

DSS: CMP
F.# 2013R00444

13 M 0278

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - - X

UNITED STATES OF AMERICA

- against -

ELVIS RAFAEL RODRIGUEZ,
also known as
"elvis_rr26@hotmail.com,"

Defendant.

SEALED COMPLAINT AND
AFFIDAVIT IN SUPPORT
OF ARREST WARRANT

(18 U.S.C. § 1029)

- - - - - X

EASTERN DISTRICT OF NEW YORK, SS:

CHRISTIAN WILSON, being duly sworn, deposes and states that he is a Special Agent with the United States Secret Service, duly appointed according to law and acting as such.

Upon information and belief, in or about and between October 2012 and March 2013, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant ELVIS RAFAEL RODRIGUEZ, also known as "elvis_rr26@hotmail.com," together with others, did knowingly and with intent to defraud conspire to effect transactions with one or more access devices issued to another person or persons, to wit: debit cards used to withdraw funds from automated teller machines, to receive payment and other things of value during a

one-year period, the aggregate value of which was equal to or greater than \$1,000, in a manner affecting interstate commerce, contrary to Title 18, United States Code, Section 1029(a)(5).

(Title 18, United States Code, Section 1029(b)(2)).

The source of your deponent's information and the grounds for his belief are as follows:¹

1. I am a Special Agent with the United States Secret Service ("USSS"). I have been employed by the USSS for approximately five years. I am responsible for conducting and assisting in investigations into the illegal use of computers and computer networks by individuals and criminal groups. These investigations are conducted in both an undercover and overt capacity. This assignment requires extensive training in the investigative techniques associated with computer investigations and knowledge of legitimate computer applications. 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

¹ Because this affidavit is submitted for the limited purpose of establishing probable cause, I have not set forth each and every fact learned during the course of the investigation.

activities from detection by law enforcement authorities. I am also familiar with the tools and materials used by individuals carrying out their attacks against computer systems or using computers to facilitate their illegal acts.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: (a) my personal participation in this investigation, (b) reports made to me by other law enforcement authorities, (c) information obtained from confidential sources of information, and (d) interviews with witnesses and victims.

BACKGROUND OF THE INVESTIGATION

3. The USSS is currently investigating an ongoing international conspiracy to hack into the computer systems of financial institutions and other businesses in the United States and abroad for the purpose of stealing confidential financial account information, including account numbers and personal identification numbers ("PINs"). The hackers in turn sell this information to individuals in the United States and other countries over the Internet. The hackers and their associates generally transmit this information through an array of online communication mechanisms, such as email and instant messaging.

Ultimately, the purchasers of the stolen financial information use the account numbers to encode plastic cards, such as gift cards and hotel card keys, which they then use to withdraw currency from automated teller machines ("ATMs") located at banks in the United States and elsewhere in a scheme known as a "PIN cashout," "PIN cashing" or "carding."

4. Based on my experience investigating this and similar carding schemes, I am aware that the participants in such schemes operate in a fluid organizational structure. According to information I have learned through searching email accounts, computers, servers and other forms of electronic evidence, monitoring consensually-recorded communications, and debriefing cooperating witnesses at every level of this informal structure, among other sources, I am aware that the hackers and their financial backers are generally responsible for targeting the victim financial institution; planning the intrusion and executing the attack. These individuals often rely upon a trusted group of business associates to disseminate the stolen financial information globally to managers around the world. These managers generally run local "cashing" crews of individuals (known as "cashers" or "cashiers") who actually conduct the fraudulent transactions via ATM withdrawals and

fraudulent purchases. The majority of the proceeds of PIN cashout operations flow up from the cashers to their managers and then to the higher levels of the operation; the cashers often transfer the funds via international wire transfer services as Western Union and MoneyGram, among other methods. In sophisticated cashout operations, the hackers and their closest business associate may access the victim network during and even after the attack in order to monitor the fraudulent financial transactions and to ensure that they are not being cheated by the cashers and managers.

5. In or about December 2012, an Indian credit card processor that handles Visa and MasterCard prepaid debit cards was the victim of an extensive network intrusion. As a result of this intrusion, the hackers were able to increase the withdrawal limits on prepaid MasterCard debit card accounts associated with the Bank Identification Number ("BIN") 529549. The BIN identifies the issuing financial institution, which in this case was RAKBank, located in the United Arab Emirates. This type of scheme is known in the PIN cashout and carding community as an "unlimited operation." In such operations, hackers in the past have successfully manipulated account balances and in some cases security protocols to effectively

eliminate any withdrawal limits on individual accounts. As a result, even a few compromised bank account numbers can result in tremendous financial loss to the victim financial institution. Based on my experience investigating this and similar operations, I am aware that successful unlimited operations are rare events requiring a high degree of technical proficiency, coordination and patience on the part of criminal actors.

A. The RAKBank Unlimited Operation

6. Between approximately December 21, 2012 and December 22, 2012, five account numbers for the compromised RAKBank accounts with increased balances were distributed to individuals located in approximately 20 countries around the world, including numerous transactions conducted in Brooklyn, Queens and Long Island, among other United States locations. The individuals receiving these card numbers encoded the data onto magnetic stripe cards, such as gift cards and hotel key cards, and used those cards to withdraw funds from ATMs in their respective locations. In total, more than 5,700 ATM transactions were attempted using the compromised RAKBank account data, resulting in a total loss of approximately \$5 million.

B. The Bank of Muscat Unlimited Operation

7. In or about February 2013, a credit card processor based in the United States that handles Visa and MasterCard prepaid debit cards was the victim of an extensive network intrusion that resulted in yet another unlimited operation, in which the hackers increased the withdrawal limits on MasterCard prepaid debit card accounts. In this instance the compromised accounts included multiple BINs, such as 530553, 530555, 530551, 511318 and others, which identified Bank of Muscat, located in Oman, as the issuing financial institution for the compromised accounts.

8. Between approximately February 19, 2013 and February 20, 2013, 12 account numbers for the compromised Bank of Muscat accounts with increased balances were distributed to individuals located in approximately 24 countries across the globe, including numerous transactions conducted in Brooklyn, among other United States locations. The total loss resulting from the Bank of Muscat unlimited operation was approximately \$40 million.

PROBABLE CAUSE

9. In the days following the RAKBank unlimited operation, the USSS obtained surveillance images from various financial institutions and other entities that owned or operated many of the ATMs used to make the fraudulent withdrawals. Surveillance images showed the defendant ELVIS RAFAEL RODRIGUEZ making withdrawals using the same compromised RAKBank account number at several different locations on December 22, 2012. I compared the male described in the following surveillance images to a photograph of RODRIGUEZ that he submitted with his United States passport application on December 5, 2012 and found them to be the same person:

- Surveillance images from the Bank of America ATM located at 2461 Broadway, New York, New York 10025, show RODRIGUEZ making five withdrawals totaling approximately \$4,010 using the same compromised RAKBank account number in a three-minute time period (between 17:08 and 17:11) on December 22, 2012.
- Surveillance images from the Bank of America location at 2077 Broadway, New York, New York 10023 show that in the three-minute period between approximately 17:51 and 17:54 on December 22, 2012, RODRIGUEZ made four fraudulent withdrawals totaling approximately \$3,212 using the same compromised RAKBank account number. Two co-conspirators unidentified in this complaint were simultaneously conducting fraudulent transactions at this location using the same compromised RAKBank account number as RODRIGUEZ.
- Notably, in each of these surveillance images, RODRIGUEZ was wearing a black sock cap emblazoned with

a logo for Domino's Pizza. On RODRIGUEZ's United States passport application submitted in December 2012, he listed his place of employment as Domino's Pizza.

10. The compromised account number that RODRIGUEZ used during the RAKBank unlimited operation was used by co-conspirators to conduct approximately 705 successful ATM withdrawals totaling approximately \$382,597 in and around New York City. Globally, the same compromised RAKBank account number was used to conduct approximately 1,084 fraudulent withdrawals for a total loss of approximately \$628,985.

11. In the days following the Bank of Muscat unlimited operation on approximately February 19, 2013 and February 20, 2013, the USSS obtained surveillance images from the various financial institutions and other entities around the world that owned or operated ATMs used to make fraudulent withdrawals with the same various compromised Bank of Muscat account numbers. Although RODRIGUEZ has not yet been positively identified in any of these images, three of RODRIGUEZ's co-conspirators who were identified in ATM surveillance footage making fraudulent withdrawals during the RAKBank unlimited operation (using the same compromised RAKBank account number as RODRIGUEZ) have been identified as making fraudulent withdrawals in and around New York City using the same compromised Bank of

Muscat account number. Based on my experience investigating these and similar unlimited operations, I am aware that the leaders of these criminal operations generally distribute only a single compromised account number to a particular "crew" so that the leaders of the operation can monitor the total fraudulent withdrawals for any given account number in order to make sure that they are not being cheated out of their share. Thus, I believe that RODRIGUEZ is part of the same crew that participated in both the RAKBank and Bank of Muscat unlimited operations. The compromised account number used by RODRIGUEZ's three coconspirators during the Bank of Muscat unlimited operation resulted in approximately 2,904 successful ATM withdrawals in the immediate vicinity of New York with a total loss of approximately \$2.4 million. Globally, this compromised Bank of Muscat account number was used to conduct approximately 11,778 fraudulent withdrawals for a total loss of approximately \$8.9 million. Coconspirator communications obtained by the USSS indicate that the withdrawal limit for this particular compromised Bank of Muscat account had been increased to \$40 million as a result of the network intrusion.

