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 MULTIPLE ACCOUNTS THAT ARE STORED ON THE SERVER HOSTING TOR HIDDEN SERVICE ALPHABAY

Case No.

APPLICATION FOR A SEARCH WARRANT

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):*
computer servers and records of the Tor network website AlphaBay, as identified by the Tor URLs http://pwoah7foa6au2pul.onion and http://pwoah7foa6au2pul.onion/forum, the current location of which is concealed

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:
certain property, namely electronic information stored on the AlphaBay servers, as described in more detail in the attached affidavit and attachments thereto

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

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

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 844(e)	Bomb Threats
18 U.S.C. § 875(c)	Threats in Interstate Commerce
18 U.S.C. § 1038	False Information and Hoaxes

The application is based on these facts:

See attached affidavit incorporated by reference as if fully restated herein.

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 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

MICHELLE TAYLOR, SPECIAL AGENT
Printed name and title

Sworn to before me and signed in my presence.

Date: 04/06/2017

_____
Judge's signature

City and state: Washington, D.C.

U.S. MAGISTRATE DEBORAH A. ROBINSON
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF: INFORMATION ASSOCIATED WITH Darknet_Legend, itzme9089z, veetgergs, Player001, Anon10, TheMerchant, Vendor_X, Bestworks, alphabaytopbuyer1, topuser1000, The_Hero, StormTeamUP, theuser5185, newplayer1, bbestworks, member10, member 11, bestworks2, XUsername, AlphaBay-Mod-Raspi, AccountShop, belvin830c, Vendor_X_Recovery, Vendor_X_Recovery123c, Vendor_X_2, and randomuser1000 THAT ARE STORED ON THE SERVER HOSTING TOR HIDDEN SERVICE ALPHABAY	Case No. _____ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Michelle Carron Taylor, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41(b)(6)(A) of the Federal Rules of Criminal Procedure for a warrant to search the TARGET ACCOUNTS, further described below and in Attachment A, for the information described in Attachment B.

2. Your affiant is a Special Agent of the Federal Bureau of Investigation, and, as such, is an investigative or law enforcement officer of the United States within the meaning of Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure. Your affiant is engaged in the enforcement of criminal laws and is within a category of officers authorized by the Attorney General to request and execute search warrants pursuant to Title 18, U.S.C., Section 3052 and 3107; and DOJ regulations set forth at Title 28, C.F.R., Sections 0.85 and 60.2(a).

3. I have been a Special Agent (SA) with the Federal Bureau of Investigation ("FBI") since November 2005. I successfully completed New Agent Training at Quantico, Virginia, where I received extensive instruction on criminal investigations. I have also attended training specific to the conduct of public corruption and fraud investigations. During my employment with the FBI, I have conducted and/or assisted criminal investigations involving a variety of crimes against the United States, to include fraud and related activity associated with computers. I have training and experience in the enforcement of the laws of the United States, including the preparation and presentation of affidavits in support of warrants.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 844(e), bomb threats, 18 U.S.C. § 875(c), threats in interstate commerce, and 18 U.S.C. § 1038, false information and hoaxes. There is also probable cause to search the information described below and in Attachment A for evidence, instrumentalities, contraband and fruits of these crimes as described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant under Rule 41(b)(6)(A) because the above facts establish there is probable cause to believe that the district where the information is located has been concealed through technological means and that there is probable cause to believe that activities related to the crime being investigated occurred within this judicial district. As discussed more fully below, acts or omissions in furtherance of the offenses under investigation occurred within Washington, D.C. *See* 18 U.S.C. § 3237. Finally, the

offenses under investigation are the subject of a grand jury investigation in the District of Columbia.

IDENTIFICATION OF THE TARGET ACCOUNTS

7. This warrant authorizes the use of a remote search technique to be deployed on the computer servers hosting the AlphaBay market and forum, obtaining information described in Attachment B from the accounts described below.

8. The computer server is the server operating the Tor network website AlphaBay, as identified by the Tor URL http://pwoah7foa6au2pul.onion and http://pwoah7foa6au2pul.onion/forum, the current location of which is concealed through technological means.

