

## UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)APPLE IPHONE SEIZED FROM 534 BALTIMORE STREET, DAYTON,  
OHIO 45404, CURRENTLY LOCATED IN THE SECURE EVIDENCE  
LOCKER OF THE REGIONAL ELECTRONICS COMPUTER  
INTELLIGENCE TASK FORCE, 644 LINN STREET SUITE 600,  
CINCINNATI, OHIO 45203

Case No. 1:19-MJ-00681

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

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

See Attachment B

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

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

The search is related to a violation of:

Code Section  
18 U.S.C. 4  
18 U.S.C. 1028A  
18 U.S.C. 1544

Misprison of a Felony  
Aggravated Identity Theft  
Misuse of a Passport

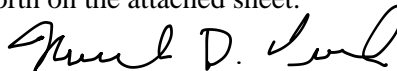
Offense Description

The application is based on these facts:

See Attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

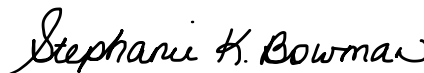
Michael Reigle, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: Oct 16, 2019

City and state: Cincinnati, Ohio



Judge's signature

Hon. Stephanie K. Bowman, U.S. Magistrate Judge

Printed name and title



**ATTACHMENT A**

The property to be searched is an Apple iPhone, enclosed in a clear case, seized from the residence located at 534 Baltimore Street, Dayton, Ohio, 45404, on October 11, 2019, hereinafter the “Device.” The Device is in the lawful possession of the FBI, currently located in the secure evidence locker of the Regional Electronics Computer Intelligence task Force at 644 Linn Street, Suite 601, Cincinnati, Ohio, 45203. Photographs of the Device are included below.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.



**ATTACHMENT A CONTINUED**



**ATTACHMENT B**

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, § 4 (misprision of a felony), 1028A (aggravated identity theft); and 1544 (misuse of a passport) and involve **BARIS ALI KOCH**, since **July 2019**, including:
2. Any records of communication between KOCH and his brother, Izmir Koch, during the above described time-period, including those regarding the improper use of KOCH's passport, or other identification documents, to enter a foreign country; and photographs, images, records, regarding the same;
3. Any records of communication between KOCH and others regarding the improper use of KOCH's passport, or other identification documents, to enter a foreign country; and photographs, images, records, regarding the same;
4. Bills, shipping records, and other records related to travel or the shipment of packages;
5. Any evidence tending to show KOCH's knowledge regarding the misuse of his passport and identity;
6. All bank records, checks, credit card bills, account information, and other financial records; and
7. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF OHIO  
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF  
AN APPLE IPHONE SEIZED FROM 534  
BALTIMORE STREET, DAYTON, OHIO  
45404, CURRENTLY LOCATED IN THE  
SECURE EVIDENCE LOCKER OF THE  
REGIONAL ELECTRONICS COMPUTER  
INTELLIGENCE TASK FORCE, 644 LINN  
STREET, SUITE 601, CINCINNATI, OHIO  
45203

Case No. **1:19-MJ-00681**  
UNDER SEAL

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

I, Michael D. Reigle, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been employed as a Special Agent (“SA”) of the Federal Bureau of Investigation (“FBI”) since 2002, and am currently assigned to the Cincinnati Division. During my employment with the FBI, I have been assigned to a variety of matters, to include white collar crime, counterintelligence, and counterterrorism. I have gained experience through training at the FBI, conferences, and everyday work related to conducting investigations into these types of matters. In the course of my employment, I have gained knowledge regarding the evidentiary value of electronic devices such as computers and cell phones. As a federal agent, I

am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

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

#### **IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

4. The property to be searched is an Apple iPhone seized from the residence located at 534 Baltimore Street, Dayton, Ohio, 45404, on October 11, 2019, hereinafter the “Device.” The Device, which is in the lawful possession of the FBI, is currently located in a secure evidence locker of the Regional Electronics Computer Intelligence Task Force located at 644 Linn Street, Suite 601, Cincinnati, Ohio, 45203.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

#### **PROBABLE CAUSE**

6. Izmir Ali Koch, a.k.a. Izmir Kuchaliyevich Vafiev, the older brother of BARIS ALI KOCH, was convicted on December 17, 2018, for one count each of Title 18, United States Code, §§ 249 and 1001, in violation of the Matthew Shepard and James Byrd, Jr. Hate Crimes Prevention Act, and Making False Statements, respectively, in United States District Court for the Southern District of Ohio in case number 1:18:CR-034.

7. On July 9, 2019, Izmir Ali Koch was sentenced to 30 months incarceration, a \$10,000 fine, \$9,200 in restitution, and three years of supervised release in the aforementioned case. Izmir Ali Koch was allowed to self-report and was designated by the United States Bureau

of Prisons to report to Federal Correctional Institution (FCI) Gilmer, located in Glenville, West Virginia, on August 16, 2019.

8. Izmir Ali Koch failed to self-surrender and an arrest warrant was issued by United States District Court Judge Susan J. Dlott, on Tuesday, August 20, 2019, when the United States Marshals Service confirmed he had failed to report.

9. On September 4, 2019, in the Southern District of Ohio, Izmir Ali Koch was indicted in case number 1:19:CR-107 on one count of Title 18, United States Code, § 3146(a)(2) failure to appear for service of a sentence, and an arrest warrant was issued by the Honorable United States Magistrate Court Judge Stephanie K. Bowman. Both arrest warrants were entered into the National Crime Information Center database.

10. Izmir Ali Koch and BARIS ALI KOCH were both born in Toytepa, Uzbekistan. They both resided in Kholmskaya, Russia, when they filed their paperwork to come to the United States as refugees. They have both maintained their Russian passports, in addition to their United States passports, and have used both to travel back and forth to the Krasnodar region in Russia, prior to the recent criminal proceedings. Their stated travel purposes included visiting family and attending weddings in Rostov, Russia. Zamira Kuchalievna Redvanova, their only sister, has lived in Rostov, Russia, and her husband, Ravshan Redvanov, still resides there. FBI investigation indicates that she splits her time between Russia and the United States.

11. BARIS ALI KOCH attended all of the hearings, the trial, and the sentencing of Izmir Ali Koch.

12. On August 13 or 14, 2019, BARIS ALI KOCH contacted Izmir Ali Koch's former defense attorney and told him that he was worried about Izmir Ali Koch because he had



left his telephone at the office the night before and nobody had seen him since. The attorney asked BARIS ALI KOCH if he had reported him missing and was told that he had not. The attorney warned BARIS ALI KOCH that if Izmir did not report, Izmir would be in serious trouble and that anybody who is helping him could face criminal charges as well. BARIS ALI KOCH told the attorney that neither he, nor anyone in his family, knew where Izmir Ali Koch was, nor were they helping him.

13. After Izmir Ali Koch failed to self-surrender for punishment of his felony conviction, BARIS ALI KOCH was interviewed on September 11, 2019, about Izmir Ali Koch's whereabouts. Also present at the location of the interview was Murad Ali Koch and Ali Koch, Izmir Ali Koch's older brother and father, respectively. BARIS ALI KOCH told the interviewing agents that he last saw Izmir Ali Koch on or about Friday, August 9, 2019, at their family business, located at 1501 Webster Street, Dayton, Ohio 45404. Izmir Ali Koch was driving his 2013 black Mercedes when he arrived, but left it at the business, along with his mobile telephone, number (937) 760-3666, keys, business cards, a bank debit card, and an old driver's license. Izmir Ali Koch only stayed for approximately 10 minutes, but neither BARIS ALI KOCH nor Murad Ali Koch knew where Izmir Ali Koch went or how Izmir Ali Koch was traveling. Additionally, BARIS ALI KOCH commented that he did not think Izmir Ali Koch could have left the United States, as BARIS ALI KOCH had assisted Izmir Ali Koch in surrendering both his United States and Russian passports to the court.

14. When asked where Izmir Ali Koch's 2013 black Mercedes was currently, BARIS ALI KOCH said he sold it to pay for debts Izmir Ali Koch had left for the family. A review of the registration records for Izmir Ali Koch's black Mercedes, Vehicle Identification Number WDDLJ9BB7DA075958, revealed that Izmir Ali Koch had transferred the vehicle to BARIS

ALI KOCH, on August 6, 2019. At the time of the transfer, the vehicle mileage was 56,500. On August 26, 2019, BARIS ALI KOCH sold the vehicle to Carmax Auto Superstores Inc., located in Dayton, Ohio. At the time of the sale, the vehicle had 56,692 miles on it.

15. On September 4, 2019, Nargiz Koch, Izmir Ali Koch's wife, was interviewed about the whereabouts of her husband. Nargiz Koch said the last time she saw her husband was on August 10, 2019. However, in a prior interview on August 26, 2019, her brother, Osman Mardall, reported the last time Nargiz Koch saw Izmir Ali Koch was on or about August 7, 2019. Nargiz Koch said that she and her children have been very upset since her husband disappeared and BARIS ALI KOCH has been looking for Izmir Ali Koch without success. Nargiz Koch celebrated a big holiday on August 11, 2019, at Izmir Ali Koch's mother's house, located at 534 Baltimore Street, Dayton, Ohio 45404. All of Izmir Ali Koch's family was there, except for Izmir Ali Koch.

