

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

UNDER SEAL

In the Matter of the Search of:

The Microsoft account fshraiteh@hotmail.com, further described in Attachment A

Case Number:

18M143 7

SEARCH AND SEIZURE WARRANT

To: John P. Farley and any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California:

See Attachment A

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:

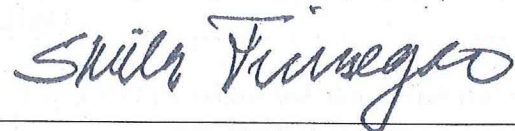
See Attachment A, Part III

YOU ARE HEREBY COMMANDED to execute this warrant on or before March 9, 2018 in the daytime (6:00 a.m. to 10:00 p.m.).

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 the issuing United States Magistrate Judge.

Date and time issued: February 23, 2018



Judge's signature

City and State: Chicago, Illinois

Sheila Finnegan, U.S. Magistrate Judge

Printed name and title

with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing and payment records.

g. All records indicating the services available to subscribers of the electronic mail addresses and/or individual account described above.

h. All account contents previously preserved by Microsoft, in electronic or printed form, including all e-mail, including attachments thereto, and for the account described above).

III. Information to be Seized by Law Enforcement Personnel

a. All information described above in Section II that constitutes evidence concerning violations of Title 18, United States Code, Section 2339B, as follows:

1. Items relating to travel, including travel documents, passport information, visas, and methods of travel into or through Syria, Turkey, and Iraq;

2. Items relating to Syria, Iraq, Islamic State of Iraq and al-Sham ("ISIS"), Islamic State of Iraq and the Levant ("ISIL"), and the Islamic State, Abu Bakr al-Baghdadi, and other known names for ISIS and members of ISIS;

3. Items relating to Nader, Omar, and Faress and their travel and/or support for foreign terrorist organizations;

4. Items relating to weapons, attack planning, or acts of violence;

5. Items relating to the identities, and current and past physical location, of the users of the accounts, or the individuals the users are communicating with;

c. opening or reading portions of electronic mail, and attachments thereto, in order to determine whether their contents fall within the items to be seized as set forth herein, and/or

d. performing key word searches through all electronic mail and attachments thereto, to determine whether occurrences of language contained in such electronic mail, and attachments thereto, exist that are likely to appear in the information to be seized described in Section III of Attachment A.

Law enforcement personnel are not authorized to conduct additional searches on any information beyond the scope of the items to be seized by this warrant.

RECEIVED
AUSA Baily Jones (312) 886-8027

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

FEB 23 2018
MAGISTRATE JUDGE
SHEILA M. FINNEGAN

UNDER SEAL

In the Matter of the Search of:

Case Number: **18M143**

The Microsoft account fshraitech@hotmail.com further described in Attachment A

APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT

I, John P. Farley, a Special Agent of the Federal Bureau of Investigation, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property or premises:

See Attachment A and Attachment A

located in the Northern District of California, there is now concealed:

See Attachment A, Part III

The basis for the search under Fed. R. Crim. P. 41(c) is evidence.

The search is related to a violation of:

Code Section

Offense Description

Title 18, United States Code, Section 2339B

material support to a foreign terrorist organization

The application is based on these facts:

See Attached Affidavit,

Continued on the attached sheet.

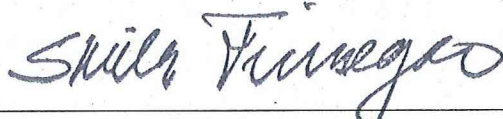
Applicant's Signature

JOHN P. FARLEY, Special Agent, Federal Bureau of Investigation

Printed name and title

Sworn to before me and signed in my presence.

Date: February 23, 2018



Judge's signature

City and State: Chicago, Illinois

Sheila Finnegan, U.S. Magistrate Judge

Printed name and title

persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence of violations of Title 18, United States Code, Section 2339B, are located in the **Subject Account**.

