AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Maryland

United States of America
v.
Mohamed ELSHINAWY,
a/k/a "Mojoe," a/k/a "Mo Jo"

Case No. 15-2716 TJS

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of February 2015 to the present in the county of _____ in the _____ District of Maryland, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 2339B(a)(1)	Attempting to provide material support or resources to a designated foreign terrorist organization, namely ISIL
18 U.S.C. § 1505	Obstruction of agency proceedings
18 U.S.C. § 1001	Making material false statements and falsifying or concealing material facts

This criminal complaint is based on these facts:

See Attached Affidavit

☑ Continued on the attached sheet.

Complainant's signature

David A. Rodski, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: December 11, 2015

Judge's signature

City and state: Baltimore, MD

Timothy J. Sullivan, United States Magistrate Judge

Printed name and title

15-2716TJS – 15-2718TJS

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND ARREST AND SEARCH WARRANTS

I, David A. Rodski, being duly sworn, hereby state as follows:

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed for more than thirteen years. I am currently assigned to the Baltimore Division of the FBI where my responsibilities have included investigating a variety of criminal offenses, including drug trafficking, white collar crimes, bank robberies, and federal terrorism-related crimes and other national security violations. In the course of my employment with the FBI I have received extensive training on conducting criminal and counterterrorism investigations. I have authored affidavits in support of court orders, search warrants and criminal complaints for violations of federal criminal laws. I have also provided training to domestic and international agencies on counterterrorism matters.

2. This affidavit is being submitted in support of a criminal complaint and arrest warrant for Mohamed ELSHINAWY, a/k/a "Mojoe," a/k/a "Mo Jo," charging him with the following offenses: attempting to provide material support or resources to a designated foreign terrorist organization in violation of 18 U.S.C. § 2339B(a)(1); obstruction of agency proceedings in violation of 18 U.S.C. § 1505; and making material false statements and falsifying or concealing material facts in violation of 18 U.S.C. § 1001.

3. This affidavit is also being submitted in support of an application for authorization to search ELSHINAWY's residence at 335 McCann Street in Edgewood, Maryland, and his silver Honda Accord, Maryland license number 8BX9525, both of which are fully described in Attachment A. ELSHINAWY's residence and ownership of his vehicle were confirmed through surveillance and records checks with the Maryland Motor Vehicle Administration, credit agencies, and phone and cable providers. Both the residence and the

vehicle were the subject of federal search warrants issued on October 8, 2015, and executed by FBI agents on October 9, 2015. I respectfully submit there is probable cause to believe that the items sought by this request for search warrants constitute evidence, fruits and instrumentalities of the offenses identified in paragraph 2 above.

4. The information contained in this affidavit is based upon my personal knowledge of this investigation, my own observations and/or review of documents, review of investigation conducted by and documents authored by other law enforcement officers, or reliable information provided to me by other law enforcement personnel involved in this matter. Because this affidavit is being submitted for the limited purpose of enabling the Court to make a judicial determination of probable cause to issue arrest and search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish the legal basis for the issuance of the requested warrants. I have not, however, omitted any information that would tend to defeat a finding of probable cause.

Probable Cause

5. On October 15, 2004, the United States Secretary of State designated al-Qa'ida 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. On May 15, 2014, the Secretary of State amended the designation of al-Qa'ida in Iraq ("AQI") as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224 to add

the alias Islamic State of Iraq and the Levant ("ISIL") as its primary name. The Secretary also added the following aliases to the ISIL listing: the Islamic State of Iraq and al-Sham ("ISIS"), the Islamic State of Iraq and Syria ("ISIS"), 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 (AQI)," this name has frequently been used to describe it through its history. To date, ISIL remains a designated FTO. In an audio recording publicly released on or around June 29, 2014, ISIL announced a formal change of its name to the Islamic State ("IS").

6. I know from my training and experience that ISIL uses social media outlets to exhort its supporters to conduct attacks in their home countries, to include the United States. In June 2015, the FBI became aware of an individual located in Egypt who was attempting to send money to the United States, possibly for nefarious purposes. Through review of Western Union transactional records, the FBI was able to confirm that on June 28, 2015, this individual wire-transferred a sum of $1,000 (exclusive of transaction fees) to ELSHINAWY from a location in Egypt. The Western Union records identified ELSHINAWY as the payee at his residential address in Maryland. The pay agent was identified as a convenience store located near ELSHINAWY's residence.

7. The Western Union records confirm that ELSHINAWY received the $1,000 remittance from the individual in Egypt on the date of transfer, June 28, 2015. After receiving the money, FBI surveillance agents observed ELSHINAWY drive to his local bank branch where he conducted a transaction at the drive-up ATM. A review of the bank's records confirm that ELSHINAWY made an $800 cash deposit into his account at that time and subsequently

transferred $200 from that deposit to a joint account held with his wife.

8. On July 17, 2015, ELSHINAWY consented to a non-custodial interview by Baltimore FBI agents. Upon being questioned about the nature of the $1,000 Western Union transfer, ELSHINAWY claimed that the money had come from his mother who resides in Egypt. After being shown the Western Union receipt with the sender's name, ELSHINAWY claimed that the money was to purchase an iPhone for a friend. Upon being advised that making a false statement to law enforcement was a criminal offense for which he could face imprisonment, ELSHINAWY finally revealed that he had a childhood friend who had been arrested on terrorism-related offenses in Egypt and had fled to Syria upon his release from custody. ELSHINAWY indicated that he and his friend began communicating thereafter through social media. A review of business records confirmed the real name of ELSHINAWY's childhood friend (hereafter "childhood friend").

9. During his July 17 interview, ELSHINAWY further indicated that his childhood friend had contacted him a few months earlier to connect him, through social media, with a member of ISIL. Believing that he would be able to get some money from ISIL, ELSHINAWY agreed to the contact. ELSHINAWY began communicating with the ISIL operative, whose name he did not know (hereafter "unidentified ISIL operative"), utilizing a method of communication that I know, through my training and experience, is being used by ISIL members.

10. ELSHINAWY advised the interviewing agents that he ultimately received a total of $4,000 in two payments from the unidentified ISIL operative. The first payment of $3,000 was sent to him from a company located overseas (hereafter "Overseas Company") on May 14,

2015, via eBay/Paypal. After fees, the net payment to ELSHINAWY was approximately $2,882.70. ELSHINAWY showed the interviewing agents the eBay/PayPal receipt of transaction on his laptop computer. ELSHINAWY stated that he received the transactional details of the $1,000 Western Union transfer from the individual in Egypt whom he understood to be an ISIL operative (hereafter "Egyptian ISIL operative"). ELSHINAWY indicated that he did not know the identity of this individual.

11. ELSHINAWY provided the interviewing agents a phone number for the unidentified ISIL operative that he had obtained during the course of their communications. ELSHINAWY stated that he was instructed to use the monies he received from the unidentified ISIL operative for "operational purposes," which ELSHINAWY understood to mean causing destruction or conducting a terrorist attack in the United States. ELSHINAWY stated that the unidentified ISIL operative did not provide specific guidance as to what weapons to buy or how to conduct an attack, but the Draw Mohammed Contest in Texas was given as an example.[1] ELSHINAWY stated he knew the money he was sent was to fund a terrorist attack, but he claimed that he never intended to conduct such an attack. Rather, he claimed he saw an opportunity to make money and take it from "thieves," and felt that the FBI should reward him for what he had done. ELSHINAWY stated that he was instructed that if he ever determined he was under surveillance by law enforcement, he was to stop whatever activities he was doing in connection with executing an attack.

[1] During the July 17 interview, it was unclear as to when this particular communication occurred between ELSHINAWY and the unidentified ISIL operative. On May 3, 2015, two individuals attempted to attack and kill attendees at an art contest in Garland, Texas, depicting drawings of the Prophet Mohammed. The individuals were immediately killed by law enforcement officers as they attempted to launch their attack.

12. On July 20, 2015, ELSHINAWY consented to a second non-custodial interview with Baltimore FBI agents, during which he stated his awareness that lying to law enforcement agents was an offense for which he could face imprisonment. During the interview, which was recorded, ELSHINAWY sought to portray himself as someone who was simply trying to scam some money from ISIL members. He stated emphatically that he received no other funds from ISIL other than the $4,000 he had previously disclosed, which he used to buy some furniture and pay bills. He touted his success at having taken ISIL's money and felt that his efforts should be applauded. He thought he should be offered a job to work with the FBI to identify ISIL's money network. Towards the end of the interview, ELSHINAWY indicated that he suddenly remembered that he had received another $1,200 from ISIL through Paypal. He said that the money came from the same unidentified ISIL operative by order of a guy in Syria. Again, the guidance he received was to use the money to do something destructive that ISIL could claim.

13. During this second interview, ELSHINAWY explained that in order to receive the $1,200 from the unidentified ISIL operative, he created a scheme by which he pretended to sell printers on eBay that would serve as a cover for the payments he received from ISIL. He provided an email address ("Email Account 1") to the unidentified ISIL operative to complete the money transfer via Paypal. Records received from Paypal confirm that ELSHINAWY is the registered user of a Paypal account associated with Email Account 1. Investigation revealed that ELSHINAWY utilized this method during the time frame of June 2-7, 2015, which would have coincided with the $1,200 payment he received from the unidentified ISIL operative.

14. It is my belief, given what was subsequently discovered by the FBI after ELSHINAWY had been interviewed, that he was providing the FBI with a detailed cover story

in order to conceal the extent and true nature of the transactions he had with individuals he understood to be ISIL members and his true relationship with those individuals. A review of Paypal records indicates that ELSHINAWY concealed from the FBI at least $3,500 of the $7,700 in funds he received from the Overseas Company in his identified Paypal account between March and June 2015. The total identified Paypal payments (exclusive of processing fees) were received by ELSHINAWY as follows: $1,500 on March 23; $1,000 on April 16; $1,000 on May 1; $3,000 on May 14; and $1,200 on June 7. This last payment occurred in concert with ELSHINAWY's creation of one of his accounts on the online store. With the addition of the $1,000 sent by the Egyptian ISIL operative via Western Union, ELSHINAWY received a total of at least $8,700 from individuals ELSHINAWY understood to be associated with ISIL.

15. The FBI has confirmed that eight days after the payment on March 23, ELSHINAWY used the monies to purchase a laptop computer and a cell phone. Based on the information set forth below, it is my belief that these items were used by ELSHINAWY to further activities with, and by, ISIL members. To date, a review of bank records for dates surrounding ELSHINAWY's receipt of monies from the Overseas Company has revealed that out of those funds: 1) at least $1350 was spent for communication devices such as phones, calling cards, the laptop computer (referenced above), a hotspot for Internet access, a private VPN network, all of which appears, as referenced in more detail below, to have been utilized in connection with ISIL-related activities of ELSHINAWY and his associates; 2) at least $3000 was converted into cash by ELSHINAWY through ATM withdrawals that is neither traceable nor accounted for; 3) a portion of the remaining funds appear to have been used for personal expenses, but not all of it can be accounted for with certainty.

16. It is significant to note that records for ELSHINAWY's Paypal account indicate no activity for ten months starting in May of 2014. The Paypal account suddenly became active again two days prior to ELSHINAWY receiving his first payment from ISIL. Most logins to ELSHINAWY's Paypal account during the three month period encompassing March 21 through June 21, 2015, were from U.S.-based IP addresses primarily resolving to the area where ELSHINAWY resides in Maryland. However, during this same period, there were three successful logins to ELSHINAWY's Paypal account resolving to IP addresses at overseas locations during dates coinciding with the $3,000 payment and the $1,200 payment that ELSHINAWY admitted he received from the unidentified ISIL operative.

17. On June 30, 2015, ELSHINAWY was stopped in his vehicle and briefly questioned by Baltimore County police officers after having being observed loitering in a known drug area. Shortly thereafter, ELSHINAWY was observed by law enforcement agents visiting a Walmart store in the nearby vicinity. Subsequently, law enforcement confirmed that ELSHINAWY purchased two "pay as you go" cell phones and two phone cards from the Walmart he was observed visiting. Sprint records indicate that on July 1, 2015, ELSHINAWY began utilizing a new cell phone number ("Cell Phone 1"), which he registered in the name "MO JO," listing his residential address. During his July 17 interview, ELSHINAWY claimed that he had destroyed one of his cell phones because he had informed the unidentified ISIL operative that he was out of the game due his belief he was under observation. ELSHINAWY told the interviewing agents he thought this would be a good excuse that would not be questioned and would disassociate his old phone number ("Cell Phone 2") with the communication platforms he was using when communicating with ISIL members. ELSHINAWY stated that he transferred

the phone number for the unidentified ISIL operative into his new phone along with all of his other contacts.

18. During its investigation, the FBI became aware that there were additional communications between the Egyptian ISIL operative and ELSHINAWY regarding the $1,000 Western Union transfer, which ELSHINAWY did not fully reveal during his consensual interviews. Law enforcement confirmed through a review of records that Cell Phone 2 was registered to ELSHINAWY, and a search of open sources connected that number to his social media account, which, according to business records, was created on July 11, 2010. Those records confirmed that Cell Phone 1 was also associated with his social media account. During his July 20 interview, ELSHINAWY advised that he continued to communicate with individuals he understood to be ISIL members, including his childhood friend. He stated that his childhood friend had sought to contact him through social media during the weekend of July 18-19, 2015.

19. At the time of his initial non-custodial interview on July 17, ELSHINAWY consented to a search of his Dell and HP laptop computers (which were subsequently returned to him on July 20, 2015). A forensic analysis revealed that the hard drive of the HP laptop had been damaged. More significantly, the HP laptop was utilizing a particular type of operating system that allows for no information to be stored on the computer. Accordingly, no retrievable information or evidence was found on the HP laptop computer.

20. A forensic analysis of the Dell laptop revealed several pictures documenting significant damage to the Italian Consulate in Cairo, Egypt, which was bombed on July 11, 2015. The analysis also revealed that the laptop had been used to access another email account ("Email Account 2"), and that the account had been accessed on July 11, 2015 – the same day as the

consulate bombing. In addition to revealing that the account was registered under the pseudonym "Egyptian Lion Heart," the subscriber records for the account also revealed a secondary email referenced in more detail below ("Email Account 3), and yet another telephone number ("Cell Phone 3"). Law enforcement has confirmed that through review of records that ELSHINAWY is the subscriber of Cell Phone 3. Additionally, during his interview on July 17, ELSHINAWY was shown photographs of the July 11th attack by the interviewing agents. He denied having ever seen any photos of the attack.

21. On July 24, 2015, additional forensic analysis of ELSHINAWY's Dell laptop revealed that it had been used to access multiple email accounts. Law enforcement has confirmed that the accounts were subscribed to by ELSHINAWY, in some instances utilizing pseudonyms or other identifiers in an apparent attempt to conceal his true identity. For example, on March 8, 2010, while ELSHINAWY was in Egypt, a third email account ("Email Account 3") was created utilizing a pseudonym. The records link ELSHINAWY to the account through the listing, among other things, of one of his cell phones – Cell Phone 2. According to Customs and Border Protection (CBP) records, ELSHINAWY traveled from the United States to Cairo, Egypt, on November 27, 2008, and did not return until June 11, 2010. During this time, ELSHINAWY applied for a replacement United States passport. He reported that the prior passport had been lost or stolen, which I know from experience and training is a technique often used to conceal foreign travel (i.e., documentation of travel in the original passport). The replacement passport was issued on April 21, 2010.

22. Subscriber records indicate that ELSHINAWY last accessed another email account ("Email Account 4") on July 2, 2015, approximately three months after its creation on

April 6, 2015. The records associate the account to ELSHINAWY through listing of Email Account 3 and another cell phone number previously unknown to the FBI ("Cell Phone 4). Law enforcement has confirmed that Cell Phone 4 was activated on April 2, 2015, under the name "Black Eyes" and address "earth planet, Aberdeen, Maryland." The number was disconnected on May 3, 2015. According to the subscriber records for Email Account 4, the account was logged into approximately 85 times, which was almost every single day during the period from April 6 through July 2, 2015, which was the same time period during which ELSHINAWY was receiving funds from individual he understood to be ISIL members.

23. A review of records from one of ELSHINAWY's social media accounts revealed that ELSHINAWY took steps to conceal his communications between himself and his childhood friend. A review of records from a social media account of the childhood friend revealed that he and ELSHINAWY did, in fact, engage in numerous communications dating back to February 2015. The substance of these communications reflected ELSHINAWY's and the childhood friend's allegiance to the ISIL cause. The public profile from October 2015 for the social media account of the childhood friend contained several images that I recognize from my background, training and experience as ISIL-related propaganda.

24. The .social media communications between ELSHINAWY and his childhood friend were all in Arabic and have since been translated by an FBI linguist, who is a native Egyptian Arabic speaker. Many of these communications contain statements that I recognize from my experience and training to be jihadist rhetoric found in ISIL- and other terrorist-related propaganda. For example:

a. On February 17, 2015, ELSHINAWY pledged his allegiance to ISIL and

asked his childhood friend to deliver his message of loyalty. He stated that he was a soldier of the State but was temporarily away. ELSHINAWY also stated that his soul was over there with the jihadists and that every time he saw the news, he smiled. I know through training and experience that members of ISIL take a pledge, or "bayat," swearing unconditional loyalty to the group, or its leader ("Emir"), and its cause. The use of the term "mujahideen," translated in this communication as "jihadists," is a common reference to individuals engaged in violent jihad, such as ISIL fighters. Around the time of this conversation, ISIL had conducted a series of attacks and gained territory in Iraq. On February 16, 2015, a video was publicly released showing the execution of 21 Egyptian nationals in Libya by ISIL extremists. I believe that ELSHINAWY's reference to seeing and hearing news that made him smile was a reference to the news in the media regarding ISIL's terrorist acts.

b. Also on February 17, 2015, the childhood friend told ELSHINAWY to seek God's help and to not discuss his plans for a terrorist attack with anyone. ELSHINAWY agreed, and acknowledged that it is a crime in the United States. ELSHINAWY further declared his allegiance to committing violent jihad.

c. On March 13, 2015, ELSHINAWY told his childhood friend that he believed that his phone was bugged, and told him to tell their friend (believed to be an ISIL member or possibly the unidentified ISIL operative) that he (ELSHINAWY) was preparing himself for jihad and taking extreme security measures. He also told his childhood friend that he would contact him soon. On March 29, 2015, ELSHINAWY told his childhood friend that he would soon have a phone on which they could talk any time. As previously noted, ELSHINAWY used some of the monies he received from ISIL on March 23, 2015, to purchase a

laptop and a cell phone. Law enforcement has confirmed that ELSHINAWY purchased an LG brand cell phone at a local Walmart on March 28, 2015, and had it activated on April 2, 2015.

d. On April 3, 2015, ELSHINAWY told his childhood friend that he would soon hear good news, to which the childhood friend told him to remain steadfast in his planning. ELSHINAWY indicated that he had many targets, to which the childhood friend responded, "Alluhu'Akhbar," which translates to "God is great." ELSHINAWY stated that he was taking his time and being careful in undertaking certain acts for ISIL with the ultimate goal of joining his childhood friend overseas. ELSHINAWY also told his childhood friend that he was indebted to him for showing him the way to martyrdom, and that his childhood friend should continue to fight. I believe, based on my training and experience with terrorism cases, that ELSHINAWY was discussing supporting ISIL and violent jihad.

e. On April 21, 2015, the childhood friend told ELSHINAWY that God was with them and would grant them victory. He also stated that being a martyr is their way to heaven and whoever commits jihad does it for God. ELSHINAWY agreed.

f. On April 22, 2015, ELSHINAWY and his childhood friend discussed making what I believe, based on my review of the communication, to be an explosive device. ELSHINAWY asked his childhood friend whether making the device with a silencer would be difficult or easy. He also stated that he would make a device himself. ELSHINAWY also told his childhood friend to listen to the lessons of Sheikh Al-Adnani. I know from training, experience and public sources that Sheikh Al-Adnani is in Syria and a senior leader within ISIL, as well as its official spokesperson.

g. On April 25, 2015, ELSHINAWY and his childhood friend discussed the

use of a type of communication platform. The childhood friend asked ELSHINAWY for an un-attributable phone number so ISIL operatives could send messages to him. ELSHINAWY provided the number for Cell Phone 4 that until review of the childhood friend's social media records was unknown to the FBI.

h. On May 2, 2015, ELSHINAWY declared to his childhood friend his love of jihad, his desire to eliminate "the bastards," and his commitment to breaking the Cross. I know from my training and experience that the reference to "breaking the Cross" is a specific term used by ISIL in its propaganda. The phrase first appeared in mid-2014 when ISIL publicly threatened attacks in the United States, and then again in October 2014 when ISIL made public threats to attack the Vatican and "break the cross."

25. Law enforcement has confirmed that the childhood friend made numerous attempts in mid-July and August to contact ELSHINAWY through social media; however, ELSHINAWY did not respond. At that point, ELSHINAWY had been interviewed by the FBI about his activities in July 2015. A review of one of ELSHINAWY's social media accounts indicates that at some point in time (currently unknown), ELSHINAWY blocked his childhood friend from his social media account in an apparent attempt to further conceal his own activities with ISIL members. The records also indicate that on July 18, 2015, the day after he was first interviewed by Baltimore FBI agents, ELSHINAWY removed a particular named individual as a friend from his account. A review of the public portion of the ELSHINAWY's social media account for that individual indicated that he had changed his name to an alias, and his account contained extensive ISIL-related propaganda and other information indicative of someone who is an ISIL sympathizer or member.

26. Law enforcement has confirmed that a social media account associated with the childhood friend includes his discussions about his own ISIL-related activities overseas, ISIL martyrs, and logistics needed to aid ISIL's ongoing overseas activities. For example:

a. On June 25, 2015, the childhood friend attempted to recruit an individual to join ISIL and discussed the blessing of becoming a martyr and entering paradise.

b. On July 24, 2015, the childhood friend and an ISIL associate, possibly a family member, discussed how authorities were watching them. They shared ISIL propaganda suggesting that the authorities should be killed.

c. On September 4, 2015, the childhood friend acknowledged to his associate that he was an ISIL member that ISIL kills the enemies of God.

d. On October 16, 2015, the childhood friend was asked by his associate about ISIL logistics and operations overseas. The childhood friend expressed his concern that the associate might get captured.

27. As previously mentioned, Cell Phone 4 was activated on April 2, 2015, and disconnected on May 3, 2015. Law enforcement has also confirmed that from May 18 through June 18, 2015, ELSHINAWY, using Email Account 1 activated another cellular phone ("Cell Phone 5") that he registered under the name "David John" at a location near his residential address.

28. Law enforcement has confirmed that Cell Phone 4 operated as a "pay as you go" . The registration information for the phone listed Email Account 5, the pseudonym "Black Eyes," and the address "earth planet" at a location in Maryland. I know through my training and experience that criminal actors commonly use "pay as you go" phones in order to conceal their

identities, since personal identifying information is not required to obtain service for the phones. Call detail records indicate the majority of phone calls for this number were to one of ELSHINAWY's other previously referenced telephone numbers – Cell Phone 2 – which could be indicative of ELSHINAWY checking voicemails or texts made to the prior number. ELSHINAWY could also have been utilizing either phone to communicate via the previously mentioned Internet-based communications platforms, which would not register on the call detail records. During his July 17 interview, ELSHINAWY specifically denied having, or utilizing, any phone numbers other than Cell Phone 2.

29. Review of records for ELSHINAWY's various electronic accounts confirms that they were used to facilitate communication with regards to the transfer of funds by ISIL operatives to ELSHINAWY. During the time frame of the payments, at least five of ELSHINAWY's email accounts were accessed from overseas locations. Comcast records indicate that ELSHINAWY had Comcast service from April 1 through June 15, 2015. It was determined during a search of his residence in October 2015 that he had a mobile hotspot with a different service provider that he obtained on February 21, 2015. This date corresponds to the date on which ELSHINAWY pledged his allegiance to ISIL. An internet "hot spot" is a virtual machine that offers its user accessibility to the Internet from any location, and also allows the user to access the Internet quasi-anonymously.

30. I also know from my experience and training that there are other methods by which individuals can conceal their true location while communicating over their electronic devices. These methods also provide users complete anonymity and make it almost impossible for law enforcement to identify the actual source of the activity. Law enforcement has confirmed

that ELSHINAWY utilized a number of these methods in addition to his mobile hotspot. Additionally, these records indicate that a number of ELSHINAWY's electronic and online accounts may have been accessed overseas.

31. The FBI has determined that since in or about 2010, ELSHINAWY has been utilizing a specific social media account under the pseudonym "Egyptt in USA." A review of ELSHINAWY's bank and Paypal records indicate that ELSHINAWY used a portion of the $1,200 he admitted receiving from the unidentified ISIL operative on June 7, 2015, to purchase credits on the chat application's website. This would have enabled ELSHINAWY and/or his overseas associate to engage in additional chat communications anonymously. This account was utilized in connection with the June 2015 payment from ISIL operatives to ELSHINAWY.

32. Records from one of ELSHINAWY's social media accounts reflect that on June 28, 2015, just hours after receiving the $1,000 wire transfer from the Egyptian ISIL operative, ELSHINAWY logged into the account and communicated with an individual identified by a particular pseudonym. The FBI has identified that this individual is, in fact, located overseas and is believed to be his brother. The records also show that ELSHINAWY and his brother communicated on June 4 and June 6, 2015. As was the case with communications with ELSHINAWY's childhood friend, ELSHINAWY took steps to conceal his communications with his brother. ELSHINAWY's communications with his brother in June were close in time to the transfer of monies to ELSHINAWY from ISIL operatives. When the FBI executed a search warrant at ELSHINAWY's home on October 9, 2015, ELSHINAWY's phone reflected an instant message on that same date from the individual believed to be his brother. This confirms ELSHINAWY's continued contact with an individual whose prior communications with

ELSHINAWY over his social media account are most likely related to ELSHINAWY's activities relating to ISIL.

33. Law enforcement has recently confirmed that the social media account believed to be associated with ELSHINAWY's brother included the following (per English summary translations of the Arabic provided by a FBI linguist):

a. On March 11, 2015, ELSHINAWY asked his brother if he had joined the Islamic State; his brother replied in the negative. ELSHINAWY then told his brother that he planned to pledge his allegiance soon through the phone to an Emir overseas, and instructed that his brother keep this information secret. ELSHINAWY indicated that his childhood friend had already pledged his allegiance personally with Abu Bakr Al-Baghdadi (who is the publicly recognized leader of ISIL). ELSHINAWY's brother cautioned ELSHINAWY not to pledge his allegiance in case he was being monitored. ELSHINAWY replied that he pays full attention to his surroundings and had intentionally reset his phone to make it appear broken. ELSHINAWY indicated that he had intended to go join his childhood friend overseas, but now he had his own higher plan and would stay here (in the United States) for now. He indicated that eventually he would go to Syria or Iraq and take his wife with him. ELSHINAWY further stated that he would become one of the mujahideen like his childhood friend, and if he died in the sake of Allah, that would not be a problem for him. When asked by his brother what ELSHINAWY had to do once he pledged allegiance to the Islamic State, ELSHINAWY replied that he had to show loyalty and obedience. He stated his wish was to live among the Islamic State, and that he believed that Islam would soon control the world.

b. On April 27, 2015, ELSHINAWY advised his brother that he had pledged

allegiance to Da'ish, which he stated was the acronym of the Islamic State in Iraq and Al-Sham (also known as ISIL). When asked by his brother how he felt after having pledged his allegiance to ISIL, ELSHINAWY responded that he felt that he was a Muslim with dignity and pride unlike the Jews and Christians. He indicated that real life means that the heart is to be with God, and waiting and death is to be in the name of God. I know from my experience and training that this statement is a common reference to jihad and martyrdom. ELSHINAWY advised that he had received a lot of money (presumably a reference to the money he had received from individuals he understood to be ISIL members) and would receive more. In what appeared to be an effort by ELSHINAWY to recruit his brother into the ISIL cause (who had indicated in their conversation that he was uncertain as to whether he felt the same way about the ISIL), ELSHINAWY told his brother to search for the State of Sinai, adding that people in the Sinai have pledged their allegiance to ISIL in light the publicly known ISIL- sponsored attacks in the Sinai. ELSHINAWY then instructed his brother to take steps to conceal their communications referencing the Islamic State (i.e., ISIL).

c. On April 28, 2015, subsequent to the unrest that took place in Baltimore following the death of Freddie Gray in police custody, ELSHINAWY confirmed for his brother the events that were taking place in Baltimore, and stated his belief that it was "great" and "let them burn the police, and all together they are infidels."

d. On May 25, 2015, ELSHINAWY stated that he wanted to die as a martyr.

e. On May 29, 2015, ELSHINAWY stated that he dreamt of the State (believed to be a reference to the Islamic State) almost every day. He described a dream he had in which he had a gun and went to a church where he killed people. At the end of the

conversation, ELSHINAWY asked his brother to remember the mujahideen in his prayers, to which his brother agreed.

f. On August 12, 2015, ELSHINAWY's brother advised that ELSHINAWY's childhood friend had contacted him and asked for ELSHINAWY's contact information. ELSHINAWY told his brother not to provide any information to the childhood friend. ELSHINAWY confirmed that he was now avoiding contact with his childhood friend and had taken steps to conceal their communications over his social media account.

g. On August 15, 2015, ELSHINAWY informed his brother that he had stopped communicating with the childhood friend because everything around him (ELSHINAWY) was being monitored and that is was a very big issue.

h. On August 31, 2015, ELSHINAWY instructed his brother to tell the childhood friend that he (ELSHINAWY) had been completely revealed and uncovered (an obvious reference to the FBI's contacts with ELSHINAWY in July 2015). ELSHINAWY stated that as soon as the brother told this to the childhood friend, the friend would understand what it meant. ELSHINAWY also instructed his brother to take steps to conceal their communications on this subject, and any communications with the childhood friend about this subject.

34. Finally, in reviewing records for one of ELSHINAWY's social media accounts, it was observed that ELSHINAWY had joined numerous social media networks that reflected support for ISIL and violent jihad, or involved information relating to ISIL activities and electronic hacking. One of the individuals that ELSHINAWY had identified as a "friend" on his account had photos and other ISIL-propaganda included on his public social media page. On July 18, 2015, the day after ELSHINAWY was first interviewed by Baltimore FBI agents,

ELSHINAWY took steps to conceal his association with this friend. During execution of the search warrant at ELSHINAWY's residence on October 9, 2015, the name of this individual was displayed on ELSHINAWY's phone as an account that ELSHINAWY was "following" as of that day, thereby demonstrating that the relationship between the two men continued. A review on November 12, 2015, of the public postings on this individual's social media account reveal that he has since changed his name to another alias. The attempts by ELSHINAWY and this individual to conceal their identities and/or communications clearly indicates a concern regarding law enforcement learning about the true nature of their relationship or communications. Records from this individual's social media account reveal multiple photos of ISIL soldiers, the black ISIL flag, tanks and guns, news coverage of "Jihadi John" (the individual seen in numerous ISIL beheading videos), and a map of ISIL-held or proposed ISIL territories.