12. In addition to the bank records, surveillance images and other evidence described above, in the course of

investigating this access device fraud conspiracy, the government also executed multiple search warrants for email accounts associated with the subjects of this investigation. On March 4, 2013, United States Magistrate Judge James Orenstein authorized the issuance of a search warrant for the email accounts "marcostaveraz@yahoo.com" (the "Marcos Account") and "joeironjoe@yahoo.com" (the "IronJoe Account") based upon evidence indicating that the owner of these email accounts (Coconspirator #1, or "CC #1") used them in furtherance of access device fraud conspiracy, including the above-described unlimited operations. Multiple email messages found in the Marcos and IronJoe Accounts discussed various types of financial account fraud and computer intrusions involving RODRIGUEZ:

- On or about October 24, 2012, CC #1 sent an email from the Marcos Account to RODRIGUEZ at "elvis_rr26@hotmail.com" (the "Elvis Account"), which is the email address provided by RODRIGUEZ in his December 5, 2012 U.S. passport application. This email included information for 10 compromised accounts with the BIN 465859, including the PINs for the accounts. Based on my training and experience investigating unlimited operations and similar "carding" activities, I believe that CC #1 was providing RODRIGUEZ with this compromised account data so that RODRIGUEZ or his associates use the stolen card numbers to conduct fraudulent transactions.
- On or about November 2, 2012, CC #1 sent an email from the Marcos Account to RODRIGUEZ at the Elvis Account including approximately 23 unique compromised accounts and PINs.

- On or about November 5, 2012, an email message was sent from the account "noreply@sprint.com" to the Marcos Account verifying a previously placed order with Sprint for two mobile devices. This Sprint confirmation email indicates that the mobile devices were shipped to "ELVIS RODRIGUEZ" at 153 Mansion Avenue, Yonkers, New York 10704. RODRIGUEZ's December 5, 2012 U.S. passport address lists this address as his primary residence. The government has learned that these two mobile devices were fraudulently purchased using a compromised Sprint business account belonging to a company in Connecticut.
- On or about December 28, 2012, CC #1 sent an email from the IronJoe Account to "support@wmirk.ru" with the following details in the body of the message:

Sender: Elvis Rodriguez
City: New York
State: New York
Country: USA
Receiver: Roman ivanovich kruchinin
MTCN: 895-862-8712
Amount: 950
LR Account: U7093888

Based on my experience in this and other carding investigations, I am aware that the email address "support@wmirk.ru" is associated with an organization based in St. Petersburg, Russia that specializes in laundering the proceeds of criminal activity. As a result, I believe that this email indicates that RODRIGUEZ ("Sender") sent a wire transfer via Western Union ("MTCN" refers to "Money Transfer Control Number," a numeric wire transfer identification system used by Western Union) to fund an account at Liberty Reserve ("LR"), an electronic currency service frequently used to transfer criminal proceeds in carding activities.

- On or about January 8, 2013, an email message was forwarded from the email account "dkrifrad@msn.com" (the "Dkrifrad Account") with the subject line "FW: E.

RODRIGUEZ 01/09/13 Itinerary" to the IronJoe Account, forwarding an email originally sent from "americanairlines@aa.com" to RODRIGUEZ at the Elvis Account. The American Airlines message included an itinerary for round-trip travel for RODRIGUEZ and two other individuals from John F. Kennedy International Airport to Bucharest, Romania from January 9, 2013 to January 11, 2013. "ELVIS RODRIGUEZ" was included among the individuals traveling on the reservation. Email and chat conversations discovered on the computer of an individual arrested by USSS on access device fraud charges in February 2013 indicate that RODRIGUEZ and the two others listed on the flight itinerary traveled to Romania in order to pay approximately \$300,000 in US currency to the organizers of the RAKBank unlimited operation. According to American Airlines, their original reservation was cancelled because the airline was concerned that a stolen credit card had been used to book the flight. Consequently, the reservation was rebooked on the day of the travel and RODRIGUEZ paid for the tickets in cash at the American Airlines reservations desk at JFK Airport.

WHEREFORE, your affiant respectfully requests that an arrest warrant be issued for ELVIS RAFAEL RODRIGUEZ, also known as "elvis_rr26@hotmail.com," so that he may be dealt with according to law.

Furthermore, in light of the defendant ELVIS RAFAEL RODRIGUEZ's sophistication with computers and the Internet, your affiant respectfully requests that this affidavit, arrest warrant and any other papers submitted in support of this application be sealed until further order of the Court so as to prevent notifying the defendant of the pending warrant, which could result in his destruction of evidence and/or alteration of travel plans to avoid arrest.

C.A.W.
CHRISTIAN A. WILSON
Special Agent
United States Secret Service

Sworn to before me this
26th day of March 2013

THE HONORABLE MARILYN D. GO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK