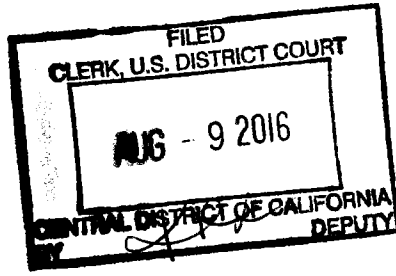
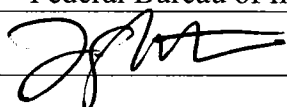
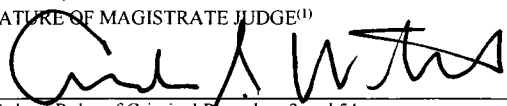


ORIGINAL

AO 91 (Rev. 11/82)

## CRIMINAL COMPLAINT

UNITED STATES DISTRICT COURT		CENTRAL DISTRICT OF CALIFORNIA	
UNITED STATES OF AMERICA v. MIKHAIL KONSTANTINOV MALYKHIN		DOCKET NO.	
		MAGISTRATE'S CASE <b>M 16 01594</b>	
Complaint for violation of Title 18, United States Code, Section 1029(b)(2)			
NAME OF MAGISTRATE JUDGE HONORABLE ANDREW J. WISTRICH		UNITED STATES MAGISTRATE JUDGE	LOCATION Los Angeles, California
DATE OF OFFENSE From a date unknown to on or about April 18, 2016	PLACE OF OFFENSE Los Angeles County	ADDRESS OF ACCUSED (IF KNOWN)	
COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION:  <p style="text-align: center;">[18 U.S.C. § 1029(b)(2)]</p> <p>Beginning on a date unknown and continuing to on or about April 18, 2016, in Los Angeles County, within the Central District of California, defendant MIKHAIL KONSTANTINOV MALYKHIN knowingly and intentionally conspired to use unauthorized access devices in a one-year period to obtain things of value aggregating to \$1,000 or more.</p> <div style="text-align: right;">  </div>			
BASIS OF COMPLAINANT'S CHARGE AGAINST THE ACCUSED: (See attached affidavit which is incorporated as part of this Complaint)			
MATERIAL WITNESSES IN RELATION TO THIS CHARGE: N/A			
Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge.	SIGNATURE OF COMPLAINANT <b>LEROY SHELTON</b>		
	OFFICIAL TITLE Special Agent – Federal Bureau of Investigation		
Sworn to before me and subscribed in my presence, 			
SIGNATURE OF MAGISTRATE JUDGE <sup>(1)</sup> 			DATE August 9, 2016

<sup>(1)</sup> See Federal Rules of Criminal Procedure 3 and 54

**AFFIDAVIT**

I, Leroy Shelton, being duly sworn, declare and state as follows:

**I. INTRODUCTION**

1. I am a Special Agent (“SA”) with the Federal Bureau of Investigation (“FBI”) and have been so employed since 2012. I am currently assigned to the Los Angeles Field Office, Cyber Crime Squad, which is responsible for investigating computer and high-technology crimes. During my career as an FBI SA, I have participated in numerous cyber-related investigations. During the investigation of these cases, I have participated in the execution of numerous arrests, search warrants, and seizures of evidence. Since my assignment to the Cyber Crime Squad, I have received both formal and informal training from the FBI regarding cyber investigations. Through these means, I have learned about schemes and designs commonly used to commit financial- and technology-based crimes, as well as the practices that individuals who commit financial- and technology-based crimes employ while attempting to thwart law enforcement’s efforts to effectively investigate those crimes.

**II. PURPOSE OF AFFIDAVIT**

2. This affidavit is made in support of a criminal complaint against, and arrest warrant for, Mikhail Konstantinov MALYKHIN (“MALYKHIN”) for a violation of 18 U.S.C. § 1029(b)(2) (conspiracy to commit access device fraud).

3. This affidavit is also made in support of an application for a warrant to search:

- a. the residence located at 6220 W. 3rd Street, Apartment 213, Los Angeles, California 90036 (the “SUBJECT PREMISES”); and
- b. a gray Infiniti QX70 bearing vehicle identification number JN8AS1MW2GM734514 and California license plate 7FBE086 (the “SUBJECT VEHICLE”).

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for

the requested complaint and warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

### **III. SUBJECT PREMISES**

5. The SUBJECT PREMISES to be searched is located at 6220 W. 3rd Street, Apartment 213, Los Angeles, California and further described in Attachment A-1, which is incorporated herein by reference.

### **IV. SUBJECT VEHICLE**

6. The SUBJECT VEHICLE to be searched is a gray Infiniti QX70 bearing vehicle identification number JN8BS1MW9EM400148 and California license plate 7FBE086, and described in Attachment A-2, which is incorporated herein by reference.

### **V. SUMMARY OF PROBABLE CAUSE**

7. On or about December 18, 2015, a cyber intruder(s) accessed the software system of Polestar Benefits, Inc. ("Polestar"), a healthcare third-party administrator. During this intrusion, the cyber intruder(s) re-activated the accounts of 43 previous employees of one of Polestar's clients, affiliated those accounts to a Dependent Care Plan, and then ordered 10 Flexible Spending Account cards, which functioned essentially as high-limit credit cards, to be mailed to a variety of locations, including to persons in Southern California. Among the cards ordered were: (a) a MasterCard ending in 6977 in the name of Anthony Kleiner ("MasterCard 6977"); (b) a MasterCard ending in 8116 in the name of Andrey Chan Woo ("MasterCard 8116"); and (c) a MasterCard ending in 4504 in the name of Damir Zhanov ("MasterCard 4504").

8. During the investigation, multiple individuals were identified purchasing items at local Best Buy, Apple, Home Depot, and furniture and hydroponic stores. On April 18, 2016, multiple arrest and search warrants authorized by the Honorable Jacqueline Chooljian, United States Magistrate Judge, Central District of California, in Case No. 16-0825M were executed on four co-conspirators. On approximately April 21, 2016, one of the four defendants arrested (the

“cooperator”)<sup>1</sup> agreed to cooperate with law enforcement and identified MALYKHIN as the individual responsible for the Polestar intrusion. The cooperator also indicated that MALYKHIN is responsible for a number of other computer intrusions and credit card fraud using a laptop computer that is stored at the SUBJECT PREMISES, and that MALYKHIN stores a backup of his computer on a SanDisk flash drive that is kept in the middle console of SUBJECT VEHICLE. Surveillance video gathered during the investigation corroborates MALYKHIN’s involvement in the conspiracy. Specifically, surveillance video shows MALYKHIN entering a Best Buy store and accompanying the cooperator while the cooperator purchased items with MasterCard 8116. MALYKHIN was also captured on video exiting the store with a shopping cart of the purchased items.

## **VI. STATEMENT OF PROBABLE CAUSE**

### **A. FBI Investigation**

9. The FBI Portland and Los Angeles Field Offices are currently investigating the unauthorized access of computer systems alleged to have been conducted by a Russian Organized Crime Syndicate (“ROCS”) located in Los Angeles, California, and Russia. Based on the investigation to date, documented reports, and my discussions with other investigating agents, I have learned that, on or about December 18, 2015, perpetrator(s) accessed computer systems of victim company Alegeus Technologies (“Alegeus”), a provider of platforms for corporate insurance plans through the Internet,<sup>2</sup> by using stolen login credentials of a third-party

---

<sup>1</sup> The cooperator’s criminal history consists of a domestic violence-related conviction in January 2016. The cooperator’s motivation for cooperation is to seek leniency from the government in the cooperator’s criminal case. The cooperator understands that no promises have been made with respect to what, if any, consideration the cooperator will receive in exchange for providing the information described herein. The cooperator has provided law enforcement with the passwords to five of his/her email accounts. I was able to access two of those accounts with the provided passwords, but was unable to access the other three accounts with the passwords the cooperator provided.

<sup>2</sup> The Internet is a collection of computers and computer networks which are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information. Connections between Internet computers exist across state and international borders; therefore, information sent between two computers connected to the Internet frequently crosses state and international borders even when the two computers are located in the same state.

administrator, Polestar. During the computer intrusion, perpetrator(s) re-activated 43 accounts of one of Polestar's clients and ordered ten Flexible Spending Account ("FSA") cards, which functioned essentially as high-limit credit cards. The total credit limit set was approximately \$91 million and the cards were mailed to a variety of locations. Among the cards ordered and used in southern California were MasterCard 6977, MasterCard 8116, and MasterCard 4504.

## **B. Polestar**

10. Based on the investigation to date and my review of reports of documented conversations with Polestar President Eric Graham and Operations Manager Karen Montgomery, and my discussions with other investigating agents, I have learned that, on or about January 19, 2016, Polestar contacted the FBI and reported the unauthorized access and purchases referenced above. At the time of the report, Polestar was only aware of approximately \$440,000 in fraudulent charges but the final figure was approximately \$510,000.

11. Based on the investigation to date and reports of documented conversations and my discussions with other investigating agents, I have learned that Polestar is a Lake Oswego, Oregon-based healthcare third-party administrator that offers FSAs and COBRA services to their clients. FSAs are special accounts into which a person puts pre-tax money directly from their paychecks to pay for out-of-pocket health care expenses. When an FSA is funded, a debit card is issued to the account holder to use for payment of medical or health care expenses such as doctor visits and prescriptions. These debit cards are limited by Merchant Category Codes ("MCC"), which limit their use to certain types of purchase transactions. Pre-tax money may also be allotted for dependent care. Dependent care accounts may be used only to pay for childcare expenses or elderly care expenses. The person funding the dependent care account must prove that he or she is eligible. Debit cards are not issued for dependent care accounts. Instead, the person pays the cost for the dependent care up-front and is reimbursed from the dependent care account once they provide the receipts for such care. Polestar facilitates two types of FSA accounts: (1) medical expenses previously not reimbursed by health insurers, and (2) dependent care expenses. One of Polestar's clients is Lane Community College ("LCC"), a two-year

Community college located in Eugene, Oregon. Polestar uses online software services provided by Alegeus, a Massachusetts company, to facilitate their business. Using the Alegeus software platform, Polestar account managers facilitate FSA and dependent care accounts for businesses like LCC which contract with Polestar to provide such benefits. Polestar creates the plans for each customer, assigns MCCs for the FSA cards, and funds the FSA cards. Once FSA cards are created and issued using this platform, a MasterCard-approved fulfillment vendor is notified, which then mails the FSA cards to the recipients. Polestar was hired to set up dependent care accounts for LCC employees who opted to have one. The funds in dependent care accounts are used to reimburse LCC employees once they provide the receipts showing they have paid for the care of a dependent.

12. Based on my discussions with other investigating agents, and my review of reports documenting conversations with Polestar employees and records provided by Alegeus, I have learned that Polestar believes that between approximately December 18, 2015 and January 18, 2016, perpetrator(s) accessed Alegeus computer systems using the credentials of an account manager employed by Polestar without authorization from Polestar. Polestar only became aware of the cyber intrusion when they viewed their account manager's profile and saw the unauthorized charges on that account. Polestar learned that the perpetrator(s) re-activated the accounts of 43 previous employees of LCC and affiliated those re-activated accounts to dependent care accounts that the perpetrator(s) created. Once the affiliation was complete, the perpetrator(s) ordered several debit cards under the plan and mailed the cards to a variety of locations. The perpetrator(s) set various limits for the cards ranging from \$500,000 to as high as \$5 million. The cards were created and modified in such a way that they functioned as regular credit cards. Specifically, instead of the cards having a limited number of MCCs assigned to them under a particular plan as is typical for FSAs, these cards were placed under a plan created by the perpetrator(s) using the account manager's credentials in which all MCCs were enabled. It is unknown at this time how the plan for dependent care was created, issued, and funded.

13. Based on the investigation to date and my review of reports documenting conversations with Polestar employees, I have learned that, of the 43 LCC accounts that were fraudulently re-activated, ten cards were ultimately funded, mailed, and subsequently used to make in-store point-of-sale (“POS”) purchases at multiple retail outlets in California, Maryland, New Jersey, and Moscow, Russia.

**C. Perpetrators Identified in Los Angeles, California**

14. Based on the investigation to date and the comparison of surveillance videos from the retail stores to photographs on file with the California Department of Motor Vehicles (“DMV”), the following individuals were identified as individuals making at least approximately \$200,000 of the more than \$390,000 in fraudulent purchases: Dmitry Fedoseev (“Fedoseev”), Irina Fedoseeva (“Fedoseeva”), Siarhei Patapau (“Patapau”), and Timur Safin (“Safin”). Surveillance video for the remaining transactions is unavailable at this time.

15. Based on the investigation to date it has been determined that Patapau used MasterCard 4504 to make over \$162,000 in purchases at various retail stores in Los Angeles, California and its adjacent counties, between January 16 and 18, 2016. It is further believed that Patapau and/or his associates returned some items purchased for cash and/or store credit and kept the remaining items for themselves and/or to sell at a later date.

16. Based on the investigation to date it has been determined that Safin used MasterCard 6977 to make over \$137,000 in purchases at various retail stores in Los Angeles, California and its adjacent counties between January 16 and 18, 2016. It is further believed that Safin and/or his associates returned some items purchased for cash and/or store credit and kept the remaining items for themselves and/or to sell at a later date.

17. Based on the investigation to date it has been determined that Fedoseev and Fedoseeva used MasterCard 8116 to make over \$91,000 in purchases at various retail stores in Los Angeles, California between January 17 and 18, 2016. It has also been determined that Fedoseev had returned over \$11,000 worth of items purchased for store credit. They spent more than \$45,000 on furniture at Rapport International Furniture (“Rapport”) on January 17, 2016

between 4:55 p.m. and 6:14 p.m. No surveillance video of the transactions was available upon request, but store employees identified Fedoseev and Fedoseeva as making the purchases using MasterCard 8116. The following items were purchased: a gray Fly modular sofa with chaise longue, a taupe Riflesso rug, a grey Viaggio armchair, a 10" high Tempo central table, a walnut 350 credenza with three drawers, a beige Riflesso rug, a Volo reclining sofa, a Hyper model 2026 cocktail table, a Skagen dining table, a Haven laptop desk with caviar glass and smoke grey walnut finish, a beige Poliziano sofa, a white Logos armchair, and a Ferrari Red Parabolica swivel chair.

**D. Items Purchased by Patapau, Safin, Fedoseev and Fedoseeva at Best Buy, Target, and Apple**

18. Based on my review of documented reports and receipts, I learned the following were among items purchased with MasterCard 4504, MasterCard 6977, and MasterCard 8116 at Best Buy, Target, and Apple: televisions, computer tablets, media players, smart watches, cellular telephones, drones, laptop computers, computer software, hard drives, routers, cameras, audio headphones and speakers, robotic vacuums, video game consoles and games, cameras, electric razors, toothbrushes, and streaming devices.

**E. Arrest and Search Warrants Executed on Patapau, Safin, Fedoseev and Fedoseeva**

19. Based on my review of documented reports and my conversations with other investigating agents, I learned that on April 18, 2016, the Honorable Jacqueline Chooljian, United States Magistrate Judge, Central District of California, authorized arrest warrants for Patapau, Safin, Fedoseev, and Fedoseeva, as well as searches of their respective residences and vehicles. All four individuals have been permanently detained pending trial on charges including violations of 18 U.S.C. §§ 1028A (aggravated identity theft) and 1029(b)(2) (conspiracy to commit access device fraud).



**F. Identification of MALYKHIN as Head of ROCS and the Hacker Responsible For Computer Intrusions**

20. On April 21, 2016, May 24, 2016, and June 17, 2016, the cooperator was interviewed and provided the following information, among other things:

a. The cooperator identified MALYKHIN as the “hacker” responsible for the computer intrusions into Alegeus, Polestar, and FlexMagic Consulting (“FlexMagic”), another third-party administrator defrauded of approximately \$3.5 million on or about March 2016. [Agent’s Note: on April 26, 2016, the CEO of FlexMagic was interviewed by FBI Special Agent Samantha Baltzersen and confirmed being victimized of \$3.5 million dollars in fraudulent transactions over the weekend of March 26, 2016. The transactions originated from Los Angeles, New York, and overseas. FlexMagic could not pay the fraudulent transactions and has been forced to close its business, thus leaving the responsibility for the losses on Alegeus.]

b. The cooperator and MALYKHIN have known each other for approximately 14 years and have been conducting various types of fraud together during that time. The cooperator met MALYKHIN in Russia where MALYKHIN first taught the cooperator how to conduct fraud using eBay. MALYKHIN is known to use the online monikers “LAX” and “EBay” to sell items on eBay. MALYKHIN eventually moved to the United States (“U.S.”) and helped the cooperator move to the U.S. as well. By that time, MALYKHIN was no longer involved in eBay fraud and had moved on to “carding” (credit card fraud). MALYKHIN is in possession of a Washington State driver’s license because he was never able to obtain a California driver’s license due to not having the proper legal documentation. MALYKHIN claims that Washington State driver’s licenses are easy to obtain.

c. The cooperator moved to the United States approximately nine years ago. The cooperator does not recall MALYKHIN ever having a job other than “carding” and committing other types of fraud such as filing false tax returns. MALYKHIN started filing false tax returns approximately three years ago.

d. MALYKHIN told the cooperator that he has approximately \$5 million in a safety deposit box located at a vault on Olympic Boulevard, Los Angeles, California. MALYKHIN accesses the vault through an iris scan. The cooperator believes the money came from a combination of filing false tax returns and from ATM cash-out schemes.<sup>3</sup> The tax return funds came from approximately 5,000 American Express prepaid cards that were preloaded with false tax return proceeds, filed and processed by 20 or 30 people who were paid 20 to 30 percent of the proceeds for their help. The ATM funds came from cash-out schemes. The cooperator recalled receiving 20 ATM cards in approximately January 2016 from MALYKHIN, who instructed the cooperator to withdraw cash from ATMs. These ATM cards were not associated to any of the victim companies mentioned in this affidavit. The cooperator withdrew \$90,000 in cash one night and brought it to the SUBJECT PREMISES. The cooperator estimates seeing \$500,000 in cash at MALYKHIN's apartment, and received \$10,000 from MALYKHIN for the cooperator's help. The cooperator helped deliver the cash to MALYKHIN's vault but was not able to enter the vault. The cooperator last visited MALYKHIN's vault approximately six months ago. In addition to the vault, MALYKHIN keeps his money in a few different places, including a safety deposit box, bank accounts, and Russia.

e. MALYKHIN owns a trucking company with co-conspirator/partner Sergey Smolin ("Smolin"), which they use primarily to launder money obtained through their fraud schemes. MALYKHIN met Smolin approximately six years ago through a mutual friend known only as "Igor." MALYKHIN's trucking company is managed by a friend known only as "Alec." According to the cooperator, MALYKHIN is the head of the ROCS and uses Smolin because Smolin "knows people." Smolin recruits Russian college students through the website vk.ru, a Russian equivalent of the social media website Facebook.com. The students are in the U.S on J-1 visas and are paid to file false tax returns, obtain fake driver's licenses, open residential and P.O. Box addresses, conduct ATM cash-out schemes, and commit other types of

---

<sup>3</sup> ATM cash-out schemes refer to the simultaneous withdrawals of cash from numerous ATMs.

acts to further MALYKHIN's fraud schemes. [Agent's Note: On April 20, 2016, the FBI Portland Field Office conducted database queries on MALYKHIN. The results of the query confirmed MALYKHIN and Smolin own a 2012 Volvo truck tractor. Accurant database checks also attribute Evgeny Igorevich Barsukov ("Barsukov") as an associate of MALYKHIN. Based on my training and experience, I believe Barsukov could also be known as "Igor," short for Igorevich.]

f. MALYKHIN also works with his brother Roman Malykhin ("R. Malykhin"), who lives in Russia. MALYKHIN sends R. Malykhin credit card numbers and stolen proceeds through various currency exchange companies. MALYKHIN once gave the cooperator a number of ATM cards and \$100 to purchase a card reader to scan the cards and send the card numbers to R. Malykhin. The cooperator did as instructed and sent the cards via sendspace.com, which is an online file-sharing service. MALYKHIN pays the cooperator ten percent of the cash withdrawals he makes from the cards given to him by MALYKHIN.

g. MALYKHIN is a member of the underground forums<sup>4</sup> "cardingworld.cc" and/or "cardingworld.cw," "verified," "Motherfucker," and "Korovka." The websites are designed as online platforms for criminals to communicate, sell/buy stolen information, and to make contacts, among other things. MALYKHIN's email addresses are "padonak@mail.ru" and "paddonak@gmail.com." [Agent's Note: On April 20, 2016, FBI Portland Field Office conducted an internal law enforcement database query on MALYKHIN. The results of the query confirmed MALYKHIN is associated with email address "paddonak@gmail.com."]

h. MALYKHIN is technically savvy with computers but relies on a computer hacker (the "Hacker"), who owns a BOTNET,<sup>5</sup> to provide him with stolen login credentials.

---

<sup>4</sup> An Internet forum, or message board, is an online discussion site where people can hold conversations in the form of posted messages. They differ from chat rooms in that messages are often longer than one line of text, and are at least temporarily archived.

<sup>5</sup> A BOTNET is a network of private computers infected with malicious software and controlled as a group without the owners' knowledge. The word BOTNET is a combination of the words robot and network. The term is usually used with a negative or malicious connotation.

MALYKHIN met the Hacker in an online Russian forum a long time ago and communicates with the Hacker through Jabber, a free instant messaging service. The Hacker compromises victim computers through malware<sup>6</sup> that is distributed via SPAM emails. The SPAM emails contain a file (malware) which, once executed, provides the Hacker with full access to the victim computer which is then added to the Hacker's BOTNET. The malware acts as a keylogger.<sup>7</sup> This specific keylogger logs all username and passwords. Once the Hacker collects the raw data, it is given to MALYKHIN, who mines it for information of value and conducts searches using search phrases like "insurance admin login." MALYKHIN lent the Hacker \$100,000 to purchase additional domain names and to improve the BOTNET. At one point, MALYKHIN had access to the BOTNET and was able to search the exfiltrated logs for terms like "insurance account usernames and passwords." However, the cooperator believes MALYKHIN's access to the BOTNET was taken away sometime in early 2016.

i. MALYKHIN uses a Toshiba Qosmio laptop to conduct his fraud.

MALYKHIN's laptop is located at the SUBJECT PREMISES. MALYKHIN's laptop runs Microsoft Windows 7 and has VMware<sup>8</sup> installed. VMware software allows MALYKHIN to run a virtual computer ("VM") instance which also runs Microsoft Windows 7 on a TrueCrypt<sup>9</sup> encrypted volume. MALYKHIN uses a paid virtual private network ("VPN"<sup>10</sup>) and proxy

---

<sup>6</sup> Malware is an abbreviated term meaning "malicious software." This software is specifically designed to gain access or damage computer without the knowledge of the owner.

<sup>7</sup> A keylogger is a type of surveillance software (considered to be either software or spyware) that has the capability to record every keystroke. A keylogger recorder can record instant messages, e-mail, and any information you type at any time using your keyboard.

<sup>8</sup> In computing, a virtual machine (VM) is an emulation of a particular computer system. Virtual machines operate based on the computer architecture and functions of a real or hypothetical computer, and their implementations may involve specialized hardware, software, or a combination of both.

<sup>9</sup> TrueCrypt is a discontinued source-available freeware utility used for on-the-fly encryption. It can create a virtual encrypted disk within a file or encrypt a partition or the entire storage device.

<sup>10</sup> A VPN is a method used to add security and privacy to private and public networks, like WIFI Hotspots and the Internet. VPN's are used by hackers for its 'tunnel-like' connection.

service<sup>11</sup> to obscure his true IP address<sup>12</sup> within his VM. MALYKHIN layers both services on top of each other to strengthen his anonymity. MALYKHIN stores a complete backup of his VM on a SanDisk flash drive which he kept in the middle console of SUBJECT VEHICLE.

j. MALYKHIN logged into the Alegeus online platform upon the discovery of the Polestar login credentials. MALYKHIN is not a programmer but does understand a lot about computers and the inner-workings of the financial system. Upon gaining access to the Alegeus system, MALYKHIN re-activated the 43 LCC accounts (described above), increased the spending limits, and ordered the FSA cards. Several of the benefit cards were mailed directly to Russia. After the FSA cards arrived, Smolin arranged for some individuals to work with MALYKHIN to validate the FSA cards by making a few small purchases. The purchases were declined but generated a rejection code which MALYKHIN subsequently entered into the Alegeus system so that the cards would work. MALYKHIN had the cards re-validated and they worked. MALYKHIN provided FSA cards to “Smolin’s people” and gave the cooperator a Polestar FSA card in the name of Andrey Chan Woo (“Woo”). The cooperator states that he found Woo’s California driver’s license in his mailbox and gave it to MALYKHIN. MALYKHIN returned Woo’s driver’s license to the cooperator with MasterCard 8116. Woo’s true name is Andrew Chan Woo Choe.

k. In approximately January 2016, MALYKHIN instructed the cooperator to buy furniture for MALYKHIN and himself at Rapport. As instructed, the cooperator purchased a number of items under the fake name “Sergei Ivanov” and arranged for a delivery truck to deliver the furniture to SUBJECT PREMISES. [Agent Note: prior to the furniture pickup, the

---

It allows the user’s IP address to be masked, providing a layer of all-important privacy and anonymity.

<sup>11</sup> A Proxy server is a dedicated computer or a software system running on a computer that acts as an intermediary between an endpoint device, such as a computer, and another server from which a user or client is requesting information.

<sup>12</sup> An Internet Protocol address (“IP address”) is a unique numeric address used by each computer 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 must be assigned an IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most ISPs control a range of IP addresses.

cooperator hired a local “Mexican” day laborer known only as “Samuel” to help him with the pickup and delivery.] The cooperator attempted to deliver the items to MALYKHIN at the SUBJECT PREMISES but MALYKHIN was not there. A few days later MALYKHIN picked up the furniture and brought it to SUBJECT PREMISES. The cooperator also purchased furniture for MALYKHIN in approximately March 2016 with a FlexMagic FSA card. The cooperator recalls seeing some of the purchased furniture and other fraudulently-acquired items at the SUBJECT PREMISES in approximately March 2016. The cooperator described the items as being a bed, two tables, a white sofa, a dinner table, an LG flat screen TV, Apple iPhones (some opened, some not), and an Apple MacBook Pro purchased for MALYKHIN’s girlfriend known to the cooperator as “Viktoriia.” The cooperator also saw at the SUBJECT PREMISES a “MSR206” card reader and numerous blank credit cards. [Agent’s Note: Per the MSR206 manual which I obtained from the Internet, “a MSR206 card reader is designed to offer a magnetic card reading/writing solution for ISO 7811-6 formats. It reads and writes up to 3 tracks of data simultaneously. Also, the MSR206 provides a standard RS232 interface to communicate with a host system or other terminal computer.”]

l. The cooperator claims that Viktoriia is aware of MALYKHIN’s fraud and is complicit in it. Also, MALYKHIN tells everyone what he does for a living. [Agent’s Note: based on my training and experience and knowledge of this investigation, I believe that this means that MALYKHIN is open about conducting fraud for a living.] Viktoriia received a number of items from MALYKHIN, including an Apple MacBook Pro laptop and an electronic keyboard all purchased with fraudulently-obtained funds. The cooperator has seen these items at Viktoriia’s apartment located at 7660 Beverly Blvd, Los Angeles, California. Viktoriia lives in the same apartment complex as MALYKHIN’s estranged ex-wife and drives a Maserati but does not have a job. MALYKHIN recently paid for plastic surgery for both Viktoriia and another unknown female who supposedly is MALYKHIN’s “fake wife” for U.S. citizenship purposes.

m. The cooperator described the SUBJECT PREMISES as a one bedroom, one bathroom apartment.

21. Based on my review of reports of interviews, I learned that on January 22, 2016, FBI Special Agent Jeffrey Pritchett interviewed a Rapport associate regarding purchases made with MasterCard 8116 totaling over \$45,000 on January 17, 2016. The Rapport associate stated the customer returned on January 19, 2016 with a small box truck bearing California license plate ending in 18B1, accompanied by a driver.

a. A subsequent investigation by Special Agent Pritchett into the California license plate number ending in 18B1 indicated the registered owner of the box truck is Samuel Molina ("Molina"), consistent with the cooperator's statement that he was assisted by "Samuel." Attempts to locate Molina have been unsuccessful to date.

b. On February 9, 2016, Special Agent Pritchett interviewed a Rapport associate, who indicated that all four purchases made by MasterCard 8116 were made by an individual named "Sergey Ivanov," as indicated by the cooperator.

22. Based on my review of reports, I learned that on February 11, 2016, FBI Special Agent Tsoler Kojayn and Los Angeles Police Department Detective Asatur Mkrtchyan interviewed Rapport sales associates regarding purchases made with MasterCard 8116. During the interview, the sales associates were shown pictures of the cooperator and positively identified the cooperator as one of the two individuals whom they observed using MasterCard 8116.

23. At the end of the cooperator's May 24, 2016 interview, the cooperator provided agents with the passcode to unlock the cooperator's Apple iPhone 6 seized during the execution of a search warrant on the cooperator's residence.

a. On approximately June 9, 2016, I forensically imaged the cooperator's cellular telephone. Upon completion, I created a working copy and started my review of the cooperator's photographs.

b. During the cooperator's June 17, 2016 interview, FBI Special Agent William Cone III showed the cooperator a number of photographs found on the cooperator's cellular telephone. One of the photographs depicted a dining room table displayed at Rapport.



The cooperator acknowledged purchasing the table for MALYKHIN and delivering it to the SUBJECT PREMISES. The dining table is a solid wood table, brown in color.

24. On June 24, 2016, I spoke with an associate of the property management company of the SUBJECT PREMISES. The associate confirmed that MALYKHIN was a tenant of SUBJECT PREMISES and was obligated to pay the rent through September 19, 2016, per his lease agreement. The property management associate also confirmed that MALYKHIN listed the SUBJECT VEHICLE as his on his lease agreement. MALYKHIN is assigned to tandem parking stalls 191 and 192. During my visit, I also received a layout design of SUBJECT PREMISES, which is consistent with what the cooperator described: a small one bedroom, one bathroom apartment.

