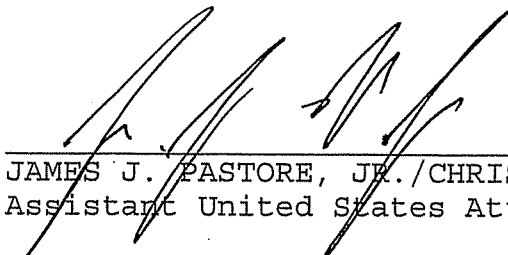


Approved:


JAMES J. PASTORE, JR./CHRISTINE I. MAGDO
Assistant United States Attorneys

Before:

THE HONORABLE HENRY B. PITMAN
United States Magistrate Judge
Southern District of New York

12 MAG 799

----- x
UNITED STATES OF AMERICA

:
: SEALED COMPLAINT

- v -

:
: Violations of
: 18 U.S.C.

RANA KHANDAKAR,
a/k/a "Rick Shinwat," and
USAWAN SAELIM,

:
: §§ 1028A, 1029 and 2

Defendants.

:
: COUNTY OF OFFENSE:
: NEW YORK

----- x
SOUTHERN DISTRICT OF NEW YORK, ss.:

TIMOTHY G. DESROCHERS, being sworn, deposes and says that he is a Special Agent of the United States Secret Service (the "Secret Service") and charges as follows:

COUNT ONE

(Conspiracy to Commit Access Device Fraud)

1. From at least in or about November 2008, up to and including on or about March 26, 2012, in the Southern District of New York and elsewhere, RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, and others known and unknown, willfully and knowingly did combine, conspire, confederate and agree together and with each other to commit offenses under Title 18, United States Code, Section 1029(a).

2. It was a part and object of the conspiracy that RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, and others known and unknown, knowingly, and with intent to defraud, would and did effect transactions with one and more access devices issued to another person or persons, and would and did receive payment and things of value during a 1-year period the aggregate value of which was equal to and greater than \$1,000, in violation of Title 18, United States Code, Section 1029(a) (5).

3. It was a further part and an object of the conspiracy that RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, knowingly, and with intent to defraud, would and did possess fifteen and more devices which were counterfeit and unauthorized access devices, in violation of Title 18, United States Code, Section 1029(a)(3).

Overt Acts

4. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. In or about November 2008, RANA KHANDAKAR, a/k/a "Rick Shinwat," the defendant, established a fraudulent merchant account in the name of a business known as "Tips."

b. In or about late 2010, RANA KHANDAKAR, a/k/a "Rick Shinwat," the defendant, established a fraudulent merchant account in the name of a business known as "uDiapers Inc."

c. In or about June 2010, USAWAN SAELIM, the defendant, established a bank account that was used to receive the proceeds of fraudulent credit/debit card charges made through uDiapers Inc., and to incur charges made through certain fraudulent merchant accounts.

d. Throughout 2011 and 2012, the defendants caused fraudulent credit/debit card transactions to be processed by a computer server located in New York, New York.

e. In or about 2012, RANA KHANDAKAR, a/k/a "Rick Shinwat," the defendant, caused to be mailed materials related to an EZ Pass account to an address in New York, New York.

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

COUNT TWO

(Aggravated Identity Theft)

5. From at least in or about November 2008 up to and including on or about March 26, 2012, in the Southern District of New York and elsewhere, RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, during and in relation to a felony violation

enumerated in Title 18, United States Code, Section 1028(A)(c), to wit, KHANDAKAR and SAELIM used the names, social security numbers, credit/debit card account numbers, and other personal identification information of other persons to establish fraudulent merchant accounts, and to make fraudulent credit card charges as part of the access device fraud conspiracy charged in Count One of this Complaint.

(Title 18, United States Code, Sections 1028A and 2).

The bases for my knowledge and the foregoing charges are, in part, as follows:

6. I have been a Special Agent with the United States Secret Service since 2009. I am currently assigned to the Electronic Crimes Task Force, a squad that investigates online crimes, including identity theft, intellectual property theft, and Internet-based frauds. I have received training regarding computer technology, intellectual property offenses, and how the Internet can be used to commit and facilitate various frauds. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

Overview Of The Fraudulent Scheme

7. Since at least December 2011, the Secret Service, the Metropolitan Transportation Authority's Office of the Inspector General, the New York State Police, and the Port Authority of New York and New Jersey Office of the Inspector General, among other agencies, have been investigating a large-scale and sophisticated fraud scheme involving fraudulent charges made on credit and debit card accounts. Hundreds of those accounts were stolen, and then used to incur fraudulent charges.

Hundreds more were charged by an online merchant for goods that the merchant failed to deliver. Still other accounts were fraudulently opened using the personal identification information of others, and then used to incur charges.

8. Based on interviews, my review of bank records and other documents, emails obtained pursuant to search warrants, and physical surveillance, I believe that, since at least 2008, RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, have engaged in a scheme to commit, and attempt to commit, fraud in excess of \$6,000,000. As part of their scheme, the defendants used a variety of Internet-based methods to make more than \$6,000,000 worth of charges on 1,400 credit and debit

card accounts. The defendants obtained at least \$4,000,000 worth of goods, services, and cash through the scheme, including items ranging from luxury goods - for instance, a Mercedes-Benz automobile - to personal items such as pet insurance, and even daily expenses such as food, often using other individuals' credit and debit card accounts to order takeout meals delivered three times a day.

9. As detailed below, there were several ways in which RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, executed the fraudulent scheme. First, the defendants used stolen American Express credit card numbers to fraudulently purchase EZ Pass tags and credits. The defendants then re-sold the EZ Pass tags and credits - often at a discount - through two websites: one that is located online at www.drezpass.com (the "Dr. EZ Pass Website"), and the other that is located online at www.ezpasstag.com (the "EZ Pass Tag Website" and, collectively, the "Websites"). Neither of the Websites is an authorized EZ Pass retailer. The investigation has identified at least 900 EZ Pass accounts that appear to have been involved in the fraud, and which have incurred more than \$100,000 worth of charges since July 2011. At least 50 stolen American Express credit card accounts were charged in connection with this part of the defendants' fraudulent scheme.

10. Second, RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, established several merchant accounts that were used to make fraudulent charges, and the proceeds from those fraudulent charges were deposited into bank accounts controlled by the defendants. Typically, the charges were made on stolen credit/debit card accounts. With respect to at least one merchant account - uDiapers Inc. - the defendants established a website that purported to sell childcare related products. Using credit and debit card accounts, customers ordered merchandise through the uDiapers website, which the defendants failed to deliver as promised. Rather than fulfilling the orders, the defendants instead simply pocketed the proceeds from the charges. The fraudulent merchant accounts were used to attempt more than \$3,000,000 worth of charges on at least 385 stolen American Express credit card accounts. In addition, the fraudulent merchant accounts were used to attempt more than \$2,000,000 worth of charges on more than 1,000 credit/debit card accounts from Citibank, JP Morgan Chase, Bank of America, and Discover, among others. Some of the same credit card accounts that incurred charges through the fraudulent merchant accounts also were used to fraudulently purchase EZ Pass tags and credits that were then re-sold through the Websites.

11. These are only some of the ways in which RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the

defendants, obtained money, goods, and services through fraud. The investigation has revealed that the defendants also have (i) used stolen credit/debit card accounts to purchase electronics and other expensive merchandise that they shipped to themselves; (ii) counterfeited checks; (iii) opened bank accounts and obtained credit/debit cards using other individuals' personal identification information; and (iv) fraudulently placed credits on gift cards which they then used to purchase merchandise.

The EZ Pass Fraud

12. Based on the investigation, I believe that RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, operated two Websites that purported to be authorized sellers of EZ Pass tags and credits. In truth and in fact, when a customer ordered an EZ Pass tag through one of the Websites, the defendants would fulfill that order by purchasing an EZ Pass tag with stolen credit card numbers. In this way, the defendants essentially obtained the EZ Pass tag for free, and then profited by re-selling that tag.

Background Regarding EZ Pass

13. From speaking with employees of the Metropolitan Transportation Authority ("MTA"), I have learned, in substance and among other things:

a. EZ Pass is an electronic system that allows drivers to automatically pay tolls at various bridges, tunnels, and/or turnpikes that accept EZ Pass. In order to use the EZ Pass system, a customer must obtain an EZ Pass physical device or "tag," which uses Radio Frequency Identification ("RFID") technology to wirelessly communicate with toll locations.

b. Each tag is associated with a particular EZ Pass account. The EZ Pass tag can either be pre-loaded with a certain amount credited to an EZ Pass account, or can be linked to a payment method, such as a credit card, that allows EZ Pass customers to have their account charged for the usage of the tag. Credits may also be purchased to refill an EZ Pass tag.

c. Pre-loaded EZ Pass tags are available for sale through several authorized, independent merchants. EZ Pass tags also can be purchased from municipal entities, such as the MTA, the Port Authority of New York and New Jersey, and the New York State Thruway Authority, among others.

d. When an EZ Pass account is created, the customer is prompted to supply certain information, some of which is mandatory and some of which is optional. Among other things,

a customer can provide EZ Pass with an email account, so that EZ Pass can communicate by email with the customer.

The Undercover Purchase From Dr. EZ Pass

14. On or about January 12, 2012, I purchased a \$100 EZ Pass tag through the Dr. EZ Pass Website using an undercover identity. I provided to the Dr. EZ Pass Website a name, address, and PayPal account, and the make, model and license plate number of a vehicle. I did not provide any credit or debit card account information to the Dr. EZ Pass Website. The undercover PayPal account was charged \$100 by Dr. EZ Pass, purportedly for the EZ Pass tag.

15. Records obtained from the MTA revealed that, after I provided the undercover personal and vehicle information to the Dr. EZ Pass Website, an actual EZ Pass account was opened at www.e-zpassny.com (an authorized EZ Pass website) using the information I had provided. However, that EZ Pass account was linked to two, stolen American Express card numbers. I did not provide those, or any other, credit card numbers to the Dr. EZ Pass Website.

16. I learned from American Express that the two stolen American Express card accounts incurred charges for the EZ Pass tag associated with the undercover EZ Pass account. (The charges were credited back to the victims.)

17. After placing my order, an EZ Pass tag was sent through the U.S. mail from a processing center in Staten Island, New York, to an address located in New York, New York. I also received a second mailing at the New York, New York address, with a return address of 694 Myrtle Avenue, in Brooklyn, New York (the "Myrtle Avenue Address")¹ and a return addressee of "Dr. EZ Pass." This second mailing from "Dr. EZ Pass" contained documents that included, among other information, a username and password to log into the legitimate EZ Pass website located at www.e-zpassny.com. Documents provided by "Dr. EZ Pass" instructed me that I was not to change the username or password for the account on www.e-zpassny.com. Based on my training and experience, and my familiarity with this investigation, I believe

¹ As discussed in more detail below, the Myrtle Avenue Address is in fact a stationery store that offers, among other services, mailbox rentals. The Myrtle Avenue Address is a mailbox rented in the name of RANA KHANDAKAR, the defendant, and appears to be used by KHANDAKAR and USAWAN SAELIM, the defendants, as an address to which they ship merchandise purchased with stolen credit/debit card accounts.

that "Dr. EZ Pass" told me not to change the log-in information so that "Dr. EZ Pass" could continue to have access to my EZ Pass account through www.e-zpassny.com.

18. Based on the undercover purchase and the records I have reviewed, I believe that, after I provided the personal and vehicle information through the Dr. EZ Pass Website, that information was used to establish an EZ Pass account through www.e-zpassny.com, and to order a \$100 EZ Pass tag. Although "Dr. EZ Pass" charged my undercover PayPal account \$100 for this transaction, that money was not actually used to buy the EZ Pass. Instead, "Dr. EZ Pass" used stolen credit cards to purchase the EZ Pass tag, and then pocketed the \$100 from my PayPal account. In other words, "Dr. EZ Pass" obtained the EZ Pass tag essentially for free by using stolen credit cards, and then "sold" it to me for \$100 through the Dr. EZ Pass Website. In this way, the Dr. EZ Pass Website functions like a high-tech "fence" for stolen goods: here, EZ Pass tags obtained through fraudulent credit-card charges.

Other Fraudulent EZ Pass Accounts

19. From speaking with employees of the MTA, and from reviewing records provided by the MTA, I have learned, in substance and among other things:

a. The MTA has identified at least 900 EZ Pass accounts that appear to have been fraudulently established, much in the same way that the undercover account described above was established. That is, the EZ Pass accounts were paid for using stolen credit cards (the "Fraudulent EZ Pass Accounts").

b. Each of the Fraudulent EZ Pass Accounts was established online, and credit card charges associated with each of the Fraudulent EZ Pass Accounts were processed by computer servers located in Tarrytown, New York. The first of the Fraudulent EZ Pass Accounts was established in or about July 2011 in the name of "Rick Shinwat."

c. The Fraudulent EZ Pass Accounts shared several common attributes. Among other things, the Fraudulent EZ Pass Accounts were associated with one or more of several email addresses believed to be controlled by the defendants: drezpass@gmail.com, life0311@gmail.com, life0312@gmail.com, ezpasstag@gmail.com, and/or support@ezpasstag.com (the "Enabling Email Accounts"). As discussed in more detail below, during this investigation, the Government obtained search warrants for the contents of the Enabling Email Accounts.

d. Neither of the Websites is an authorized EZ

Pass retailer.

e. Some of the physical EZ Pass tags associated with the Fraudulent EZ Pass Accounts were mailed from a processing location in Staten Island, New York to, among other locations, addresses in New York, New York; New Jersey; Maryland, Pennsylvania; and North and South Carolina.

20. From speaking with an employee of American Express, I have learned, in substance and among other things, that at least 50 stolen American Express credit card accounts (the "Stolen AMEX Accounts") were linked to all 900 of the Fraudulent EZ Pass Accounts. In other words, the same 50 cards were used to incur charges associated with all of the hundreds of Fraudulent EZ Pass Accounts.

21. For several reasons, I believe that the EZ Pass Tag Website was part of the same criminal conspiracy that established and used the Dr. EZ Pass Website. Among other things, hosting fees for both of the Websites were paid using the same compromised JP Morgan Chase credit/debit card number. In addition, the same Internet Protocol ("IP") address² that was used to renew the hosting services for the Dr. EZ Pass Website also was used to establish hosting services for the EZ Pass Tag Website (as noted below, at times relevant to this Complaint, the IP address was assigned to an account in the name of USAWAN SAELIM, the defendant (the "SAELIM INTERNET ACCOUNT")). Finally, several of the Stolen AMEX Accounts that were used to purchase EZ Pass tags and/or credits on the Dr. EZ Pass Website also were used to purchase EZ Pass tags and/or credits on the EZ Pass Tag Website.

The Defendants' Links To The Fraudulent EZ Pass Accounts

22. Some of the documents that I received from "Dr. EZ Pass" in connection with the undercover operation were submitted to the Forensic Services Division of the Secret Service to test them for fingerprints. From reviewing a report regarding the forensic tests, I have learned, in substance and among other things, that the fingerprints on some of the "Dr. EZ Pass" documents were compared with fingerprints taken of RANA KHANDAKAR, a/k/a "Rick Shinwat," the defendant, when he was

² An IP address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0 to 255, separated by periods. 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 directed properly from its source to its destination.

arrested by the New York City Police Department and charged with torturing or injuring animals in violation of New York Agriculture and Markets Law Section 353, a class A misdemeanor. The two sets of fingerprints matched. That is, KHANDAKAR's fingerprints were on some of the documents sent to me from "Dr. EZ Pass."

23. The Dr. EZ Pass Website also has been linked to RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, through IP addresses. Specifically, on or about October 3, 2011, the domain name www.dreypass.com was purchased by an individual using an IP address ending in 171.62 (the "171.62 IP Address"). The person who purchased www.dreypass.com provided a contact email address of rickshinwat@gmail.com (the "SHINWAT EMAIL ACCOUNT").

24. During this investigation, the Government obtained a search warrant and subpoenaed records regarding the SHINWAT EMAIL ACCOUNT. From reviewing those records, I have learned, in substance and among other things, that at various times relevant to this Complaint, including in or about December 2011, the SHINWAT EMAIL ACCOUNT was accessed from the 171.62 IP Address, the same IP Address used to purchase www.dreypass.com.

25. I have also reviewed subscriber records for the 171.62 IP Address. Those records reveal, in substance and among other things, that from in or about October 2009 through in or about January 2012, the 171.62 IP Address was assigned to an account subscribed to USAWAN SAELIM, the defendant. Currently, the account is subscribed in SAELIM's name and lists as her address a particular apartment on Lafayette Avenue in Brooklyn, New York (the "Lafayette Avenue Apartment"). Physical surveillance has confirmed that SAELIM is currently residing at the Lafayette Avenue Apartment.

26. I reviewed a copy of the lease for the Lafayette Avenue Apartment, and the lease indicated that the Lafayette Avenue Apartment was rented to "Rana Khandakar" since at least in or about 2011. Physical surveillance conducted by the Secret Service also has confirmed that RANA KHANDAKAR, a/k/a "Rick Shinwat," the defendant, is currently residing in the Lafayette Avenue Apartment with SAELIM.

27. Another IP Address that ended in 211.222 (the "211.222" IP Address) was used to log into the life0312@gmail.com account during December 2011, which, as noted above, was used as the contact email for some of the Fraudulent EZ Pass Accounts. Pursuant to a subpoena issued to the Internet Service Provider that administers the 211.222 IP Address, I have learned, in substance and among other things, that the 211.222 IP Address

was, at the time of the log-ins to the life0312@gmail.com account, assigned to an account subscribed in the name of a particular individual ("Nunez") at the Lafayette Avenue Apartment.

28. Pursuant to a search warrant on the life0312@gmail.com account, I have learned, in substance and among other things, that the account contains emails addressed to Nunez. The account also contains emails addressed to RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants. For instance, one of the emails was a communication from SAELIM's car insurance company enclosing an insurance card in her name for a Mercedes-Benz that is registered in her name. Another email consists of a communication from the New York State Department of Motor Vehicles and contains a receipt for a \$425 payment from "Rana Khandakar." From these emails, I have concluded that both RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, are using an email account at which they receive not only personal emails directed to them, but also emails directed to Nunez - an identity they appear to have taken over.

29. That the defendants have assumed the Nunez identity is further confirmed from my review of a check that RANA KHANDAKAR, a/k/a "Rick Shinwat," the defendant, used to pay the first and last months' rent and the security deposit for the Lafayette Avenue Apartment. The check purports to be from an account in the name of "Shrimp Boat JohnPaul." In fact, however, the bank account was in Nunez's name, and not in the name "Shrimp Boat JohnPaul." Accordingly, it appears that KHANDAKAR used a counterfeited check to pay rent and a security deposit for the apartment where he and USAWAN SAELIM, the defendant, are living, and that the check was drawn on a bank account in Nunez's name.

The Merchant Account Fraud

30. The investigation has further shown that RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, also established merchant accounts that were then used to incur fraudulent charges on credit and/or debit card accounts. Some of the charges were made on stolen credit/debit card accounts. Other charges were made to credit/debit card accounts of people who purchased - but never received - goods from one of the defendants' businesses.

Background Regarding Merchant Accounts

31. By way of background, from my training and experience, I know that, in order to process credit and/or debit card transactions, a business entity (known as a "merchant") must

first establish an account with a credit/debit-card processor (known as a "merchant processor"). Typically, in order to establish an account with a merchant processor (known as a "merchant account"), a business is required to provide information such as the business's name, bank account information, physical address, and other contact information including a phone number and/or email address. In addition, an individual must sign as the party responsible for the merchant account and provide identification, including, for instance, his or her Social Security number, and contact information.

32. Each merchant account is linked to one or more bank accounts provided by the merchant so that, when a credit or debit card transaction is processed, a deposit ultimately is made to the bank account(s) of the merchant.

33. Typically, there are two main ways in which merchants can process credit/debit card transactions. First, the merchant may receive a physical piece of equipment (known as a "terminal") that can be used to charge a card by swiping it through the terminal or keying the card information into the terminal, such as when a credit card is used to pay for goods at a cash register.