9. The AlphaBay and AlphaBay forum accounts to be searched are described by the usernames Darknet_Legend, itzme9089z, veetgergs, Player001, Anon10, TheMerchant, Vendor_X, Bestworks, alphabaytopbuyer1, topuser1000, The_Hero, StormTeamUP, theuser5185, newplayer1, bbestworks, member10, member 11, bestworks2, XUsername, AlphaBay-Mod-Raspi, AccountShop, belvin830c, Vendor_X_Recovery, Vendor_X_Recovery123c, Vendor_X_2, and randomuser1000.

PROBABLE CAUSE

BACKGROUND CONCERNING THE INVESTIGATION

10. The FBI is investigating telephonic and email threats made toward a number of Jewish establishments, predominantly Jewish Community Centers ("JCC") in the United States, received from January 2017 through March 2017. During this time period over seventy telephonic threats and over fifty threatening emails were transmitted to JCCs, schools, and major

airports across the United States. In each case, the entity was threatened with either a bomb threat or a threat of an active shooter event.

11. On March 8, 2017, between approximately 2:31 p.m. EST[1] and 2:34 p.m. EST, six administrators at Rancho Cotate High School in Rohnert Park, California, received threatening emails from email address brinnubethsj@gmail.com.

12. The first email was sent with the following text:

> I'm concerning Rancho Cotate High School. My comrades successfully planted a few bombs at School. We have bombs hidden around the center. They are pipe bombs, hidden around the JCC. They will be detonated via lighter by my team. To top all that off, We have assault rifles and Machine pistols. The Children and Staff will be massacred mercilessly shortly.

13. The subsequent emails to Rancho Cotate High School were sent with the following text:

> I'm concerning Rancho Cotate High School. My comrades successfully planted a few bombs at School. We have bombs hidden around the center. They are pipe bombs, hidden around the School. They will be detonated via lighter by my team. To top all that off, We have assault rifles and Machine pistols. The Children and Staff will be massacred mercilessly shortly.

14. Analysis of the email text determined the text was identical except for the word "JCC" in the first email and "School" in the subsequent emails. Your affiant is aware similarly worded emails were sent to JCCs across the United States. In particular, on March 8, 2017, on or about 12:35:22 a.m. EST, the JCC of Louisville received an email from email address 744846648363a@gmail.com with the following text:

> I'm talking Jewish Community Center of Louisville. My fellow comrades successfully planted a few bombs at JCC. We have bombs hidden around the center. They are pipe bombs, hidden around the JCC. They will be detonated via a lighter by my team. To top

[1] To the extent possible, your affiant has standardized times throughout this affidavit to Eastern Standard Time (EST).

> all that off, We have assault rifles and Machine pistols. The Jewry and there Servants will be massacred mercilessly tomorrow.

15. The following day, March 9, 2017, at approximately 8:31 a.m. EST, the Consular-Department in the Embassy of Israel in Washington, D.C. received an email from the email account saranczak@yahoo.com, which stated:

> This Concerns the Israeli Embassy In Washington. A group of Individuals who I use to work for with have successfully planted pipe bombs at the embassy and the devices are set to go off soon at a busy hour of the day. To my knowledge I am aware there are 2 pipe bombs scattered throughout the embassy. They will be detonated via a cell phone that my group leader has in his possession. I am also aware that an insider at the embassy has assisted the group in placing the bombs in the embassy. Without insider none of this would be possible to achieve. My group has been planning this bombing for a few months already, this is going to be a well planned attack. I will not comment on the motivation of the group neither will I tell you there identity. You may ask why I'm Informing you about the impending attack as it does not make sense to tell you about it because it will prevent the attack from happening, Well I made wrong decisions in my life which I deeply regret. I befriended those people and went on with them to carry out this attack.
>
> I recently cleared my mind and I want to prevent this bombing attack for taking place by notifying you.
>
> I do hope you succeed in preventing the bombing from talking place. I do not want to see people die from this attack. I know you may not take this notification seriously because all the recent bomb threats to JCC's in the past few weeks. This totally unrelated to those hoax's, My group is of serious men and is for absolute certainly they are going to detonate the device later. This is no Hoax.
>
> I do not know what your going to do but I wish you the best of luck.

16. On March 23, 2017, the Israeli National Police (INP) arrested an individual by the name Michael Kadar, located in Ashkelon, Israel on suspicion of his involvement in the submission of the threatening communications. Subsequent to his arrest, the INP searched and seized a number of electronic media from his residence. On March 26, 2017, the INP shared images of the media relevant to the FBI’s investigation pursuant to a Mutual Legal Assistance

Treaty between the United States and Israel. Among the items was an imaged copy of an electronic storage device, described by INP as, "128GB Sandisk thumb drive from Michael's room (was attached to his computer)," hereinafter "the thumb drive."

17. Upon review of the material contained on the thumb drive were files indicating Kadar's knowledge of and involvement in the threatening email and telephone call scheme. Nearly all of the subfolders and files in the folder "My Stuff 8680" appear to relate to various online accounts used by Kadar, and others as yet unknown, to perpetuate the threats scheme or schemes. In particular, the drive contained the following folder and subfolder string: "My Stuff 8680/TARGETS/THE ARCHIVE OF TARGETS/2017." Within the "2017" folder were folders labeled "January 2017," "February 2017," and "March 2017." The folders, further compartmented by country and targeted entity, contained recordings of threatening telephone calls and screenshots of threatening emails from the perspective of the "sent" folder.

18. The aforementioned "March 2017" folder contained a subfolder of what your affiant assesses to be evidence of of the threatening communications, e.g., screen shots of emails and/or recordings of phone calls. Contained within the "March 2017" folder is a screenshot from the sent folder of the email account saranczak@yahoo.com displaying the March 9th threatening email to the Israeli Embassy; a screenshot from the sent folder of the email account 744846648363a@gmail.com to the JCC of Louisville; and a file titled "Rancho Cotate High School Rohnert Park, California 8 March 2017.PNG" containing an image of text, "email not saved."

19. Your affiant submits that there is probable cause to believe that the thumb drive contains evidence that Kadar sent threatening emails from a variety of email accounts and saved proof of the transmission of the threats for either his own personal database or to provide proof of service to a purchaser of his services, and/or evidence provided to Kadar regarding additional threats conducted by another individual or individuals.

USE OF ALPHABAY ACCOUNTS IN FURTHERANCE OF SCHEME

20. Darknet_Legend is the username of an AlphaBay vendor whose profile indicates he has been active since February 8, 2017. Darknet_Legend advertises a "School Email Bomb Threat Service" on his vendor account. In a posting on AlphaBay captured by law enforcement on March 19, 2017, the Darknet_Legend vendor listed a product description as follows:

> READ MY NOTES AND POSTAGE OPTIONS BEFORE PLACING AN ORDER
>
> What is this service ?
> This is unique emailing service for all of you, I email bomb threats to schools on your requests. If you feel you need someone to do this job for you then this service is for you.
>
> NOTES:
> - I have the right to refuse to work with you in any case.
> - This listing is only for bomb threat emails to schools, If you request a different type of service then message me.
> - I am available most of the time to make bomb threat emails.
> - I have saved email bomb threat texts when I email the bomb threat. If you request that I send the school a custom email text that you wrote then give me the bomb threat text that you wrote in the buyer notes and I will send the school the text you provided.
> - I will not tell the customer the email address I use to send the threat
> - Refund policy, I offer refunds for non-successful threats. If there is no evidence that the emailed bomb threat was a success then you will be refunded. Evidence of success can be a news post, facebook post or all other.
> - If you have any questions or requests then send me a message.
> - As for my Framing Someone for it, there is a no guarantee that the police will question or arrest the framed person. I just add the persons name to the email. In addition in my experience of doing bomb threats putting someones name in the emailed threat will

reduce the chance of the threat being successful. But it's up to you if you would like me to frame someone.

****
Bellow are you postage options and the info to provide me with.

1. Emailed Bomb Threat To A School $30.00
2. Emailed Bomb Threat To A School + Framing Someone for it For $45.00
3. Emailed Bomb Threat To A School District\Multiple Schools For $60.00
4. Emailed Bomb Threat To A School Districts\Multiple Schools + Framing Someone for it for $90.00

(Attention regarding Bomb Threat To A School District, This does not include large city school districts only small ones and not more than 12 schools. If it's a district with more than 12 schools then the price is more expensive and message me for custom listing.)

Provide me with the following info in the buyer notes:

Name of School Or School District (REQUIRED)
Email Address of School/Police or webpage of the school to contact if the school does not have an email (REQUIRED)

Custom Bomb Threat Text If you Have one, If not then I will use my own bomb threat text (OPTIONAL)
Other Information about the target (OPTIONAL)
Framed victims info: (OPTIONAL)

DO NOTE FORGET TO LEAVE ME WITH THE (Required Must Have Info) IN THE BUYER NOTES.

21. Review of the thumb drive revealed a .txt file titled "2.txt" in the My Stuff 8680/Database of Accounts and Others/VENDORS ACCOUNT DATA/NEW/Darknet_Legend folder. The properties of 2.txt indicate the document was created on March 6, 2017. The text is nearly identical to that of the aforementioned AlphaBay listing on the DarkNet_Legend vendor page.

READ MY NOTES AND POSTAGE OPTIONS BEFORE PLACING AN ORDER WITH ME.

What is this service ?
This is unique emailing service for all of you, I email bomb threats to schools on your requests. If you feel you need someone to do this job for you then this service is for you.

NOTES:
- I have the right to refuse to work with you in any case.
- This listing is only for bomb threat emails to schools, If you request a different type of service then message me.
- I am available almost 24/7 to make emails unlike my calling services.
- I have saved email bomb threat texts in English that I use. If you request that I send the school a custom email text that you wrote then give me the bomb threat text that you wrote and I will send the school the text you gave me.
- I will not tell U the customer the email service I use to send the threat neither will I provide the customer with my own bomb text that I wrote. I'll also not tell the customer my OPSEC methods.
- Refund policy, I offer refunds for non-successful threats. If there is no evidence that the emailed bomb threat was a success then you will be refunded. Evidence of success can be a news post, facebook post or all other.
- If you have any questions or requests then send me a message.

****
****
Bellow are you postage options and the info to provide me with.

1. Emailed Bomb Threat To A School $30.00
2. Emailed Bomb Threat To A School District\Multiple Schools For $60.00

Provide me with the following info in the buyer notes:
Name of School Or School District (Required Must Have Info)
Email Address of School/Police or webpage of the school to contact if the school does not have an email (Required Must Have Info)
Custom Bomb Threat Text If you Have one, If not then I will use my own bomb threat text (Optional, You don't have to leave me with this info)
Other Information about the target (Optional, You don't have to leave me with this info)

22. Your affiant compared the text of the DarkNet_Legend posting and the 2.txt file and determined the language and punctuation to be nearly identical.

23. A review of the Darknet_Legend user profile on AlphaBay revealed user feedback from a user stating, “Amazing on time and on target. We got evacuated and got the day cut short.” The date and time stamp of the posting was March 9, 2017 at 2:29 a.m. According to

media reports, on March 8, 2017, upon receipt of the threatening emails, Rancho Cotate High School was evacuated and students were released early.

24. Investigators determined the thumb drive contains a sub-folder called "Database of Accounts and Others." This sub-folder is contained within the aforementioned "My Stuff 8680" folder on the thumb drive, which consists largely of information related to the bomb threat scheme. "Database of Accounts and Others" contains various subfolders, some of which contain text and files with AlphaBay usernames (with corresponding passwords) believed to be under Kadar's control. The sub-folder "CURRENT BITCOIN AND VENDOR ACCOUNTS" includes the text file with the DarkNet_Legend account and password information. That same sub-folder and other sub-folders within it includes text files with the following AlphaBay accounts (with their corresponding passwords): itzme9089z, veetgergs, Player001, Anon10, TheMerchant, Vendor_X, Bestworks, alphabaytopbuyer1, topuser1000, The_Hero, StormTeamUP, theuser5185, newplayer1, bbestworks, member10, member 11, bestworks2, XUsername, , AccountShop, belvin830c, Vendor_X_Recovery, Vendor_X_Recovery123c, Vendor_X_2, and randomuser1000. An AlphaBay account and password for AlphaBay_Mod_Raspi was located in a sub-folder of "Database of Accounts and Others" called "AB FORUM VENDOR FORUM ACCOUNTS SCAM TO DELETE." According to information available on AlphaBay, those accounts were all created in 2016 or 2017. "Player001"; TheMerchant;"; "bestworks"; and "AccountShop" purport to deal in hacked accounts. "Vendor_X" purports to deal in passports and fraud guides, among other things.

25. Your affiant is aware, based on my training and experience, as well as conversations with other law enforcement agents, that individuals often use multiple accounts on Darknet sites

in order to further mask their identities from other users of the sites. For example, users have been known to create different AlphaBay accounts to buy and sell hacked accounts or credit card information for later use in bomb-threat schemes (so as to not link the sale of those accounts to the later threats); to leave positive feedback on one's own listings; or to leave negative feedbacks on other users' listings. Your affiant submits that there is probable cause to believe that the AlphaBay usernames listed in Attachment A were created by Kadar and/or others to use in different elements of his scheme and that Kadar had access to them in furtherance of his scheme. Additionally, your affiant is aware the threatening calls started prior to the published creation date of the DarkNet_Legend account.

26. Based on the foregoing, your affiant submits that there is probable cause to believe Michael Kadar and others as yet unknown, were responsible for transmitting a series of threatening communications in the District of Columbia and elsewhere, and that the identity of possible co-conspirators as well as fruits, evidence, and instrumentalities of the crime will be found within the AlphaBay accounts that appear to be under his control, specifically Darknet_Legend, itzme9089z, veetgergs, Player001, Anon10, TheMerchant, Vendor_X, Bestworks, alphabaytopbuyer1, topuser1000, The_Hero, StormTeamUP, theuser5185, newplayer1, bbestworks, member10, member 11, bestworks2, XUsername, AlphaBay-Mod-Raspi, AccountShop, belvin830c, Vendor_X_Recovery, Vendor_X_Recovery123c, Vendor_X_2, and randomuser1000.

BACKGROUND CONCERNING TOR

27. The Tor network is designed specifically to facilitate anonymous communication over the Internet. Information documenting what Tor is and how it works is provided on the publicly accessible Tor website at www.torproject.org. In order to access the Tor network, a user

must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org.[2] Use of the Tor software bounces a user's communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user. Because of the way Tor routes communications through other computers, traditional IP identification techniques are not viable. When a user on the Tor network accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. There is no practical way to trace the user's actual IP address back through that Tor exit node IP address. A criminal suspect's use of Tor accordingly makes it extremely difficult for law enforcement agents who are investigating a Tor Hidden Service to detect the host's, administrator's, or users' actual IP addresses or physical locations.

28. Within the Tor network itself, entire websites can be set up as "hidden services." "Hidden services" operate the same as regular public websites with one critical exception. The IP address for the web server is hidden and instead is replaced with a Tor-based web address, which is a series of algorithm-generated characters, such as "asdlk8fs9dflku7f" followed by the suffix ".onion." A user can only reach these "hidden services" if the user is using the Tor client and operating in the Tor network. And unlike an open Internet website, is not possible to determine through public lookups the IP address of a computer hosting a Tor "hidden service." Neither law

[2] Users may also access Tor through so-called "gateways" on the open Internet, however, use of those gateways does not provide users with the anonymizing benefits of the Tor network.

enforcement nor users can therefore determine the location of the computer that hosts the website through those public lookups.

BACKGROUND CONCERNING ALPHABAY

29. "AlphaBay" is an online, Darknet marketplace for registered users to buy and sell controlled substances, compromised payment card credentials and financial information, firearms, malicious computer software, and other contraband over the Internet. AlphaBay is one of the largest and most popular Darknet marketplaces, and currently has more than approximately 250,000 of listings offering items for sale. Listings on AlphaBay are organized by category (e.g., fraud, drugs and chemicals, weapons, etc.) and are searchable. In addition to the marketplace, AlphaBay also contains a forums section which maintains an electronic public posting area as well as a private messaging ("PM") area for users to communicate on a variety of topics.

30. AlphaBay is only accessible on the Darknet through the "The Onion Router" ("Tor"). It is a hidden service, as described above. In addition to the anonymizing services offered by Tor, users of AlphaBay may also employ virtual private networks ("VPN") to increase online privacy and security. VPN technology creates a secure encrypted connection to share information over a less secure network infrastructure, such as the Internet. An AlphaBay user, for example, can purchase a VPN from a VPN service provider in order to prevent the user's Internet Service Provider from seeing his/her online activity, and to conceal his/her true IP address from any website the user visits (such as AlphaBay) or computers with whom the user communicates (such as buyers or sellers on AlphaBay). In addition, VPNs can be used in conjunction with Tor to further anonymize online activity.

31. Once on AlphaBay, individuals who wish to buy or sell goods on the site must create an account. An account consists of, at a minimum, a username (i.e., an online moniker which is often an alias), password, and personal identification number ("PIN"). Users may also provide additional information, including but not limited to their public Pretty Good Privacy ("PGP") key used to encrypt communications. As further described below, AlphaBay encourages users to use encryption, such as PGP, to protect their identities.

32. Upon information and belief, the vast majority of transactions conducted on AlphaBay violate U.S. law, and the proceeds from such transactions derive from unlawful activity.

33. Transactions on AlphaBay are conducted using digital currency. One of the digital currencies often used on AlphaBay is Bitcoin. Bitcoin is a decentralized form of digital currency utilized to purchase goods and services over the Internet. Bitcoin is not managed by any one central authority or government, but rather collectively by Bitcoin users and the participating Internet community.

34. Each AlphaBay user is assigned an AlphaBay wallet to make purchases or receive payments. An AlphaBay user can transfer Bitcoins from an external wallet into their AlphaBay wallet by sending Bitcoins to the AlphaBay deposit address assigned to their AlphaBay account. A user's AlphaBay deposit address changes periodically to thwart tracing. The same process, in reverse, is used to transfer Bitcoins out of a user's AlphaBay wallet. To safeguard against fraud, AlphaBay offers an escrow service for buyers and sellers. Specifically, when a buyer purchases a good or service on AlphaBay, the buyer's Bitcoins are held in escrow by AlphaBay. The buyer must acknowledge receipt of a good or service to release the funds to the seller. If the buyer does not acknowledge receipt in fifteen days for a physical good or three days for an

electronically transmitted purchase, AlphaBay automatically finalizes the transaction and releases the bitcoins to the vendor. AlphaBay also provides for expedited processing for "trusted" sellers who have "Finalize Early" ("FE") status. FE status allows certain sellers to receive payment in full or in part, as soon as the seller acknowledges that an item is shipped or electronically transferred. AlphaBay staff members grant FE status to certain sellers on a case-by-case basis, most often when a seller has a substantial sales history and receives favorable buyer feedback.

35. In some cases, Alphabay users will communicate directly with a AlphaBay site administrators by use of AlphaBay's grievance forum about issues relating to their account, including technical problems, billing inquiries, or complaints from other users. Site administrators typically retain records about such communications, including records of contacts between the user and the support services, as well records of any actions taken by the administrator or user as a result of the communications. Furthermore, Alphabay accounts may also have additional transaction records of other cyber criminals that have purchased stolen information or access, as well as related communications, to included online identifiers.

THE REMOTE SEARCH TECHNIQUE

36. Based on my training, experience, and the investigation described above, I have concluded that using a remote search technique may help FBI agents to locate additional evidence of Kadar's criminal activity, identify possible buyers of his services, and identify additional victims. Accordingly, I request authority to use the remote search technique to investigate the above referenced Alphabay accounts.

37. The remote search of the accounts will entail an FBI agent or FBI task force officer logging into the accounts and checking the account profile, the account transaction logs, and other portions of the account that may contain records related to individuals requesting Kadar's services. An FBI agent or task force officer will use the Alphabay account information to log into the site, from a covert Internet connection. The FBI will save the webpages as individual files and/or take screenshots of the specific pages. The FBI will not make any changes to the account.

38. Each of these categories of information described in Attachment B may constitute evidence of the crimes under investigation, showing a direct link and profit from the sale of threatening communications services.

AUTHORIZATION REQUEST; DELAYED NOTICE

39. Pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), I request that this Court authorize the officers executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed.

40. This application seeks a warrant authorizing the use of a remote search technique to extract information from the above-described user accounts on the AlphaBay servers. It is expected that after use of the remote search technique, this information will be available to officers authorized to execute this warrant. Thus, the warrant applied for would authorize the copying of electronically stored information under Rule 41(e)(2)(B). However, as further specified in Attachment B, which is incorporated into the warrant, the applied-for warrant does not authorize the physical seizure of any tangible property.

41. It is expected that both the use of the remote search technique and the extraction will be performed without the knowledge of the AlphaBay administrators and the owners of the affected AlphaBay accounts.

42. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Because not all possible co-conspirators and buyers of Kadar's services are known or in custody, providing immediate notice to the owner or user of the TARGET ACCOUNTS would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. See 18 U.S.C. § 3103a(b)(1).

43. To the extent that Attachment B describes stored wire or electronic information, such a seizure is reasonably necessary, because without this seizure, there would be no other way, to my knowledge, to view the information and to use it to further the investigation. Furthermore, the remote search technique does not deny the users or administrators access to the account information, nor does the technique permanently alter any of the information stored in the accounts. *See* 18 U.S.C. § 3103a(b)(2).

44. I further request that the Court authorize execution of the warrant at any time of day or night, as the warrant does not authorize the physical seizure of tangible property.

REQUEST FOR SEALING

45. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the search warrant

is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Michelle Carron Taylor
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on April 6, 2017:

THE HONORABLE DEBORAH A. ROBINSON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

1. This warrant authorizes the use of a remote search technique to be deployed on the computer servers hosting AlphaBay, obtaining information described in Attachment B from the accounts described below.

2. The computer server is the server operating the Tor network website AlphaBay, as identified by the Tor URLs http://pwoah7foa6au2pul.onion and http://pwoah7foa6au2pul.onion/forum, the current location of which are concealed through technological means.

3. The AlphaBay accounts to be searched are described by the following usernames: Darknet_Legend, itzme9089z, veetgergs, Player001, Anon10, TheMerchant, Vendor_X, Bestworks, alphabaytopbuyer1, topuser1000, The_Hero, StormTeamUP, theuser5185, newplayer1, bbestworks, member10, member 11, bestworks2, XUsername, AlphaBay-Mod-Raspi, AccountShop, belvin830c, Vendor_X_Recovery, Vendor_X_Recovery123c, Vendor_X_2, and randomuser1000.

ATTACHMENT B

Items to Be Seized

All information described in Attachment A that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 844(e), bomb threats, 18 U.S.C. § 875(c), threats in interstate commerce, and 18 U.S.C. § 1038, false information and hoaxes, including, for each account or identifier listed in Attachment A, information pertaining to the following matters:

(a) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

(b) The identity of the person(s) who created, used, or controlled the Command & Control Servers on which the Alphabay account information was located, as well as their associates and co-conspirators;

(c) The identity of the person(s) who communicated with the user IDs about matters relating to transactions for threatening communications, proxies, or other stolen information such as identities or online account information, including records that help reveal their whereabouts.

(d) The identity, whereabouts, associates, and co-conspirators of Michael Kadar;

(e) The identity and whereabouts of any and all victims of the threatening communications scheme.

This warrant does not authorize the physical seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of stored wire and electronic information as described above. *See* 18 U.S.C. § 3103a(b)(2).