25. Based on my review of reports and conversations with other investigating agents, I learned that on approximately January 17, 2016, the cooperator, accompanied by MALYKHIN and Viktoriia, made two purchases totaling over \$12,000 at Best Buy (store #393) using MasterCard 8116. During the cooperator's interview on June 17, 2016, agents showed the cooperator multiple surveillance photographs provided to the FBI by Best Buy's asset protection department on or about January 26, 2016. The cooperator identified himself/herself, MALYKHIN as a white male wearing a short black t-shirt, and Viktoriia as a white female wearing a black leather jacket.

a. In May 2016, United States Secret Service ("USSS") Special Agent Peter Gannon provided the FBI a spreadsheet of losses by FlexMagic due to the above-described cyber intrusion.

i. On June 29, 2016, I reviewed the spreadsheet of the charges incurred by FlexMagic. The spreadsheet displayed four attempted charges in the name of Viktor Bogomolov between March 27 and 28, 2016 for \$30,000 at a plastic surgery office located in Beverly Hills, California. Three of the four attempted transactions were declined and one was approved.



ii. On approximately July 1, 2016, I interviewed the doctor and office manager of the plastic surgery office located in Beverly Hills, California. The office manager provided information on the two females that came in for their consultation. The office manager positively identified one of the females as Viktoriia Levyschenko ("Levyschenko"), MALYKHIN's girlfriend, which is consistent with the cooperator's statement.

26. On approximately June 7, 2016, I conducted law enforcement database checks on MALYKHIN and confirmed that his telephone number is (323) 652-6073. MALYKHIN's telephone number was also confirmed on June 25, 2016, when I received tenant information from his property management company.

27. On approximately June 9, 2016, I conducted a search in the cooperator's iPhone for MALYKHIN's telephone number and found hundreds of text messages between the cooperator and MALYKHIN, all in Russian. Between June 13 and 17, 2016, 14 pages of text messages were reviewed by a certified Russian linguist of the USSS. USSS Special Agent Dmitriy Bukin found the following three text messages sent by MALYKHIN to the cooperator that corroborate the time of events referenced in this affidavit:

<u>Date &amp; Time</u>	<u>Text Messages Translated</u>
1/18/2016, 05:20:05 PST	Tomorrow from you (you bring) moving truck, Mexicans, and iPhones in the amount of 20K and come over (by car)
1/18/2016, 05:20:27 PST	I'll take the cash for the Mexicans
1/18/2016, 12:56:19 PST	Yes everything is fine

28. On approximately April 11, 2016, Apple, Inc. ("Apple") responded to an FBI request for information pertaining to three purchases totaling over \$20,000. Apple claimed the transactions were cancelled while the user was trying to purchase a dozen items ranging from Apple iPads to Apple MacBook Pro laptops. Included with Apple's response were video surveillance stills clearly identifying the cooperator wearing the same clothing worn the night before at Best Buy.

29. On or about June 7, 2016, I requested vehicle registration records from the FBI Operations Control Center for MALYKHIN. MALYKHIN has three vehicles registered under his name, including the SUBJECT VEHICLE.

**VII. TRAINING AND EXPERIENCE REGARDING ACCESS DEVICE FRAUD**

30. In my training and experience, individuals who are involved in criminal financial activities and computer intrusions will often keep records pertaining to the crime on computers, cellular phones, and other digital devices. That information may include, but is not limited to, contact lists, communications between parties to the crime, information on how the crimes were committed, and information specific to the digital device which shows it was used to facilitate the crime such as registry, browsing, and log information.

31. In my training and experience, individuals who are involved in criminal financial activities and computer intrusions will sometimes keep items needed to continue their schemes, and proceeds of their schemes, in their vehicles and residences, such as fraudulently-issued debit and credit cards, profile information, credit card stock such as “white plastic,” gift cards, other credit card instruments containing a magnetic strip, computers, cellular phones, thumb drives, CDs, other data storage devices, and products purchased through criminal financial activities.

32. In my training and experience, individuals who are committing financial and technology-based crimes may save paper documents related to their activities. These documents can include logs of fraudulent transactions and monies received and may refer to names of individuals and companies that have been victimized and payments to or from co-schemers, or records of the sale or transfer of the proceeds of the criminal activity.

33. In my training and experience, individuals who are committing financial and technology-based crimes who use fraudulently obtained or counterfeit credit and debit cards often use and receive cash in exchange for merchandise or gift cards purchased or received with such cards.

34. In my training and experience, individuals who are committing financial and technology-based crimes who purchase large amounts of consumer products may sell or “fence”

the fraudulently obtained goods via hand-to-hand sales transactions, street-level black markets, and/or online platforms such as eBay and Craigslist. The sale of these items is often dependent upon the item being taken outside of its packaging to assure the purchaser of existence of the actual item, either through a direct visual inspection or photograph. As such, these items may or may not still be in their original packaging.

35. In my training and experience, individuals who are committing financial and technology-based crimes utilizing fraudulently obtained or counterfeit credit or debit cards typically use stolen or fictitious personal identification information and documents, including social security numbers, driver licenses, and passports, to create false identities. The false identities are then embossed and/or encoded onto counterfeit or fraudulently obtained credit and debit cards. This allows the criminal to purchase goods and services, such as obtaining rental vehicles, without disclosing their true identities.