Microsoft

4. Based on my training and experience and information available from Microsoft's email websites (hotmail.com, outlook.com, live.com), I have learned the following about Microsoft's email services:

a. Microsoft provides email services, including hotmail.com, outlook.com, and live.com, which are available to Internet users. Subscribers obtain an account by registering with the relevant Microsoft email services on its website (e.g., hotmail.com, outlook.com, live.com). Microsoft requests subscribers to provide basic information, such as name, gender, zip code and other personal/biographical information.

b. Microsoft maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records often include account access information, email transaction information, and account application information.

c. Any email that is sent to a subscriber is stored in the subscriber's "mail box" on Microsoft servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by Microsoft. If the message is not deleted by the subscriber, the account is below the maximum storage limit, and the subscriber accesses the account periodically, that message can remain on Microsoft's servers indefinitely;

d. When the subscriber sends an email, it is initiated by the user, transferred via the Internet to Microsoft's servers, and then transmitted to its end destination. Microsoft's users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from the Microsoft server, the email can remain on the system indefinitely;

e. A Microsoft email subscriber can store files, including emails and image files, on servers maintained and/or owned by Microsoft.

5. Therefore, the computers of Microsoft are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Hotmail, such as account access information, transaction information, and account application. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities of Microsoft, to protect the rights of the subjects of the investigation and to effectively pursue this investigation, authority is sought to allow Microsoft to make a digital copy of the entire contents of the information subject to seizure specified in Section II

of Attachment A. That copy will be provided to me or to any authorized federal agent. The contents will then be analyzed to identify records and information subject to seizure pursuant to Section III of Attachment A.

**FACTS SUPPORTING PROBABLE CAUSE
TO SEARCH THE SUBJECT ACCOUNT**

SUMMARY

6. As described below, an FBI investigation of Muhammad Nader Shraiteh (Nader), Omar Muhammad Shraiteh (Omar), and Faress Muhammad Shraiteh (Faress), residents of the Northern District of Illinois, indicates that they have conspired with each other to provide material support and resources, namely, personnel in the form of themselves, to the Islamic State of Iraq and al-Sham (ISIS), a foreign terrorist organization.

7. As part of the FBI investigation, agents have determined that, in May 2015, Nader, Omar and Faress, traveled from Chicago to Turkey, through Egypt, with the intention of entering Syria to join ISIL. Faress was denied entry into Turkey because his passport was set to expire within six months. Instead of returning to the United States, Faress went to a family home in Jerusalem where he was subsequently arrested and prosecuted by the Government of Israel for his attempt to join ISIS. As detailed below, information obtained during the FBI investigation revealed that Omar and Nader entered into Syria or Iraq and have since been killed fighting for ISIS.

8. According to Faress's approved U.S. passport application to the Department of State, Faress is 21 years old and was born in the United States.

9. According to Nader's father, and Omar and Faress's father, Omar, 26, and Faress, were brothers, and are Nader's cousins. Omar, who was born in Jerusalem, moved to Chicago in 1992. He received an associate's degree in nursing but was employed as a truck driver in the United States. Faress was born in the United States and attended Wright Junior College.

The Islamic State of Iraq and al-Sham

10. On or about October 15, 2004, the U.S. Secretary of State designated al-Qaeda in Iraq (AQI), then known as Jam'at al Tawhid wa'al-Jihad, as a Foreign Terrorist Organization (FTO) under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist under section 1(b) of Executive Order 13224.

11. On or about May 15, 2014, the Secretary of State amended the designation of AQI as a FTO under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist 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 ISIL listing: the Islamic State of Iraq and al-Sham ("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. Although the group has never called itself al-Qaeda in Iraq, this name has frequently been used to describe it through its history. In an audio recording publicly released on June 29, 2014, ISIS announced a formal change of its name to 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.

12. Based on my training and experience, information provided by an Interpol informational publication, and information provided by an FBI Arabic linguist: (a) Sunni extremists and others, who are not citizens or residents of Syria and Iraq, have been traveling to Syria and Iraq to join ISIL and commonly enter Syria by crossing the border from Turkey; (b) to avoid increased law enforcement scrutiny of the common route to Syria through Turkey, foreign fighters from Western countries have traveled to locations in Egypt and on to Syria to join ISIS.

Information Provided by Members of a Mosque in Chicago

13. On or about May 14, 2015, Cook County's Department of Homeland Security and Emergency Management reported to the FBI that members of a mosque located in Chicago contacted them to report three male members were staying at a Motel 6 and may be planning on traveling overseas.

14. On or about May 14, 2015, the FBI met with Nader's father, and Omar and Faress's father, at the mosque. The fathers stated that the three travelers reported above were Nader, Omar, and Faress. The fathers informed the FBI that

Nader, Omar, and Faress left home on approximately May 4, 2015. Omar and Faress's father stated that Omar and Faress left with their passports.

Information Concerning Overseas Travel by Nader, Omar, and Faress

15. According to travel record information, on or about May 13, 2015, Nader, Omar, and Faress departed Chicago O'Hare airport via Alitalia to Italy, with a continuing flight to Egypt. The return ticket was booked for June 17, 2015, on the same airline. The email address associated with the purchase of these tickets is fshraiteh@hotmail.com (**Subject Account 2**).

16. According to records of Faress's credit card provided by TCF bank, the three tickets were purchased online on Alitalia's website with Faress's Visa credit card.

17. Based on my training and experience, I have learned that individuals aspiring to travel for purposes of supporting ISIS frequently purchase round-trip tickets to avoid detection by law enforcement officers.

18. According to records provided by Kayak, an online travel website, on May 12, 2015, a hotel room at the Pyramids Park Resort in Cairo, Egypt, was purchased for May 14 through May 25, 2015. The room was reserved under Omar's name and the email account associated with the purchase was **Subject Account 2**.

19. According to records of Faress's bank account provided by TCF Bank, an unknown individual made multiple withdrawals from Faress's bank account in the resort town of Sharm El-Sheikh in Egypt for the days surrounding May 26, 2015.

Information Provided by Individual A

20. On or about May 7, 2015, Individual A¹, a relative of Nader, Omar, and Faress, told the FBI that he had learned from other family members that Nader, Omar, and Faress had become radicalized and supported ISIS. Individual A stated that he learned from another family member that Nader moved out of the family home in Chicago, quit his job as a hairdresser, and began calling his parents from an unknown private number. According to family members, as related to the FBI by Individual A, Nader apologized to his parents for "anything he may have done wrong." According to Individual A, other family members expressed concern that this statement might have constituted an advance apology for undetermined future conduct.

21. On or about June 4, 2015, during an interview with FBI agents, Individual A stated that he had learned from family members in Jerusalem that Nader and Omar were in Turkey, and that Faress was staying with family members in Jerusalem.

22. On June 12, 2015, Individual A informed the FBI that, on that same day, Individual B (Individual A's son) had met Faress at a mosque in Jerusalem. According to Individual A, Faress stated to Individual B that he had attempted to

¹ In August 2016, Individual A, who was not a Confidential Human Source but a cooperating individual, was paid \$2,500 by the FBI for the information he had provided. Individual A also inquired about assistance to obtain a visa to travel to the United States. The FBI did not provide any of the requested assistance.

enter Turkey with Nader and Omar, but because Faress's United States passport was about to expire, the Turkish government refused to allow Faress entry into Turkey.

23. According to Individual A, Faress told Individual B that Nader and Omar were still in Turkey and that they had to leave Turkey within 90 days. Faress stated they will not return to the United States because the FBI is waiting for them since Nader's father told the FBI about Nader and Omar. Faress told Individual B that he was not planning on traveling outside of Israel and was going to attempt to get an Israeli driver's license. Faress believed the CIA was waiting for him to go back to the United States.

24. On or about April 18, 2016, during an interview with an FBI Agent and FBI linguist, Individual A stated he learned from a family member in Chicago that Omar was killed while fighting with ISIS in Syria. Further, there was a funeral for Omar in the city of Kafr Aqab. According to Individual A, the people of Kafr Aqab were divided whether to offer condolences to Omar's family because he died fighting with ISIS.