16. A review of Ohio Bureau of Motor Vehicle (BMV) records for BARIS ALI KOCH revealed that he obtained a driver's license, license number TU309704, on July 19, 2019, and a replacement license on August 21, 2019. On September 20, 2019, Jeff Payne, Chief, Ohio BMV Record Services, provided certified records documenting that BARIS ALI KOCH stated that he lost his driver's license both times he had it reissued.

17. A confidential source indicated that around the time Izmir Ali Koch was sentenced, Izmir modified his appearance to the likeness of BARIS ALI KOCH's driver's license. The confidential source saw that Izmir Ali Koch had BARIS ALI KOCH's driver's license in his possession to facilitate changing his appearance to more closely resemble that of BARIS ALI KOCH.

18. Ohio BMV records list 534 Baltimore Street, Dayton, Ohio 45404, as the residence of BARIS ALI KOCH. Additionally, Lexis-Nexis, a public records database, lists BARIS ALI KOCH residing at 534 Baltimore Street, Dayton, Ohio 45404. Finally, your affiant interviewed BARIS ALI KOCH at 534 Baltimore Street, Dayton, Ohio 45404, and he identified the residence as his home.

19. United States Department of State confirmed that a United States passport, bearing number 507493295, was issued to BARIS ALI KOCH, a.k.a. BARYSH KUCHALJEVICH, on June 12, 2013, and will expire on June 11, 2023.

20. According to the Mexican National Institute of Migration, on August 9, 2019, “Baria Ali Koch,” an individual born on February 17, 1989, who entered Mexico by land as a visitor, provided United States passport number 507493295, during a routine immigration inspection point at the Reynosa Airport requiring an official passport. BARIS ALI KOCH was, in fact, born on February 17, 1989.

21. Based on the August 9, 2019, presentation of BARIS ALI KOCH’s passport at Reynosa Airport, it is evident that BARIS ALI KOCH lied during his September 11, 2019 interview, when he claimed to have seen Izmir Ali Koch in person on August 9, 2019, as there is no record of either BARIS ALI KOCH or Izmir Ali Koch flying domestically, or internationally, from a United States airport during that time, and Izmir Ali Koch could not have driven to Mexico, from Dayton, Ohio, in time to reveal BARIS ALI KOCH’s passport to the Mexican authorities on August 9, 2019.

22. Furthermore, it is your affiant’s opinion, based on numerous contacts with BARIS ALI KOCH during the hate crime investigation involving Izmir Ali Koch and others, that BARIS

ALI KOCH has been consistently hostile and unreliable, often espousing alternative scenarios versus the truth, when speaking with law enforcement.

23. On August 15, 2019, BARIS ALI KOCH received a DHL Express Shipment, tracking number 1242783065. The package was sent to BARIS ALI KOCH, 534 Baltimore Street, Dayton, Ohio 45404. The package was sent from BARIS ALI KOCH, Pr-T Stachki 25, Rostov Na Donu, Russia 344000. The package description was listed as "PASSPORT, COPIES OF DOCUMENTS." Ali Koch signed the receipt for the package delivery. BARIS ALI KOCH did not reveal the existence of this package during his September 11, 2019 interview with agents regarding Izmir Ali Koch's possible whereabouts.

24. As a result of Izmir Ali Koch not reporting as designated by the United States Bureau of Prisons, the FBI has interviewed his family members and members of the community, as well as conducted surveillance on people and addresses related to Izmir Ali Koch. Additionally, an FBI wanted poster was created and posted to the media. No leads led to the apprehension of Izmir Ali Koch. Investigative efforts and results lead me to conclude, based on my training and experience, that Izmir Ali Koch left the United States using BARIS ALI KOCH's passport while BARIS ALI KOCH remained in the United States. No individual apart from Izmir Ali Koch had the opportunity and motive to obtain and use BARIS ALI KOCH's passport.

25. There is no record of either BARIS ALI KOCH or Izmir Ali Koch flying domestically or internationally to or from a United States airport since August 9, 2019, when BARIS ALI KOCH's passport was presented at the Reynosa Airport in Mexico. Furthermore, there is no record of BARIS ALI KOCH's passport being presented at any border checkpoints in

order to enter the United States after August 9, 2019. I am aware that the real BARIS ALI KOCH is still located within the United States, based on my personal observations. Therefore, the real BARIS ALI KOCH could not have used his passport to travel outside the United States in August 2019, and also be present in the United States in October 2019.

26. Since Izmir Ali Koch was sentenced to a prison term, BARIS ALI KOCH has made steps to sell or liquidate major assets, including his business and Izmir Ali Koch's home. Information provided during an interview of Izmir Ali Koch's neighbor described BARIS ALI KOCH showing Izmir Ali Koch's residence to prospective buyers in the community. Recent surveillance in the old north Dayton area revealed that Murad Ali Koch, BARIS ALI KOCH's brother, has put his residence up for sale. Murad Ali Koch, along with BARIS ALI KOCH and their extended family, are all aware that Izmir Ali Koch is a wanted fugitive. Recent online searches have also revealed that the Koch business location at 1501 Webster Street, Dayton, Ohio 45404, is currently for sale. All of these are indications that BARIS ALI KOCH and/or his extended family plan to move in the near future.

27. On October 11, 2019, the Honorable United States Magistrate Court Judge Stephanie K. Bowman signed an arrest warrant for BARIS ALI KOCH as well as two search warrants authorizing agents to execute searches at BARIS ALI KOCH's residence located at 534 Baltimore Street, Dayton, Ohio 45404, as well as his business located at 1501 Webster Street, Dayton, Ohio 45404. Those search warrants authorized agents to seize evidence relating to violations of Title 18, United States Code, § 4 (misprision of a felony), 1028A (aggravated identity theft); and 1544 (misuse of a passport). This warrant authorized, among other things, the seizure of electronic devices such as cell phones.

28. The Device was found in the living room of BARIS ALI KOCH's residence located at 534 Baltimore Street, Dayton, Ohio 45404 during the October 11, 2019 search. SAs saw BARIS ALI KOCH take the Device out of his pocket when they arrived at his residence. The Device belongs to BARIS ALI KOCH.

29. The Device is currently in the lawful possession of the FBI. It came into the FBI's possession after arresting BARIS ALI KOCH pursuant to an arrest warrant and execution of a search warrant at his residence. Therefore, while the FBI might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

30. SA Pamela S. Kirschner, the co-case agent for this investigation, took the Device to a secure evidence locker at the Regional Electronics Computer Intelligence Task Force located in Cincinnati, Ohio, 45203, after its seizure on October 11, 2019.

31. In my training and experience, I know that the Device has been stored and kept in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

### **TECHNICAL TERMS**

32. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication

through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.



- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. 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.

33. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at <http://apple.com>, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

#### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

34. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

35. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device 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).

Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

- b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- c. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic 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.
- d. Further, in finding evidence of how a device 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.

36. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but

not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

37. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

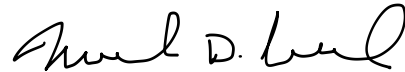
### **CONCLUSION**

38. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

### **REQUEST FOR SEALING**

39. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

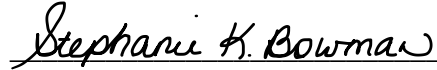
Respectfully submitted,



---

Michael D. Reigle  
Special Agent  
FBI

Subscribed and sworn to before me  
on October 16, 2019:



---

THE HONORABLE STEPHANIE K. BOWMAN  
UNITED STATES MAGISTRATE JUDGE



**ATTACHMENT A**

The property to be searched is an Apple iPhone, enclosed in a clear case, seized from the residence located at 534 Baltimore Street, Dayton, Ohio, 45404, on October 11, 2019, hereinafter the “Device.” The Device is in the lawful possession of the FBI, currently located in the secure evidence locker of the Regional Electronics Computer Intelligence task Force at 644 Linn Street, Suite 601, Cincinnati, Ohio, 45203. Photographs of the Device are included below.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.



**ATTACHMENT A CONTINUED**



**ATTACHMENT B**

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, § 4 (misprision of a felony), 1028A (aggravated identity theft); and 1544 (misuse of a passport) and involve **BARIS ALI KOCH**, since **July 2019**, including:
2. Any records of communication between KOCH and his brother, Izmir Koch, during the above described time-period, including those regarding the improper use of KOCH's passport, or other identification documents, to enter a foreign country; and photographs, images, records, regarding the same;
3. Any records of communication between KOCH and others regarding the improper use of KOCH's passport, or other identification documents, to enter a foreign country; and photographs, images, records, regarding the same;
4. Bills, shipping records, and other records related to travel or the shipment of packages;
5. Any evidence tending to show KOCH's knowledge regarding the misuse of his passport and identity;
6. All bank records, checks, credit card bills, account information, and other financial records; and
7. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;



As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.