

RMT:MEL/MW
F.#2015R01725

16M653

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

-----X
UNITED STATES OF AMERICA

TO BE FILED UNDER SEAL

- against -

VYACHESLAV KHAIMOV,

Defendants.

COMPLAINT AND
AFFIDAVIT IN SUPPORT OF
ARREST WARRANT
(18 U.S.C. §§ 371, 1343, 1344,
1956(a)(2)(B)(i), 1956(h), 2 and
3551 et. seq.)

-----X

EASTERN DISTRICT OF NEW YORK, SS:

GEORGE SCHULTZEL, being duly sworn, deposes and states that he is a special agent with the Federal Bureau of Investigation ("FBI"), duly appointed according to law and acting as such.

Count One: Conspiracy to Commit Wire Fraud and Bank Fraud

Upon information and belief, in or about and between July 2015 through May 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VYACHESLAV KHAIMOV, together with others, did knowingly and intentionally conspire to (a) devise a scheme and artifice to defraud, and obtain money and property by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals and sounds, contrary to Title 18, United States Code, Section 1343 and (b) execute a scheme or artifice to defraud a financial institution and to obtain moneys, funds, credits, assets, securities and other property under the custody and control of financial institutions by means of

materially false and fraudulent pretenses, representations and promises, all contrary to Title 18, United States Code, Section 1344.

(Title 18, United States Code, Section 371 and 3551 et seq.)

Count Two: Wire Fraud

Upon information and belief, in or about and between July 2015 through May 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VYACHESLAV KHAIMOV, together with others, did knowingly and intentionally devise a scheme and artifice to defraud, and obtain money and property by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals and sounds, to wit: wire transfers.

(Title 18, United States Code, Section 1343, 2 and 3551 et seq.)

Count Three: Bank Fraud

Upon information and belief, in or about and between July 2015 through May 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VYACHESLAV KHAIMOV, together with others, did knowingly and intentionally execute a scheme or artifice to defraud financial institutions, and to obtain moneys, funds, credits, assets, securities and other property under the custody and control of financial institutions by means of materially false and fraudulent pretenses, representations and promises.

(Title 18, United States Code, Section 1344, 2 and 3551 et seq.)

Count Four: Money Laundering Conspiracy

Upon information and belief, in or about and between July 2015 through May 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants VYACHESLAV KHAIMOV, together with others, did knowingly and intentionally conspire to transmit and transfer monetary instruments and funds from a place in the United States to a place outside the United States knowing that the monetary instrument or funds involved in the transportation, transmission or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission or transfer is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership or the control of the proceeds of specified unlawful activity, to wit: the crimes charged in Counts One through Three, contrary to Title 18, United States Code, Section 1956(a)(2)(B)(i).

(Title 18, United States Code, Section 1956(h) and 3551 et seq.)

Count Five: Money Laundering

Upon information and belief, in or about and between July 2015 through May 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants VYACHESLAV KHAIMOV, together with others, did knowingly and intentionally transmit and transfer monetary instruments and funds from a place in the United States to places outside the United States knowing that the monetary instrument or funds involved in the transportation, transmission or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission or transfer is designed in whole or in part to conceal or disguise the nature, the location, the source, the

ownership or the control of the proceeds of specified unlawful activity, to wit: the crimes charged in Counts One through Three.

(Title 18, United States Code, Section 1956(a)(2)(B)(i), 2 and 3551 et seq.)

The source of your deponent's information and the grounds for his belief are as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI").

I have been a Special Agent with the FBI for over 6 years. As a Special Agent, I have participated in numerous investigations involving computer-related crimes, fraud, public corruption, racketeering and terrorism, among others. These investigations are conducted both in an undercover and overt capacity. I have participated in investigations involving search warrants and arrest warrants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities

2. The facts in this affidavit come from my personal observations, my training and experience; information obtained from other agents, and a review of records and documents. Because the purpose of this affidavit is limited to demonstrating probable cause for the requested warrant, it does not set forth all of my knowledge about this matter. In addition, when I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated.

Factual Background

3. The FBI has been investigating a criminal network that uses malicious software ("malware") and other means to take control of victim bank accounts and illegally wire funds out of these accounts. The illegally obtained funds are then transferred via wire to

the bank accounts of a network of individuals within the United States who in turn further transmit the money, or portions of the money, either to additional U.S.-based intermediaries or directly overseas.

4. Many of the intermediary bank accounts are opened by individuals referred to as “money mules” or “mules.” Based on my training and experience as well as this investigation, mules are typically unsuspecting individuals who believe they are working for a legitimate “work from home” business. As part of their “employment,” the mules are instructed, typically via email, to open a bank account and receive the funds that have been removed from victims’ bank accounts. The mule is then provided further instructions as to where to send the money she/he has received. The FBI has learned from interviews and lawfully obtained emails that many of the mules involved in this scheme were recruited by an individual who identified himself as “Samuel Gold.” Their communications were primarily via email or over the phone, and none of these individuals had ever met Samuel Gold.

5. In or around September 2015, the FBI identified an individual residing in Long Island, New York (“Victim-1”) whose online banking credentials were believed to have been compromised by malware on or about August 12, 2015.

6. On that date, over \$44,000 was removed from Victim-1’s bank account and wired into the bank account of an individual (“Suspected Mule-1”) who, on information and belief, was recruited by members of the criminal network to serve as a mule.

7. On August 12, 2015, Suspected Mule-1 wired \$42,500 of the money stolen from Victim-1 to VYACHESLAV KHAIMOV, who resides at an address in Brooklyn,

New York. Five days later, on August 17, 2015, KHAIMOV wired \$24,580 to an overseas bank account in the name of a co-conspirator (“CC-1”) located in Thailand.

8. Further investigation revealed that since July 13, 2015, over \$230,000 in funds were fraudulently withdrawn from the bank accounts of at least eight bank account takeover victims via wire transfers from a network of intermediary mules. The \$230,000 was deposited into bank accounts held individually in KHAIMOV’s name and bank accounts in the name of Global Universal, a company owned and controlled by KHAIMOV. Of that amount, KHAIMOV subsequently transferred over \$110,000 overseas to accounts in the names of CC-1 and two other co-conspirators. Specifically, KHAIMOV wired over \$80,000 to CC-1 between June 2015 and October 2015; he wired over \$10,000 in illegally obtained funds to another co-conspirator (“CC-2”) in July 2015; and over \$18,000 to a third co-conspirator (“CC-3”) between March 2015 and August 2015.¹

9. For two victims (“Victim-2” and “Victim-3”), whose money was sent overseas by KHAIMOV in July 2015, their accounts were unlawfully accessed via the same IP address (“IP Address-1”) during the course of the thefts.² Investigation revealed that IP Address-1 was also previously used in connection with the bank account compromises of four other victims between October 2014 and June 2015 (“Victim-4,” “Victim-5,” “Victim-6,” and

¹ The investigation has revealed fourteen bank accounts in the name of CC-2 at eleven different banks in three different countries.

² An IP address is a unique numerical label assigned to each device (e.g., a computer or a printer) that participates in a computer network that uses the internet protocol for communication. Typically, if a target uses a computer connected to the network and law enforcement obtains the IP address for that network, law enforcement can determine where that computer is located, and thus where the target is located.

During the course of the theft, Victim-2’s account was also accessed by a second IP address connected with this scheme. See *infra* paragraph 12.

“Victim-7”). Specifically, on October 23, 2014, approximately \$37,000 was fraudulently withdrawn from Victim-4’s account. On January 29, 2015, two fraudulent wire transfers of approximately \$22,000 and \$14,000 were made from Victim-5’s account.³ In the case of Victim-6, while investigation revealed that the account was unlawfully accessed on April 15, 2015, monies were not withdrawn. Finally, a June 24, 2015 theft of over \$32,000 from Victim-7’s account was successfully recovered by the intermediary bank before further transfers could take place.

10. The approximately \$37,000 transferred out of Victim-4’s account was deposited into the account of an individual (“Suspected Mule-2”). The next day, on October 24, 2014, Suspected Mule-2 wired approximately \$34,000 to one of CC-2’s overseas bank accounts.

11. Additionally, Suspected Mule-2 had received or attempted to receive stolen bank funds from two additional victims (“Victim-8” and “Victim-9”) during the same time frame. Specifically, Suspected Mule-2 received approximately \$42,000 from the account of Victim-8 on October 7, 2014. Suspected Mule-2 wired approximately \$39,000 the same day to an overseas account held by CC-2. The next day, on October 8, 2014, a fraudulent wire transfer to Suspected Mule-2 in the amount of approximately \$38,000 from Victim-9 was detected and returned to the victim account

12. With respect to Victim-2 and Victim-6, whose accounts were accessed by IP Address-1, a second IP address (“IP Address-2”) was also used to access their accounts during the course of the account takeovers. With respect to Victim-2, both IP Address-1 and

³ Of these, the wire transfer of approximately \$14,000 was successfully recovered by the intermediary bank before it was further transferred.

IP Address-2 were used in the course of transferring approximately \$28,000 and \$26,000 on July 23, 2015 and July 30, 2015, respectively, from his account. These funds were wired to a coconspirator ("CC-4"), who in turn wired \$27,000 and \$24,600 to KHAIMOV on July 24, 2015 and July 30, 2015, respectively. Lawfully obtained emails of CC-4 show that he was provided wire instructions by Samuel Gold.

13. On July 30, 2015, KHAIMOV wired over \$14,000 of monies sent by CC-4 to an overseas account held by CC-1. This wire transfer occurred ten days after KHAIMOV wired over \$10,000 in illegally obtained bank funds to CC-2 (see paragraph 8 supra) and approximately \$4,995 in illegally obtained bank funds to CC-3 at an overseas bank.

14. IP Address-2 was also used in connection with the account compromises of five additional victims ("Victim-10," "Victim-11," "Victim-12," "Victim-13," and "Victim-14") in connection with the theft of over \$340,000 between August 2014 and December 2015. The stolen funds were wired to, among others, KHAIMOV and an overseas bank account held in the name of CC-1. In addition, portions of the stolen funds were wired overseas to accounts in the names of "Reality Management Corp" and "First California Escrow."