25. On or about July 5, 2016, during an interview with an FBI agent and FBI linguist, Individual A stated he learned from a family member in Chicago that Nader was killed while fighting with ISIS in Iraq. Further, on July 10, 2016, FBI interviewed Nader's mother at O'Hare airport. Nader's mother confirmed that Nader had died.

Fares' Facebook Account

26. On May 18, 2015, I reviewed the Fares's public Facebook profile for Fares. A screen shot of the profile for the Facebook page, which bears the name "Fares Shraiteh," is below:

Get more out of creditcards.ca's Citi ThankYou® 3X points on travel foreign purchase fees.

New Meter From bid.g.doubleclick.net A New Meter with Counter Test Strip Copy Today!

Get more out of creditcards.ca's Citi ThankYou® 3X points on travel foreign purchase fees.

New Meter From bid.g.doubleclick.net A New Meter with Counter Test Strip Copy Today!

Recent

- 2014
- 2013
- 2012
- 2011
- 2010
- 2009
- Born

Chat (Off)

Share

27. As shown above, photographs of lions feature prominently in the profile for Fares's Facebook account. According to the Combating Terrorism Center at West

Point, the lion has become a key motif in jihadist propaganda as a symbol of honor for both major jihadi leaders and for low-ranking militants. It may also be used to suggest martyrdom or designate a martyr-to-be.

28. On June 5, 2015, pursuant to a grand jury subpoena, Facebook provided subscriber information showed that the account was opened by "Faress Shraiteh" on or about October 9, 2009. These records also showed that the Facebook account was last accessed on May 24, 2015 from **Subject Account 2**.

Interview of Faress

29. On August 15 and 17, 2016, I interviewed Faress in an Israeli police station in Jerusalem. The interview was videotaped. At the commencement of each interview, I informed Faress of modified Miranda warnings. During the August 15 interview, Faress was initially reluctant to speak with me but, after a short time, agreed to speak with me until, after several hours, he asked for an attorney. I then stopped the interview. On August 17, prior to speaking with me, Faress conferred with an attorney and agreed to continue speaking with me outside the presence of the attorney.²

² Pursuant to Government of Israel regulations, the attorney would not be allowed in the room during the questioning but can wait outside the room if he chooses. Instead of waiting outside the room, Faress's attorney went back to his office. Faress was told that if at any time he wishes to speak with his attorney, to state so and I would stop the questioning and make arrangements for the attorney and Faress to confer. At no time during the August 17 interview did Faress ask to speak with his attorney.

30. During the interview, Faress stated, in response to questions regarding the purpose of his travel to Syria, that he wanted to travel to Syria to help the Syrian people in any way he could. He did not admit to wanting to join ISIS and blamed his deceased brother Omar for the circumstances since leaving the United States.

31. During the interview, Faress acknowledged that the tickets to travel to Egypt were purchased and sent through **Subject Account 2**.

32. On or about September 15, 2017, pursuant to a grand jury subpoena, Microsoft provided subscriber information which showed that **Subject Account 2** was opened by Faress Shraiteh on or about April 6, 2013. These records also show that **Subject Account 2** was last accessed on September 28, 2016.

33. On or about November 19, 2015, July 17, 2017, and February 23, 2018, preservation letters were served on Microsoft for **Subject Account 2** to preserve the accounts for a period of 90 days.

34. On or about November 2, 2017, I served Microsoft with an order pursuant to Title 18, United States Code, Section 2703(d), signed by Chief Judge Ruben Castillo, that directed Microsoft to provide the government with historical records and other non-content information for the **Subject Account 2** for the period of time from the creation of the account to the present.

35. On or about February 8, 2018, Microsoft complied with the order and provided the government with non-content header information for **Subject Account 2**.

36. I have reviewed the non-content header information and located what appears to be an email from "confirmation@alitalia.com" to **Subject Account 2** dated May 4, 2015. The timing of the email is consistent with Faress, Omar and Nader's May 13, 2015, travel on Alitalia to Italy. I also located an email from "KAYAK <bookings-noreply5@kayak.com" dated May 12, 2015, and an email from "KAYAK, no-reply@kayak.com" dated May 26, 2015. The timing of these emails are consistent with the travelers' booking of a hotel room in Cairo, Egypt.

37. Based on my training and experience in other investigations, I believe that a search of email provider account contents often of individuals engaged in criminal conduct yields investigative leads relating to:

a. the identities of any co-conspirators and other individuals engaged in a conspiracy to provide material support or resources to a foreign terrorist organization, in violation of Title 18, United States Code, Section 2339B(a)(1);

b. the contact information of any co-conspirators and other individuals engaged in a conspiracy to provide material support or resources to a foreign terrorist organization, in violation of Title 18, United States Code, Section 2339B(a)(1);

c. the timing of communications among any co-conspirators and other individuals involved in a conspiracy to provide material support or resources to a foreign terrorist organization, in violation of Title 18, United States Code, Section 2339B(a)(1);

d. the location of any co-conspirators and other individuals involved in a conspiracy to provide material support or resources to a foreign terrorist organization, in violation of Title 18, United States Code, Section 2339B(a)(1);

e. the methods and techniques used in a conspiracy to provide material support or resources to a foreign terrorist organization, in violation of Title 18, United States Code, Section 2339B(a)(1); and

f. communications with other individuals associated with ISIS.

SEARCH PROCEDURE

38. In order to facilitate seizure by law enforcement of the records and information described in Attachment A, this affidavit and application for search warrant seek authorization, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to permit employees of Microsoft to assist agents in the execution of this warrant. In executing this warrant, the following procedures will be implemented:

a. The search warrant will be presented to Microsoft personnel who will be directed to the information described in Section II of Attachment A;

b. In order to minimize any disruption of computer service to innocent third parties, Microsoft employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II of Attachment A, including an exact duplicate of all information stored in the computer accounts and files described therein;

39. Microsoft employees will provide the exact duplicate in electronic form of the information described in Section II of the Attachment A and all information stored in those accounts and files to the agent who serves this search warrant; and

40. Following the protocol set out in the Addendum to Attachment A, law enforcement personnel will thereafter review all information and records received from Microsoft employees to locate the information to be seized by law enforcement personnel pursuant to Section III of Attachment A.


CONCLUSION

41. Based on the above information, I respectfully submit that there is probable cause to believe that evidence of violations of Title 18, United States Code, Section 2339B are located within one or more computers and/or servers found at Microsoft, headquartered at 1065 La Avenida, Building 4, Mountain View, CA 94043. By this affidavit and application, I request that the Court issue a search warrant directed to Microsoft allowing agents to seize the electronic evidence and other information stored on the Microsoft servers following the search procedure described in Attachment A, and the Addendum to Attachment A.

FURTHER AFFIANT SAYETH NOT.

John P. Farley
Special Agent
Federal Bureau of Investigation

Subscribed and sworn
before me this 23rd day of February, 2018


Honorable Sheila Finnegan
United States Magistrate Judge

ATTACHMENT A

I. SEARCH PROCEDURE

1. The search warrant will be presented to Microsoft personnel, who will be directed to isolate those accounts and files described in Section II below.

2. In order to minimize any disruption of computer service to innocent third parties, company employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

3. Microsoft employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant.

4. Following the protocol set out in the Addendum to this Attachment, law enforcement personnel will thereafter review information and records received from company employees to locate the information to be seized by law enforcement personnel specified in Section III below.

II. FILES AND ACCOUNTS TO BE COPIED BY EMPLOYEES OF MICROSOFT

To the extent that the information described below in Section III is within the possession, custody, or control of Microsoft, which are stored at premises owned, maintained, controlled, or operated by Microsoft, headquartered at 1065 La Avenida,

Building 4, Mountain View, CA 94043, Microsoft is required to disclose the following information to the government for the following accounts:

fshraiteh@hotmail.com

a. All available account contents from inception of account to present, including e-mails, attachments thereto, drafts, contact lists, address books, and search history, stored and presently contained in, or maintained pursuant to law enforcement request to preserve.

b. All electronic files stored and presently contained in, or on behalf of the account described above.

c. All search history records stored and presently contained in, or on behalf of the account described above including, if applicable, web and application activity history (including search terms), device information history, and location history.

d. All existing printouts from original storage of all the electronic mail described above.

e. All transactional information of all activity of the electronic mail addresses and/or individual account described above, including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations.

f. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described above, including applications, subscribers' full names, all screen names associated

with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing and payment records.

g. All records indicating the services available to subscribers of the electronic mail addresses and/or individual account described above.

h. All account contents previously preserved by Microsoft, in electronic or printed form, including all e-mail, including attachments thereto, and for the account described above).

III. Information to be Seized by Law Enforcement Personnel

a. All information described above in Section II that constitutes evidence concerning violations of Title 18, United States Code, Section 2339B, as follows:

1. Items relating to travel, including travel documents, passport information, visas, and methods of travel into or through Syria, Turkey, and Iraq;

2. Items relating to Syria, Iraq, Islamic State of Iraq and al-Sham ("ISIS"), Islamic State of Iraq and the Levant ("ISIL"), and the Islamic State, Abu Bakr al-Baghdadi, and other known names for ISIS and members of ISIS;

3. Items relating to Nader, Omar, and Faress and their travel and/or support for foreign terrorist organizations;

4. Items relating to weapons, attack planning, or acts of violence;

5. Items relating to the identities, and current and past physical location, of the users of the accounts, or the individuals the users are communicating with;

6. Items relating to the names, addresses, telephone numbers, email addresses, and other contact or identification information of participants involved in violations of 18 U.S.C. § 2339B; and

7. Items relating to recruitment of individuals to join ISIS, or otherwise provide, or attempt to provide, material support to ISIS, or to facilitate joining ISIS.

b. All of the records and information described in Section II (e), (f), and (g).

ADDENDUM TO ATTACHMENT A

With respect to the search of any information and records received from the free web-based electronic mail service provider, law enforcement personnel will locate the information to be seized pursuant to Section III of Attachment A according to the following protocol.

The search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. searching for and attempting to recover any hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein.

b. surveying various file directories and the electronic mail, including attachments thereto to determine whether they include data falling within the list of items to be seized as set forth herein.

c. opening or reading portions of electronic mail, and attachments thereto, in order to determine whether their contents fall within the items to be seized as set forth herein, and/or

d. performing key word searches through all electronic mail and attachments thereto, to determine whether occurrences of language contained in such electronic mail, and attachments thereto, exist that are likely to appear in the information to be seized described in Section III of Attachment A.

Law enforcement personnel are not authorized to conduct additional searches on any information beyond the scope of the items to be seized by this warrant.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In the Matter of the Search of:

The Microsoft account
fshraiteh@hotmail.com, further
described in Attachment A

Case Number:

18M143

Magistrate Judge Sheila Finnegan

UNDER SEAL

ORDER

The UNITED STATES OF AMERICA by its attorney, JOHN R. LAUSCH, JR., United States Attorney for the Northern District of Illinois, having moved this Court to Seal the Search Warrant, Application, and Affidavit, and having demonstrated good cause in support of its motion, specifically, that disclosure of the Search Warrant, Application, and Affidavit would jeopardize the investigation by disclosing the details of facts known to investigators, the identities of witnesses, and the investigative strategy.

IT IS HEREBY ORDERED THAT the Search Warrant, Application, and Affidavit be kept under seal for 60 days from the date of this Order, until April 24, 2018.

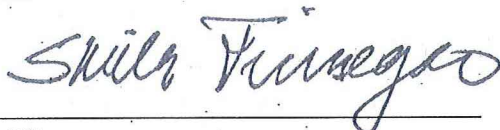
THE COURT FURTHER FINDS that there is reason to believe that notification of the existence of the warrant will seriously jeopardize the investigation, including by causing the intimidation of potential witnesses. *See* 18 U.S.C. § 2705(b).

IT IS THEREFORE ORDERED under Title 18, United States Code, Section 2705(b) that Microsoft Corp. shall not disclose the existence of the warrant, or this

Order of the Court, to the listed subscriber or to any other person, until further order of the Court, except that Microsoft Corp. may disclose the search warrant to an attorney for Microsoft Corp. for the purpose of receiving legal advice.

This Order does not prohibit law enforcement personnel from disclosing the search warrant as necessary to facilitate the enforcement of criminal law, including the execution of the warrant, or to any federal official to assist the official receiving the information in the performance of that official's duties.

ENTER:



Sheila Finnegan
United States Magistrate Judge

DATE: February 23, 2018

RECEIVED

FEB 23 2018

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

MAGISTRATE JUDGE
SHEILA M. FINNEGAN

In the Matter of the Search of:

The Microsoft account
fshraiteh@hotmail.com, further
described in Attachment A

Case Number:

18M143

Magistrate Judge Sheila Finnegan

UNDER SEAL

**GOVERNMENT'S MOTION TO SEAL
SEARCH WARRANT, APPLICATION, AND AFFIDAVIT AND TO
COMMAND MICROSOFT CORP. NOT TO NOTIFY ANY PERSON OF THE
EXISTENCE OF THE WARRANT**

Now comes the UNITED STATES OF AMERICA, by JOHN R. LAUSCH, JR.,
United States Attorney for the Northern District of Illinois, and states as follows in
support of its Motion to Seal Search Warrant, Application, and Affidavit:

On the 23rd day of February, 2018, the government applied for a Search
Warrant in this matter, and submitted an Application and Affidavit in support. The
Search Warrant Affidavit details the facts supporting probable cause to believe that
evidence concerning material support to a foreign terrorist organization offenses, in
violation of Title 18, United States Code, Section 2339B, will be found in **Subject
Account 2.**

The government will continue its investigation after execution of the Search
Warrant, and disclosure of the Application and Affidavit would jeopardize the
investigation by disclosing the details of facts known to investigators, the identities
of witnesses, and the investigative strategy. For the foregoing reasons, the

government respectfully requests that the Search Warrant, Application, and Affidavit be sealed for 60 days from the date of this Order, until April 24, 2018, except as necessary to facilitate the enforcement of criminal law, including the execution of the search warrant, or to any federal official to assist the official receiving the information in the performance of that official's duties.

In addition, Microsoft Corp. is a provider of an electronic communication service, as defined in Title 18, United States Code, Section 2510(15), and/or a remote computer service, as defined in Title 18, United States Code, Section 2711(2). Pursuant to 18 U.S.C. § 2703(b)(1)(A) and (c)(3), the government is not required to provide notice of the warrant to the subscriber or customer of the account.

Furthermore, under Title 18, United States Code, Section 2705(b), if the Court determines that that "there is reason to believe that notification of the existence of the warrant will result in—(1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation," this Court shall issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant. . . is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order."

In this case, such an order would be appropriate because the warrant relates to an ongoing criminal investigation that is neither public nor known to all of the

targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence or content of the warrant will causing the intimidation of potential witnesses. *See* 18 U.S.C. § 2705(b).

The United States respectfully requests that the Court issue an order commanding Microsoft Corp. not to disclose the existence or content of the warrant to any person, until further order of the Court, except that Microsoft Corp. may disclose the warrant to an attorney for Microsoft Corp. for the purpose of receiving legal advice.

Respectfully submitted,

JOHN R. LAUSCH, JR.
United States Attorney

By: /s/Barry Jonas
Barry Jonas
Assistant United States Attorney
219 S. Dearborn Street, Rm. 500
Chicago, Illinois 60604
(312) 886-8027

DATE: February 23, 2018