Evidence Found in Documents and Computers

35. Based upon my knowledge, training, experience and participation in other investigations, and information provided by other law enforcement officers, I know that:

a. Persons engaged in or assisting in financial crimes maintain records of their financial activity, such as receipts for expenditures by cash and check, bank records, and other financial documents, in their personal residences, place of business, or other properties under their control, such as rented storage units, vehicles, safes, safe deposit boxes, or vehicles. These records may be in the form of written notes and correspondence, receipts, negotiated instruments, contracts, bank statements, and other items. Records of this kind are also often stored on computers, mobile phones, and other electronic devices capable of media storage.

b. Persons engaged in or assisting in financial crimes often maintain financial records for long periods of time, particularly when they are involved in ongoing criminal conduct. There are many reasons for this. The evidence may be necessary business records, which must be kept for information reporting purposes, such as for state and federal tax returns, loan applications, profit and loss statements and balance sheets. The evidence may also be innocuous at first glance (e.g., financial, credit card and banking documents, travel documents,

receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, check books, videotapes and photographs, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone and pager bills, keys to safe deposit boxes, packaging materials, computer hardware and software), but have significance and relevance when considered in light of other evidence. The criminal offender may no longer realize he still possesses the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. The criminal offender may also be under the mistaken belief that he has deleted, hidden or further destroyed any computer related evidence, but which may be retrievable by a trained forensic computer expert.

36. I also know from my training, knowledge and experience that searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

a. Computer files, or remnants of such files, can be recovered months or years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost, and, if deleted, can be recovered using readily-available forensic tools. Deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long period of times before they are overwritten by new data. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed, than on a particular user's operating system, storage capacity, and computer habits.

b. Computer storage devices (like hard disks, diskettes, tapes, laser disks) can store the equivalent of millions of pieces of information. A suspect may try to conceal criminal evidence by storing it in random order with deceptive files names. This may require searching authorities to examine all the stored data to determine which particular files constitute evidence or instrumentalities of crime. This sorting process can take weeks or months depending on the volume of data

stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. Data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code embedded in the system as a "booby trap"), a controlled environment may be necessary to complete and accurate analysis. Such searches often require the seizure of most or all of a computer systems input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a computer expert can accurately retrieve the systems data in a laboratory or other controlled environment.

Conclusion

37. What is now known of ELSHINAWY's conduct and communications dating back to February 2015 is indicative of his efforts to conceal the full extent of his criminal conduct from the FBI during his meetings with agents in July 2015 and beyond. During his meetings with the FBI, ELSHINAWY made repeated false statements regarding the money transfers from ISIL; repeatedly insisted that he was telling the truth when, in fact, he was not revealing the true nature and extent of his contacts with ISIL operatives; and finally, appeared overeager to ingratiate himself with the FBI and be "a part of the team." I believe that ELSHINAWY provided his cover story to the FBI in order to conceal his true motivation and activities relating to ISIL. I also believe that his communications with his childhood friend and his brother reveal his true state of mind and support of ISIL's cause.

38. I also know from my experience and training that individuals engaged in nefarious conduct often become suspicious of law enforcement scrutiny. If one or more of the

criminal actors believe that their criminal activities or communications have been compromised, those individuals attempt to disengage from their associates and cease all communication, or make it appear as though they have done so. Based on the information contained in this affidavit, I believe that in or around July 2015, after he had been questioned by the FBI, ELSHINAWY did just that, and either ceased to communicate with his ISIL associates, or, more likely, in light of the facts referenced in this affidavit, continued to communicate through more covert means, such as the previously referenced communication platforms, or through utilization of multiple and ever-changing phones, phone numbers, and email accounts utilizing multiple anonymous methods of communication. Throughout this affidavit the evidence illustrating ELSHINAWY's concealment efforts, and his technological ability at switching out phones and accounts and deleting his substantive communications, leads me to believe that ELSHINAWY has simply dropped those communication channels he believes the FBI knows about, and substituted other communication methods that he believes are more covert.

39. Moreover, ISIL has repeatedly exhorted supporters outside of Syria and Iraq to conduct attacks in their home countries. ELSHINAWY's commitment to ISIL's cause is clearly reflected in his communications with his brother located overseas both before and after his interactions with Baltimore FBI agents. More significantly, he has created and used multiple electronic accounts, many under pseudonyms, to communicate with ISIL operatives, and appears to have allowed those individuals access to his accounts thus enabling them to use the accounts at will.

40. Based on the information contained in this affidavit, I submit there is probable cause to believe that ELSHINAWY has committed the following offenses: attempting to provide

material support to a foreign terrorist organization in violation of 18 U.S.C. § 2339B; obstruction of agency proceedings in violation of 18 U.S.C. § 1505; and making material false statements and/or falsifying or concealing material facts by trick of scheme in violation of 18 U.S.C. § 1001.

41. In addition, I submit there is probable cause to believe that additional evidence, fruits and instrumentalities of these same offenses, as identified in Attachment B, will be found within ELSHINAWY's residence and vehicle, especially any and all cellular phones and other electronic devices in the possession of ELSHINAWY and his wife. As previously noted, federal search warrants were executed on ELSHINAWY's residence and his Honda Accord on October 9, 2015. Items of evidentiary value, including certain of ELSHINAWY's electronic devices, were seized. These items included the recent contacts with overseas operatives evidenced on ELSHINAWY's cell phone, the identification of a mobile hot-spot, and documentary evidence indicating possibly other wire transfers originating from overseas, whose purpose and use have yet to be identified. After being imaged, two of ELSHINAWY's phones that were currently being utilized by ELSHINAWY and his wife were returned to them by the FBI. The computer hardware that was seized has not been returned. The FBI has no knowledge as to whether ELSHINAWY has replaced those devices since the search. Given the nature of ELSHINAWY's continued contact, via electronic means, with overseas actors and his brother located overseas, as set forth above, it is clear that he continues to utilize cell phones and/or other electronic devices in connection with his ISIL-related activities.

42. Every attempt will be made to do on-site searching and copying of the computer hardware recovered pursuant to search of the location identified herein. However, in light of the issues enumerated above, your affiant requests the Court's permission to seize the computer

hardware (and associated peripherals) that are believed to contain some or all of the evidence described in Attachment B, and conduct an off-site search of the hardware for relevant evidence if, upon arriving at the scene, the agents executing the searches conclude that it would be impractical to search the computer hardware on-site. Any search of computer hardware will be conducted in accordance with the procedure set forth in Attachment C.

Your affiant has signed this document under oath as to all assertions and allegations contained herein and states that its content are true and correct to the best of his knowledge.

David A. Rodski, Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 11th day of December, 2015.

Timothy J. Sullivan
United States Magistrate Judge

15-2716TJS – 15-2718TJS

ATTACHMENT A

The residence and vehicle for which authorization to search is requested are described as follows:

[redacted] **Edgewood, Maryland**, is described as a single story, attached residential home in a group of townhomes second one from the right. The exterior of the residence is white in color with green shutters, and the numbers "335" are clearly marked in black numbers just to the left of the front entrance.

Honda Accord is described as silver in color, and bearing Maryland license number [redacted], and Vehicle Identification Number (VIN) [redacted].

ATTACHMENT B

The following items are to be seized pursuant to the attached warrant, to include hard copy documents and electronic mail and files, and constitute evidence, fruits and instrumentalities of: attempting to provide material support to a foreign terrorist organization in violation of 18 U.S.C. § 2339B; obstruction of agency proceedings in violation of 18 U.S.C. § 1505; and making material false statements and/or falsifying or concealing material facts by trick of scheme in violation of 18 U.S.C. § 1001.

1. Records of communication with other individuals concerning the preparation for, planning of, and/or funding of terrorist-related activities.

2. Information pertaining to the solicitation and/or identification of co-conspirators and/or facilitators involved or associated with ELSHINAWY and others involved in undertaking terrorist-related activity in the United States or elsewhere.

3. Records and other information pertaining to monetary transfers, financial accounts or other monetary instruments connected to terrorist-related planning or attacks, including, but not limited to, checks, wires, journals, ledgers, faxes, diaries, credit card records, bills, receipts, deposits and withdrawal slips, bank statements, safety deposit box keys and records, and related correspondence.

4. Records indicating that data has been deleted by the account owner, potentially to hide evidence of a crime.

5. Copies of travel records and related correspondence evidencing travel to and from the United States and payment for such travel.

6. Photographs and/or videos relating to any of the subject matter described herein.

7. The United States and foreign passports of Mohammed ELSHINAWY and his

wife Rachel Rowe.

8. Contraband such as weapons, weapons parts, bulk cash, homemade bomb-related materials.

9. Cellular telephones or other portable electronic devices belonging to, or used by, Mohammad ELSHINAWY and his spouse, Rachel Rowe, and related account and purchase records.

10. Electronic records and related items referring or relating to the information sought in paragraphs above 1-9 above, including but not limited to: computers; central processing units; external and internal drives; external and internal storage equipment or media, terminal or video display units; computer software; computerized storage devices (including data stored in zip drives and any such devices' power supply hardware); account names; passwords; encryption codes; computer printouts or computer programs; computer or data processing software or data (including CD-ROMS, hard disks, and floppy disks); and portable GPRS and SMS printers and/or any type of remote printing machine (RPM).

ATTACHMENT C

Description of Methods to be Used for Searching Electronically Stored Information

This warrant authorizes the search of electronically stored information. The search shall be conducted pursuant to the following protocol in order to minimize to the greatest extent possible the likelihood that files or other information for which there is not probable cause to search are viewed.

With respect to the search of any digitally/electronically stored information seized pursuant to the instant warrant as described in Attachment A hereto, the search procedure may include the following techniques (the following is a non-exhaustive 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. examination of all the data contained in computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized;

c. physical examination of the storage device, including surveying various file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized;

d. opening or reading portions of files in order to determine whether their contents fall within the items to be seized;

e. scanning storage areas to discover data falling within the list of items to be seized, to possibly recover any such deleted data, and to search for and recover files falling within the list of items to be seized; and/or

f. performing key word searches through all electronic storage areas to determine whether occurrence of language contained in such storage areas exist that are likely to appears in the evidence to be seized.