15. Both the "Reality Management Corp" and "First California Escrow." accounts are held at banks at which CC-2 also holds accounts in his name. Additionally, bank and email records reveal that the funds sent to the overseas First California Escrow account in Thailand were sent by CC-4 from a U.S. account also in the name First California Escrow, which CC-4 opened at the request of Samuel Gold. Based on these facts, the FBI has reason

to believe that the overseas account for Reality Management Corp. is also being used by the defendant and his coconspirators in connection with this criminal scheme.

16. On December 28, 2015, CC-4 also received approximately \$62,000 from another victim account ("Victim-10"). Of that amount, approximately \$10,000 was wired to KHAIMOV the next day. In total, CC-4 has received stolen bank funds from the accounts of six victims between July 2015 and December 2015, either to an account in his name or the account he opened in the name First California Escrow.

17. Investigation of common modus operandi, common IP addresses, common intermediary mules and ultimate recipients of funds overseas has to date revealed a network of more than twenty money mules and more than thirty victims of this criminal scheme. To date, the FBI has identified over \$1.2 million in losses. Email records and interviews of mules reveal that Samuel Gold was involved in the fraudulent wire transfers pertaining to at least twenty of the victims.

18. The investigation has identified KHAIMOV as an individual residing at an address in Brooklyn, New York. KHAIMOV stated in immigration documents that that he has been employed as a manager at G&P Sports World, Inc. located at 217 Brighton Beach Avenue in Brooklyn, New York ("271 Brighton Beach") since January 1, 2009. A review of lawfully obtained e-mails showed that Samuel Gold repeatedly instructed suspected mules to ship cashier checks to KHAIMOV at 217 Brighton Beach.

a. On July 10, 2015, Gold instructed a mule ("Suspected Mule-3") to send \$17,000 in fraudulently obtained funds by certified check to KHAIMOV at 271 Brighton Beach. Bank records show that Suspected Mule-3 in fact sent this check.

b. On July 28, 2015, Gold instructed a mule (“Suspected Mule-4”) to send \$24,600 in fraudulently obtained funds by certified check written out to Global Universal to KHAIMOV at 271 Brighton Beach, which Suspected Mule-4 confirmed he did on July 30, 2015.⁴

c. On August 12, 2015, Gold instructed a mule (“Suspected Mule-5”) to send \$26,600 in fraudulently obtained funds by certified check written out to Global Universal to KHAIMOV at 271 Brighton Beach. Bank records show that Suspected Mule-5 sent this check and that it was deposited by KHAIMOV.

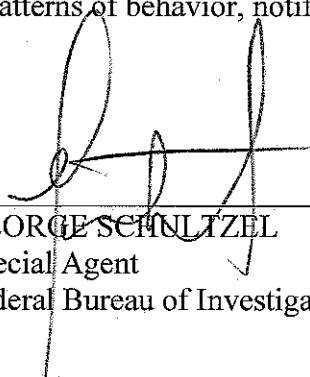
d. On October 15, 2015, Gold instructed a mule (“Suspected Mule-6”) to send \$21,000 in fraudulently obtained funds by certified check written out to Global Universal to KHAIMOV at 271 Brighton Beach. Suspected Mule-6 confirmed he did so later that same day.

e. On December 24, 2015, Gold instructed a mule (“Suspected Mule-7”) to send \$2,400 in fraudulently obtained funds to KHAIMOV at 271 Brighton Beach. On December 28, 2015, Suspected Mule-7 confirmed the check had been sent.

f. On or about May 20, 2016, Gold sent an email to Suspected Mule-4 instructing the mule to send a certified check for more than \$3,000 to KHAIMOV at 271 Brighton Beach. Tracking records show that the check arrived at the SUBJECT PREMISES on May 26, 2016 and was signed for by Khaimov.

⁴ KHAIMOV holds bank accounts in his name as well as a business named as Global Universal. As part of the bank account opening documentation for Global Universal, KHAIMOV provided his address, which is the same address that he provided as his residence in immigration documentation, as well as his telephone number and social security number.

WHEREFORE your deponent respectfully requests that an arrest warrant issue for the defendant VYACHESLAV KHAIMOV so that he may be dealt with according to law. I further request that the Court order that this application, including the affidavit and arrest warrant, be sealed until further order of the Court, except that it may be shared with the defendant and defense counsel following the defendant's arrests in connection with their initial presentment. These documents discuss an ongoing criminal investigation. Disclosure of this application and these orders would seriously jeopardize the ongoing investigation, as such a disclosure would give the targets of the investigation an opportunity to destroy evidence, harm or threaten victims or other witnesses, change patterns of behavior, notify confederates and flee from or evade prosecution.



GEORGE SCHULTZEL
Special Agent
Federal Bureau of Investigation

Sworn to before me this
12 day of July 2016



THE HONORABLE ROANNE L. MANN
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK