AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America
v.
Denis Yakovlev
a/k/a Dennis Derrett
and
Meghan Marie Toole

Case No. 6:16-mj-1406-01, 02

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 1/1/14 through 7/5/16 in the county of Brevard in the Middle District of Florida, the defendant(s) violated:

Code Section	*Offense Description*
8 U.S.C. § 1324(a)(1)(A)(iv)	Encouraging or inducing an alien to come to, enter, or reside in the United States.

This criminal complaint is based on these facts:

See affidavit

☑ Continued on the attached sheet.

Complainant's signature

Timothy Scott, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 7/6/2016

Judge's signature

City and state: Orlando, FL

David A. Baker, U.S. Magistrate Judge

Printed name and title

STATE OF FLORIDA

COUNTY OF ORANGE

Case No. 6:16-mj-1406-01, 02
Case No. 6:16-mj-1407

MASTER AFFIDAVIT

I, Timothy Scott, being duly sworn, hereby depose and say that:

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT AND COMPLAINT

1. I am a Special Agent with Homeland Security Investigations (HSI) under Immigration and Customs Enforcement (ICE), United States Department of Homeland Security, previously with the U.S. Customs Service, and have been so employed for the past fourteen years. I am presently assigned to the Office of the Resident Agent in Charge, Cocoa Beach, Florida. As a HSI Special Agent, my duties include the investigation of criminal violations of United States customs and immigration laws. I am a law enforcement officer of the United States within the meaning of Section 1401(i) of Title 19, United States Code, and am empowered to investigate and make arrests for violations of U.S. criminal laws within the meaning of Section 2510(7) of Title 18, United States Code.

2. As a Special Agent with HSI, I have received training related to the enforcement of federal criminal law both as a graduate of the Federal Law Enforcement Training Center Criminal Investigator Training Program as well as agency and multi-agency training specifically related to conducting investigations of violations of customs and immigration laws.

3. I am submitting this affidavit both in support of an arrest warrant and a search warrant. Specifically, I believe there is probable cause to believe that Denis YAKOVLEV, a.k.a. Dennis DERRETT, and Meghan Marie TOOLE did knowingly

encourage and induce an alien to come to, enter, or reside in the United States, knowing and in reckless disregard of the fact that such residence is and will be in violation of law, all in violation of Title 8, United States Code, Section 1324(a)(1)(A)(iv). Furthermore, I am seeking a search warrant of their residence at 5050 Ocean Beach Blvd, Apt. 106, Cocoa Beach, Florida (hereinafter "SUBJECT PREMISES") which is more particularly described in Attachment A, incorporated herein, and for the items specified in Attachment B, incorporated herein, which items constitute instrumentalities, fruits, and evidence of the foregoing violations, along with violations of Title 8, United States Code, Sections 1324(a)(1)(A)(v)(II), and Title 18 United States Code, Section 371. I am requesting authority to search the entire SUBJECT PREMISES to include the curtilage, including the residential dwelling and outbuildings or any other structures on the SUBJECT PREMISES, as well as any computer and computer media and electronic storage devices located therein, where the items specified in Attachment B may be found. I also request to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of criminal activity. Furthermore, as set forth in more detail below, I believe there is probable cause that YAKOVLEV and TOOLE committed a violation of bringing in and harboring certain aliens in violation of Title 8, United States Code, Section 1324(a)(1)(A)(iv).

4. I make this affidavit from personal knowledge based on my participation in this investigation, information from other criminal investigators, information from law enforcement officers, information from agency reports, and the review of documents provided to me by these witnesses and law enforcement officers. Because this affidavit is being submitted for the limited purpose of seeking a Criminal Complaint and

authorization to search the SUBJECT PREMISES, I have not set forth each and every fact learned during the course of this investigation.

STATUTORY AUTHORITY

5. Title 8, United States Code, Section 1324(a)(1)(A)(iv) prohibits a person from encouraging or inducing an alien to come to, enter, or reside in the United States, knowing or in reckless disregard of the fact that such coming to, entry or residence is or will be in violation of law. Title 8, United States Code, Section 1324(a)(1)(A)(v)(II) prohibits a person from aiding and abetting the commission of the acts described in Title 8, Section 1324(a)(1)(A)(iv). Title 18, United States Code, Section 371 prohibits two or more persons from conspiring to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose.

RELEVANT IMMIGRATION PROCEDURES OVERVIEW

6. U.S. Citizenship and Immigration Services (USCIS) is the government agency that oversees lawful immigration to the United States.

7. Pursuant to Title 8, Section 1255, an alien can apply to USCIS to adjust his/her status to that of a lawful permanent resident (LPR) based on a marriage to a United States citizen (USC). To begin this process, the USC spouse petitions for their alien relative by filling out a Petition for Alien Relative (Form I-130). The second step of this process is the filing of an Application to Register Permanent Residence or Adjust Status (Form I-485).

8. In order to establish that the petitioner is a USC, they must submit proof of such, along with proof of the claimed relationship to the beneficiary. One of many acceptable forms of proving status as a USC is in the form of a birth certificate, and a

marriage certificate can be used to show proof of the relationship with the beneficiary. 8 C.F.R. § 204.1(f), (g).

9. Furthermore, the USC petitioner must submit at least one or more of the following: documentation showing joint ownership of property, or a lease showing joint tenancy of a common residence, and/or documentation showing co-mingling of financial resources; or birth certificates of children born in wedlock, and/or affidavits sworn to or affirmed by third parties having personal knowledge of the bona fides of the marital relationship and/or any other documentation to establish that there is an ongoing marital union. 8 C.F.R. § 204.1(b); *see also* I-130 Instructions Form.

10. When filing for adjustment of status using the Form I-485, the petitioner must submit and execute a G325A, Biographic Information sheet for both the petitioner and beneficiary. 8 C.F.R. § 1245.2(a)(3)(i).

11. Unless there is an applicable exception or waiver, USCIS normally requires the married couple's presence at an in person interview at one of the local USCIS field offices to review the *bona fides* of the marriage. 8 C.F.R. § 1245.6; *see also* 8 C.F.R. § 103.2(a)(7).

12. All of the forms a USC petitioner is required to complete are available in fillable form on the internet through www.uscis.gov.

TECHNICAL TERMS

13. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the

same state.

14. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

15. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

16. *Probable cause.* I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually

disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

17. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of

the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further

suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that is connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer

may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process.

While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to encourage or induce an alien to come to, enter, or reside in the United States, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how

the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

18. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the

volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

SUMMARY OF PROBABLE CAUSE

20. This is a marriage fraud conspiracy in which YAKOVLEV and TOOLE provide a one stop shop where multiple services in furtherance of the fraud are offered to customers. Specifically, YAKOVLEV, TOOLE and others recruit USCs to enter into fraudulent marriages with non-citizen aliens for the sole purpose of the alien becoming a LPR and thereby converting to legal status in the United States. YAKOVLEV and/or TOOLE arrange for the alien and USC to travel to a Brevard County Clerk of the Courts office and apply for a marriage license and execute the marriage ceremony. Before going to the clerk's office, the USC and alien have never met, so YAKOVLEV prepares both participants in advance for what to say when talking to the clerk at the clerk's office.

21. After the license is obtained and the ceremony is completed, YAKOVLEV fills out the necessary forms (e.g. the Form I-130 and G325A) and he generally does this by typing the information into fillable forms downloaded from the USCIS website. YAKOVLEV then provides the package to the alien spouse for them to mail into USCIS but only after he directs the alien and USC "spouses" to build the *bona fides* of the marriage. YAKOVLEV generally encourages the USC to add their name to the lease of the residence of the alien. YAKOVLEV charges the alien a fee for his service. YAKOVELV pays the USC an amount of money for marrying the alien and keeps a varying amount for his services.

DETAILS OF THE INVESTIGATION

22. In October 2015, HSI Special Agent Curtis Johnson was at the Brevard County Clerk's office (Merritt Island branch) on matters unrelated to this case.

However, while there, he observed what he believed to be a fraudulent marriage taking place. Subsequently, HSI met with the Brevard County Clerk of the Court and obtained the list of marriage license applications for 2015 to 2016. Notably, there appeared to be an unusually high amount of aliens from Uzbekistan, Kazakhstan, Kyrgyzstan, and other former Soviet countries where Russian is still spoken, engaging in marriages to USCs in Brevard County. Also of note is that that many of the addresses provided by the aliens were from outside of Florida while many of the USCs provided Cocoa, Florida addresses.

23. HSI then reviewed State Department records which showed that Z.B.Y., a native and citizen of Uzbekistan, received a United States visa to enter the United States as a non-immigrant J1 student on June 18, 2012. According to records from the Brevard County Clerk of the Court's Office, on September 24, 2015, Z.B.Y. and TOOLE applied for a marriage license and were married at the Brevard County Clerk's Office, Titusville, Florida branch. On April 11, 2016, USCIS received an Immigration Form I-130, Petition for an Alien Relative, which listed TOOLE as the petitioner and Z.B.Y. as the alien spouse. In response to an HSI subpoena, MoneyGram provided that Z.B.Y. sent three wire transfers of funds from New York to TOOLE in Florida. Specifically, on December 23, 2015, Z.B.Y. wired $95.00 to TOOLE. On January 10, 2016, Z.B.Y. wired $80 to TOOLE and on January 31, 2016, Z.B.Y. wired $95 to TOOLE.

24. On April 19, 2016, I conducted surveillance of the SUBJECT PREMISES and observed YAKOVLEV arrive while driving a 2004 Nissan Armada, with Florida license plate GNEQ73. The registration for this vehicle was queried and lists the current owner as TOOLE. YAKOVLEV, carrying a plastic bag, exited the vehicle with a

dog.

25. On April 24, 2016, a cooperating source of information (SOI) received a text from (305) 310-0721, a pre-paid cell phone stating "I was looking for older guy for week they been waiting." The SOI has personal knowledge that this cell phone number belongs to YAKOVLEV and relayed the message to me. The SOI understood this text to mean that YAKOVLEV wanted her to find an older USC male to match the age of an older female foreign national asking to take part in the scheme.

26. I served a subpoena on AT&T/Cricket, who provided that (305) 310-0721 is a prepaid phone registered to Dennis DERRETT at 127 Seaport Blvd, Cape Canaveral, FL 32920. According to AT&T/Cricket, the phone was activated on September 27, 2014, and 127 Seaport Blvd. is the address listed on expired Florida Driver's License Y214-178-77-205-0, for Denis YAKOVLEV, according to Florida's Drive and Vehicle Information Database (DAVID).

27. On May 6, 2016, the SOI told me that he/she received a series of text messages from YAKOVLEV, via (305) 310-0721, where YAKOVLEV asked the SOI if the "old guy" had an identification card, birth certificate and if he had a job. Based on my training and experience and knowledge I knew that these identity documents are required for applying for a marriage license and/or filing immigration benefit applications.

28. On May 10, 2016, based on YAKOVLEV's request to the SOI for a male over the age of fifty to marry a foreign national for immigration purposes, I utilized an HSI undercover agent (UCA1) who fit the parameters requested by YAKOVLEV for this role. UCA1 used a hidden recording device to record the following events in both visual

and audio form.

29. Later that day, UCA1 met with YAKOVLEV and a woman the SOI identified as his girlfriend, TOOLE, at a picnic table outside of 5050 Ocean Beach Blvd., Cocoa Beach, Florida. After meeting, YAKOVLEV and TOOLE took UCA1 inside the SUBJECT PREMISES. Once inside, UCA1 was introduced to a foreign national, N.P., and an older male, later identified to be G.C.

30. Immigration database checks revealed that N.P. and G.C. are both citizens of Moldova. On January 25, 2012, N.P. entered the United States on a B-2 visa, which is nonimmigrant visitor for pleasure. N.P. was admitted to enter into the United States for a period not to exceed six months. There are no records of departure for N.P. and no other pending applications for status in the United States; therefore, she is no longer in a lawful status within the United States.

31. While UCA1 talked to N.P. and TOOLE, YAKOVLEV simultaneously entered into an extended conversation with N.P. and G.C. in Russian which was later interpreted by an HSI agent fluent in Russian who reviewed the audio and video recordings provided by UCA1. N.P. asked YAKOVLEV how much she was expected to pay that day. YAKOVLEV replied that he usually took 4 (understood to mean $4,000). Additionally, YAKOVLEV explained what documents were needed for the immigration applications, and highlighted the immigration document (Form AR-11) necessary to change one's address.

32. Later, N.P. asked the UCA1 to travel to Miami in the near future, where she currently resided, for purposes of preparing to pass a USCIS interview. YAKOVLOV then explained the expectations for UCA1's involvement. First, he told

UCA1 that he would need to remain married to N.P. for two years, but immediately after the marriage, N.P. would pay UCA1 $8,000. Second, YAKOVLEV told UCA1 that he would have to attend an in person interview and that N.P. would pay for his travel to Miami for the interview.

33. YAKOVLOV told UCA1 that he would do all the necessary immigration paperwork "here" (i.e. in the SUBJECT PREMISES) without UCA1 having to be present.

34. YAKOVLEV told UCA1 that he would need two passport pictures of both N.P. and UCA1 to submit as part of N.P.'s immigration petition.

35. UCA1, N.P., G.C. and the SOI traveled together to the Brevard County Clerk of the Court office (Merritt Island, Florida branch) for the marriage. Once at the clerk's office, another HSI undercover agent, UCA2, posing as a deputy clerk, provided a fictitious marriage license and performed a fictitious marriage ceremony. After the ceremony, N.P. went inside the Merritt Island Chase Bank at 760 E. Merritt Island Causeway, Merritt Island, Florida, and made a cash withdrawal. After the bank, UCA1, N.P., G.C. and the SOI returned to the SUBJECT PREMISES of YAKOVLEV in Cocoa Beach, Florida.

36. Once they arrived, UCA1 observed YAKOVLEV sitting in a chair in the living room beside the copier/printer working on a laptop type computer. YAKOVLOV asked UCA1 for his identification, a birth certificate and driver's license, which he proceeded to photocopy on a copier/printer which was located in the corner of the room. While YAKOVLOV was photocopying the documents, UCA1 viewed YAKOVLEV's computer screen and recognized that he was filling out USCIS Form G-325A (Biographic Information), i.e. one of the required forms USCIS requires in conjunction

with alien relative petitions. I know based on my training and experience as well as cooperation in this investigation by CIS that the forms observed by UCA1 are available to fill out, save and download from the USCIS website.

37. UCA1 observed as N.P. took an unknown amount of money from a bank envelope in her purse and gave it to YAKOVLOV. Then, YAKOVLOV counted the money and gave the UCA1 $800 (eight $100 bills). YAKOVLOV also reiterated to UCA1 he would receive $8,000 in total for entering into the marriage with N.P. and that he would be paid incrementally when he met with her in Miami (with travel expenses paid), when he attended the USCIS interview and when N.P. received her green card.

38. In addition to the fictitious marriage laid out in this affidavit, I believe that YAKOVLEV and/or TOOLE have arranged approximately forty similar fictitious marriages based on cross referencing names from the Brevard County Clerk of Courts with YAKOVLEV's phone records, and Western Union and MoneyGram wires sent to YAKOVLEV.

39. Based upon the foregoing, I submit that there is probable cause to charge Denis YAKOVLEV and Meghan Marie TOOLE with Title 8, United States Code, Section 1324(a)(1)(A)(iv), and probable cause to believe YAKOVLEV and TOOLE also violated Title 8, United States Code, Section 1324(a)(1)(v)(A)(II) and Title 18, United States Code, Section 371 and that probable cause exists to search 5050 Ocean Beach Blvd, Apt. 106, Cocoa Beach, Florida, identified in Attachment A, for the evidence identified in Attachment B.

Timothy Scott, Special Agent
Homeland Security Investigations

Hon. David A. Baker
United States Magistrate Judge
7/6/2016

ATTACHMENT A

Property to be searched

The property to be searched is **5050 Ocean Beach Blvd, Apt 106, Cocoa Beach, FL 32931**, further described as Multi-Story Beachfront Condominium with a parking lot and detached car garages assigned to different units. This building has two staircases on each end of the front of the building and an elevator in the middle of the front all located on the east side of the building. There are nine units located on the same level as 106. The door for the apartment/condo number is marked with 106 and the door is facing north and any storage unit and or detached garage solely assigned to Apt 106 located on the premises.

ATTACHMENT B

1. All records relating to violations of Title 8, United States Code, Sections 1324(a)(l)(A)(iv) and (v)(II); and conspiracy to commit such violations, in violation of Title 18, United States Code, Section 371 (Subject Offenses), those violations involving Denis YAKOVLEV and Meghan Marie TOOLE and occurring after January 1, 2014, including:

a. Documents, records, and files, in whatever form, related to the Subject Offenses, the identification of co-conspirators, and the obstruction of this investigation.

b. Records and information relating to the identity or location of the suspects;

c. Books, records, receipts, notes, ledgers, notebooks, banking records, airline tickets, money orders, deposit box keys and records, storage unit keys and records, and mailing and shipping records, in whatever form, related to the Subject Offenses, the identification of co-conspirators, and the obstruction of this investigation.

d. Currency, financial instruments, and other items that are fruits of the Subject Offenses, as well as such items that are evidence of financial transactions relating to obtaining, transferring, laundering, and spending the proceeds of the Subject Offenses.

e. Any computers, cellular telephones, other electronic devices, or electronic media that were or may have been used as a means to commit the offenses described on the warrant, including any computer used to

communicate concerning the Subject Offenses, to keep financial records concerning the Subject Offenses, or to keep records of the activity of the conspirators.

2. Computers or storage media used as a means to commit the violations described above, including bringing in and harboring certain aliens in violation of Title 8, United States Code, Section 1324(a)(1)(A)(iv), and aiding and abetting the commission of bringing in and harboring certain aliens, in violation of Title 8, Section 1324(a)(1)(A)(v)(II); and conspiracy to commit an offense against or defraud the United States, that is, to bring in and harbor certain aliens, in violation of Title 18, United States Code, Section 371.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as

well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.