aforementioned IP Yemen Video to YouTube using **TARGET ACCOUNT 3**. **TARGET ACCOUNT 3** was listed as the contact account for inquiries to Islamic Pulse. Information provided by Google identified the recovery account for **TARGET ACCOUNT 3** as **TARGET ACCOUNT 2**, with Recovery SMS identified as [REDACTED] 2593. According to Google records, the account holder for **TARGET ACCOUNT 2** was identified as ALI CHAWLA, who uses the alias “AliAli.” CHAWLA identified his email address as **TARGET ACCOUNT 2**, along with his alias of “AliAli,” during interviews with FBI agents on or around February 7, 2014, and on or around May 16, 2014.

74. CHAWLA's Iranian phone number, [REDACTED] 2593, was identified in a communication soliciting funds for the IP Yemen campaign. Your affiant believes that, because his email account is listed as the recovery account for **TARGET ACCOUNT 3**, CHAWLA operates both accounts and performs administrative functions for Islamic Pulse. In your affiant's knowledge and experience, the function of the recovery account is to re-establish access and/or administer the primary account thereby making CHAWLA the administrator of both accounts. In an article titled, "Foreign Students in Qom Mark Anniversary of Islamic Revolution," dated February 24, 2020, the publication the "Tehran Times," identified CHAWLA as the director of both Islamic Pulse and another website, Purestream Media. The article referred to CHAWLA as "Shaykh Ali" and "one of the key speakers at the event." In the same article, ZAIDI was identified as the event emcee. Further, on or around August 5, 2015, CHAWLA sent ZAIDI an invitation to edit a Google doc titled, "(Muzzamil) Time & Work Sheet," indicating a working relationship with ZAIDI.

75. On or around February 20, 2019, CHAWLA, using **TARGET ACCOUNT 2**, sent an invitation to edit a Google doc to [REDACTED] along with ZAIDI's Google Account and six other individuals, including CHAWLA himself. The Google doc was identified by the title "Track," the same title of the Google doc shared with ZAIDI on July 9, 2019, by **TARGET ACCOUNT 1**. Moreover, as described in paragraphs 35 and 36, this email was sent on February 20, 2019, which is after December 5, 2018, the date ZAIDI was given authority by Ayatollah Araki to collect khums and shortly before the authority was finalized on behalf of Khomeini on February 26, 2019. Based on my training and experience, your affiant submits that, based on this timing, the importance of tracking khums, the identical file name, and the fact that CHAWLA sent both invitations to edit

the document to ZAIDI (and the first to others involved), there is probable cause to believe that Google doc was used to track donations to the IP Yemen Campaign.

76. According to information provided by [REDACTED] [REDACTED] maintains a [REDACTED] account tied to the phone number he used to communicate with ZAIDI, [REDACTED] 0746, and the **MICROSOFT TARGET ACCOUNT**. [REDACTED] [REDACTED] statement contained at least three entries on or around August 2, 2019, August 10, 2019 and August 17, 2019 identified in the notes as “Islamic Pulse funds Yemen,” “Yemen,” and “Yemen funds.” As [REDACTED] email account is tied to the [REDACTED] account, and [REDACTED] often uses emails to communicate with their account-holders, including sending transaction receipts via email, in your affiant’s knowledge and experience, there is probable cause to believe information associated to these transactions and others is contained in the **MICROSOFT TARGET ACCOUNT**.

#### **BACKGROUND CONCERNING GOOGLE LLC**

77. Google LLC is the provider of **TARGET ACCOUNTS 1 through 3**. Google provides its subscribers internet-based accounts that allow them to send, receive, and store emails online. Google email accounts are typically identified by a single username, which serves as the subscriber’s default email address, but which can also function as a subscriber’s username for other Google services, such as instant messages and remote photo or file storage.

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

79. Once a subscriber has registered an account, Google provides email 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. Google subscribers can also use that same username or account in connection with other services provided by Google.<sup>8</sup>

80. In your affiant’s knowledge and experience, a Google account offers a unified login allowing end-user access to multiple Google services, including those noted in the preceding paragraph. Access, activity, and use of the various Google services is recorded and stored per user within the user’s Google account, which is identifiable by the user’s Google email address (also referred to and known as a Google username). Google services are accessible only to users who create a Google account. After creation of a Google account, users have access to the full suite of Google services. As such, a user’s Google account encompasses all aspects of the user’s online activity associated with Google.

81. As described above, the subjects used email, online searches, cloud storage, photographs, word processing, YouTube, and other Google services in furtherance of their scheme.

---

<sup>8</sup> For Google, these 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).



The subjects used email to communicate and solicit funds for the scheme; Google Drive and Google Photos to document and record receipts; Google Search to research U.S. laws pertaining to the transfer of funds overseas and travel within the United States and between the United States and other countries; Google Docs, in conjunction with Google Drive, to create and store documents; and YouTube to post a video soliciting funds for the scheme.

82. In general, user-generated content (such as email) that is written using, stored on, sent from, or sent to a Google account can be permanently stored in connection with that account, unless the subscriber deletes the material. For example, if the subscriber does not delete an email, the email can remain on Google's servers indefinitely. Even if the subscriber deletes the email, it may continue to exist on Google's servers for a certain period of time.

83. Thus, a subscriber's Google account can be used not only for email 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 Google's servers until deleted by the subscriber. Similar to emails, such user-generated content can remain on Google's servers indefinitely if not deleted by the subscriber, and even after being deleted, it may continue to be available on Google's servers for a certain period of time. Furthermore, a Google subscriber can store contacts, calendar data, images, videos, notes, documents, bookmarks, web searches, browsing history, and various other types of information on Google's servers. Based on my training and experience, I know that evidence of who controlled, used, and/or created a Google account may be found within such computer files and other information created or stored by the Google 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.

84. Based on my training and experience, I know that providers such as Google also collect and maintain information about their subscribers, including information about their use of Google's services. This information can include the date on which 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 Google 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 Google typically collect and maintain location data related to subscriber's use of Google services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.

85. Based on my training and experience, I know that providers such as Google 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 Google in order to track what devices are using Google'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 Google 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 Google account.

86. Google also allows its subscribers to access its various services through an application that can be installed on and accessed via cellular telephones and other mobile devices. This application is associated with the subscriber's Google account. In my training and experience, I have learned that when the user of a mobile application installs and launches the application on a device (such as a cellular telephone), the application directs the device in question to obtain a Push Token, a unique identifier that allows the provider associated with the application (such as Google) to locate the device on which the application is installed. After the applicable push notification service (*e.g.*, Apple Push Notifications (APN) or Google Cloud Messaging) sends a Push Token to the device, the Token is then sent to the application, which in turn sends the Push Token to the application's server/provider. Thereafter, whenever the provider needs to send notifications to the user's device, it sends both the Push Token and the payload associated with the notification (*i.e.*, the substance of what needs to be sent by the application to the device). To ensure this process works, Push Tokens associated with a subscriber's account are stored on the provider's server(s). Accordingly, the computers of Google are likely to contain useful information that may help to identify the specific device(s) used by a particular subscriber to access the subscriber's Google account via the mobile application.

87. Based on my training and experience, I know that providers such as Google use cookies and similar technologies to track users visiting Google'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 Google. 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 Google 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 Google account and determine the scope of criminal activity.

88. Based on my training and experience, I know that Google maintains records that can link different Google accounts to one another, by virtue of common identifiers, such as common email 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 Google 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 Google account.

89. Based on my training and experience, I know that subscribers can communicate directly with Google about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as Google 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.

90. In summary, based on my training and experience in this context, I believe that the computers of Google are likely to contain user-generated content such as stored electronic communications (including retrieved and unretrieved email for Google subscribers), as well as Google-generated information about its subscribers and their use of Google 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 Google with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

91. As explained above, information stored in connection with a Google 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 Google 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, email 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 Google can show how and when the account was accessed or used. For

example, providers such as Google 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 Google account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculcate 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 email). 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 Google 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).<sup>9</sup>

92. Based on my training and experience, I know that evidence of who controlled, used, and/or created a Google account may be found within the user-generated content created or stored by the Google subscriber. This type of evidence includes, for example, personal correspondence, personal photographs, purchase receipts, contact information, travel itineraries, and other content that can be uniquely connected to a specific, identifiable person or group. In addition, based on my training and experience, I know that this type of user-generated content can provide crucial

---

<sup>9</sup> At times, internet services providers such as Google can and do change the details and 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 Google'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.

identification evidence, whether or not it was generated close in time to the offenses under investigation. This is true for at least two reasons. First, people that commit crimes involving electronic accounts (*e.g.*, email accounts) typically try to hide their identities, and many people are more disciplined in that regard right before (and right after) committing a particular crime. Second, earlier-generated content may be quite valuable, because criminals typically improve their tradecraft over time. That is to say, criminals typically learn how to better separate their personal activity from their criminal activity, and they typically become more disciplined about maintaining that separation, as they become more experienced. Finally, because email accounts and similar Google accounts do not typically change hands on a frequent basis, identification evidence from one period can still be relevant to establishing the identity of the account user during a different, and even far removed, period of time.

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

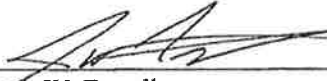
93. I respectfully request, pursuant to Rules 4.1 and 41(d)(3) of the Federal Rules of Criminal Procedure, permission to communicate information to the Court by telephone in connection with this Application for a Search Warrant. I submit that Assistant U.S. Attorney Erik M. Kenerson, an attorney for the United States, is capable of identifying my voice and telephone number for the Court.

---

**CONCLUSION**


97. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, which 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,

  
\_\_\_\_\_  
Joseph W. Ferrell  
Special Agent,  
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on July 27, 2020.



  
Deborah A. Robinson  
2020.07.27 10:49:26  
-04'00'

\_\_\_\_\_  
DEBORAH A. ROBINSON  
UNITED STATES MAGISTRATE JUDGE