#### **VIII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES**

36. As used herein, the term “digital device” includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, 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 hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a 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 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. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary 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 downloaded or viewed content. 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. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive 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 digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional

data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

37. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract

and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

38. As discussed herein, based on my training and experience I believe that digital devices will be found during the search. I know from my training and experience and my review of publicly available materials that Apple, Motorola, HTC, and Samsung, among other companies, produce devices that can be unlocked by the user with a numerical or an alpha-numerical password, or, for some newer versions of the devices, with a fingerprint placed on a fingerprint sensor. Each company has a different name for its fingerprint sensor feature; for example, Apple's is called "Touch ID." Once a user has set up the fingerprint sensor feature in the security settings of the device, the user can unlock the device by placing a finger or thumb on the device's fingerprint sensor. If that sensor recognizes the fingerprint or thumbprint, the device unlocks. Most devices can be set up to recognize multiple prints, so that different prints, not necessarily from the same person, will unlock the device. In my training and experience, users of devices with a fingerprint sensor feature often enable that feature, because it unlocks the phone more quickly than the entry of a passcode or password but still offers a layer of security.

39. In some circumstances, fingerprint sensors will not work, and a passcode must be entered to unlock the device. For example, with Apple, Touch ID will not work if (1) more than 48 hours have passed since the device has been unlocked, (2) the device has been turned on or restarted, (3) the device has received a remote lock command, or (4) five attempts to match a fingerprint have been unsuccessful. Other brands have similar restrictions. I do not know the passcodes of the devices likely to be found at the SUBJECT PREMISES.

40. For these reasons, while executing the warrant, agents will likely need to use the fingerprints or thumbprints of any user(s) of any fingerprint sensor-enabled device(s) to attempt to gain access to that device while executing the search warrant. The warrant seeks the authority to compel the use of the fingerprint and/or thumbprint of every person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint sensor-enabled device that is located at the SUBJECT



PREMISES and falls within the scope of the warrant. The government may not be able to obtain the contents of the devices if those fingerprints are not used to access the devices by depressing them against the fingerprint sensor at the time of the search. Although I do not know which of the fingers are authorized to access on any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors, and in any event all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

41. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

#### **IX. ITEMS TO BE SEIZED**

42. Based on the foregoing, I respectfully submit that there is probable cause to believe that the items listed in Attachment B, which constitute evidence of violations of 18 U.S.C. §§ 1029(b)(2) (conspiracy to commit access device fraud), and 1030(a)(2)(A), (C) (unauthorized computer access), will be found at the SUBJECT PREMISES and the SUBJECT VEHICLE.

#### **X. REQUEST FOR SERVICE AT ANY TIME OF THE DAY OR NIGHT AND REQUEST TO EXCUSE THE REQUIREMENTS OF 18 U.S.C. § 3109**

43. Based on my training, experience, conversations with other law enforcement agents, my prior experience serving search and arrest warrants, and knowledge of individuals who utilize encryption on their digital devices, I am requesting permission to serve the warrants at any time of the day or night and permission to not comply with the “knock notice” requirements of 18 U.S.C. § 3109 for the following reasons:

a. MALYKHIN maintains a high level of operational security. According to the cooperator, MALYKHIN has taken steps to mask his illegal activities online and encapsulate his digital data through encryption. Based on my training and experience, individuals who take these types of precautionary measures intend to prevent law enforcement from finding their location and/or obtaining evidence during the execution of a search warrant. In order to



maximize the chances of recovering evidence at the SUBJECT PREMISES, the warrants need to be executed while MALYKHIN is using his laptop. Otherwise, the laptop will likely be in an encrypted state that will be inaccessible by law enforcement. MALYKHIN is an unemployed career criminal and is highly unlikely to be awake at 6:00 a.m. since he does not have a job to wake up to. Indeed, based on surveillance I and other agents have conducted, we have observed that MALYKHIN and his girlfriend, Levyschenko, do not keep normal business hours and have not been observed in the early morning. I believe, based on my training and experience and knowledge of this investigation, that MALYKHIN is most likely to be using his computer at night while MALYKHIN is awake.

b. Maintaining the element of surprise by executing the warrants during the “night time” hours and without knocking and announcing will reduce the possibility that evidence will be destroyed, particularly where the encryption of digital devices is concerned. It would likely only take MALYKHIN a few keystrokes to encrypt his digital devices, effectively preventing law enforcement from ever accessing the data on those devices. Knocking and announcing would give him time to do just that.

44. The factors detailed above demonstrate reasonable suspicion that requiring executing officers to execute the warrants during standard warrant service hours and to announce their presence would be futile and inhibit the effective investigation of the crimes described herein by enabling the destruction of evidence.


## **XI. CONCLUSION**

45. For all the reasons described above, there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 1029(b)(2) (conspiracy to commit access device fraud), and 1030(a)(2)(A), (C) (unauthorized computer access), as described above and in Attachment B of this affidavit, will be found in a search of the SUBJECT PREMISES and the SUBJECT VEHICLE, as further described above and in Attachment A of this affidavit, and that

///

///

MALYKHIN has committed a violation of 18 U.S.C. § 1029(b)(2) (conspiracy to commit access device fraud).

  
\_\_\_\_\_  
Leroy Shelton, Special Agent  
Federal Bureau of Investigation

Subscribed to and sworn before me  
this 9 day of August, 2016.

  
\_\_\_\_\_  
UNITED STATES MAGISTRATE JUDGE