34. The other way that a merchant typically can process credit/debit card transactions is through the Internet, with the customer providing the requisite account information through the merchant's website.

The Fraudulent Merchant Accounts

35. One of the online merchants used in connection with the fraud was named uDiapers Inc. ("uDiapers"), which maintained a website at www.udiapers.com. (The site has since ceased operating.)³ From reviewing records provided by a merchant processor, I have learned, in substance and among other things:

a. The application for the merchant account for uDiapers lists RANA KHANDAKAR, the defendant, as the owner of uDiapers.

b. The application also lists a routing number and bank account number where proceeds from credit/debit card

³ It appears that, at least for a time, the website may have in fact sold childcare related items. However, I have reviewed numerous online complaints about uDiapers in which customers complain that they ordered items through uDiapers, were charged for that merchandise, and then never received it.

transactions were to be deposited. As explained in more detail below, bank records revealed that the account is in the name of USAWAN SAELIM, the defendant (the "SAELIM BANK ACCOUNT").

c. What purports to be a tax return was submitted in connection with the application for the uDiapers merchant account. The tax return is in the name of RANA KHANDAKAR, the defendant, and is signed by KHANDAKAR. I have compared the signature on this tax return with the signature that appears on KHANDAKAR's New York State driver's license and have determined that the signatures appear to be made by one and the same person.

d. KHANDAKAR's application for a uDiapers merchant account ultimately was approved, and an account was opened in or about late 2010.

e. The uDiapers merchant account ultimately was closed due to a high volume of reversed charges, or "chargebacks." Some of the fraudulent charges were incurred on credit/debit card accounts from Citibank, and Citibank has confirmed that it received complaints from several victim accountholders that those accountholders did not authorize charges to be made through uDiapers.

f. In fact, during one 30-day period, tens of thousands of dollars were charged through uDiapers, and the proceeds of those transactions were deposited (or were attempted to be deposited) into the SAELIM BANK ACCOUNT that was linked to the uDiapers merchant account.

36. Documents relating to the SAELIM BANK ACCOUNT were subpoenaed, and, from reviewing those documents, I have learned, in substance and among other things:

a. USAWAN SAELIM, the defendant, opened the SAELIM BANK ACCOUNT in or about June 2010 using a New Jersey driver's license. The account was closed due to fraud in or about September 2011.

b. While the SAELIM BANK ACCOUNT was open, more than ten thousand dollars was deposited into the bank account from the merchant processor administering the uDiapers account.

c. In addition, the SAELIM BANK ACCOUNT incurred small charges from other fraudulent merchant accounts identified during the investigation, including, among others, merchants known as Café 007 and La Pala Pa. These charges were under \$5.00 each. From my training and experience, I know that criminals engaging in credit/debit card fraud often will make small charges

on merchant accounts that they have opened, in order to determine whether the merchant accounts are in fact capable of processing transactions. Accordingly, here, it appears that the SAELIM BANK ACCOUNT was used to test whether certain merchant accounts were in fact able to process transactions. As discussed in more detail below, certain of those merchant accounts have been linked to the defendants.

d. The SAELIM BANK ACCOUNT also was used to pay SAELIM's personal expenses. For example, the SAELIM BANK ACCOUNT was used to make several payments to an Internet Service Provider for the SAELIM INTERNET ACCOUNT.

e. In addition, the SAELIM BANK ACCOUNT was used to make rental payments for a storage unit located in Long Island City, New York. From reviewing a copy of the rental agreement, I have learned, in substance and among other things, that the agreement is in SAELIM's name. In addition, the lease lists "Rana Khandakar" as an "authorized access person."

f. The SAELIM BANK ACCOUNT also was used to make monthly car payments for a Mercedes-Benz that is currently registered in SAELIM's name ("SAELIM'S MERCEDES-BENZ.") (At the time that the payments was made, the car was in the name of SAELIM'S mother; the car ultimately was transferred to USAWAN SAELIM, the defendant.)

37. RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, are also associated with several other merchant accounts that were used to make bogus charges on stolen credit/debit card accounts, including accounts at American Express, Citibank, JP Morgan Chase, and Bank of America, among others.

38. For instance, from reviewing documents provided by a merchant processor, I have learned, in substance and among other things:

a. On or about November 25, 2008, an application was submitted for a merchant account for a business known as "Tips." The individual listed as the owner of the business was "Rana Khandakar."

b. On or about January 8, 2009, the Tips merchant account was closed due to fraud. Specifically, a high number of the charges made through the merchant were reversed.

39. From speaking with an employee of American Express and reviewing records from American Express as well as the MTA, I have learned, in substance and among other things, that several

of the Stolen AMEX Accounts that were used to fraudulently purchase EZ Pass tags and credits as part of the EZ Pass fraud described above, also incurred fraudulent charges at Tips. For example, an American Express card ending in 1007 and another ending in 1012 were each associated with EZ Pass accounts connected to the Dr. EZ Pass Website; each of those cards also incurred charges through Tips. From speaking with an employee of American Express, I know that the accountholders for the 1007 and 1012 cards each contacted American Express regarding fraudulent charges on their accounts.

40. RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, also are linked to a fraudulent merchant account for a business known as "La Pala Pa." As noted above, the SAELIM BANK ACCOUNT was used to test whether the La Pala Pa merchant account could process credit/debit card transactions. From reviewing records subpoenaed from a merchant processor, I have learned, in substance and among other things:

a. On or about January 5, 2011, an application for a merchant account for "La Pala Pa" was submitted to the merchant processor. The owner of La Pala Pa was listed as a particular individual ("Cardova"), and also contained a Social Security number for Cardova.

b. Although the business purported to be owned by Cardova, the merchant account was linked to a bank account that was in the name of "Rana Khandakar" (the "KHANDAKAR BANK ACCOUNT"). From reviewing documents provided by the bank regarding the KHANDAKAR BANK ACCOUNT, I have learned, in substance and among other things, that the KHANDAKAR BANK ACCOUNT was not only in the name of RANA KHANDAKAR, a/k/a "Rick Shinwat," the defendant, but also purported to be an account for "Tips." In other words, the KHANDAKAR BANK ACCOUNT is linked to KHANDAKAR both because it is in his name, and because it purports to be a bank account for the fraudulent merchant Tips, which business was owned by KHANDAKAR.

c. The application for the La Pala Pa merchant account ultimately was approved; however, the account was closed due to fraud on or about February 7, 2011 (i.e., about a month after the application was submitted).

41. Another fraudulent merchant account linked to RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, was for a business known as "Café 007." As noted above, the SAELIM BANK ACCOUNT was used to test whether the Café 007 merchant account could process credit/debit card transactions. From reviewing records subpoenaed from a merchant processor, I have learned, in substance and among other things:

a. An application was submitted for a merchant account for Café 007 on or about March 4, 2011. The application listed an individual ("Miko") as the owner of Café 007. The application was accompanied by a Social Security card and driver's license for Miko. Although the application indicated that Café 007 was owned by Miko, the merchant account was linked to a bank account in the name of Nunez. The Café 007 merchant account ultimately was closed due to fraud.

b. From the investigation, it appears that RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, have taken over the identities of Miko and Nunez. Specifically, from reviewing the results of a search warrant executed on certain of the Enabling Email Accounts (i.e., the email accounts provided as the contact emails for the Fraudulent EZ Pass Accounts), I have learned, in substance and among other things, that those email accounts contain several emails addressed to Miko and to Nunez.

c. From reviewing records provided to me by American Express and by the MTA, I have learned, in substance and among other things, that several of the Stolen AMEX Accounts incurred charges at Tips, La Pala Pa, and Café 007. In other words, some of the same credit cards that incurred charges in connection with the Fraudulent EZ Pass Accounts were also used to fraudulently obtain money through merchant accounts that are linked to RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, as set forth above. Accordingly, I believe that the defendants used not only the EZ Pass Websites, but also the fraudulent merchant accounts to commit fraud.

42. In total, at least 1,400 credit/debit card accounts have been linked to fraudulent merchant accounts believed to be operated by RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, including the EZ Pass Websites. Those compromised accounts were used to attempt at least \$6,000,000 in charges, and at least \$4,000,000 of those charges were in fact processed.

The Myrtle Avenue Address & Results Of Physical Surveillance

43. During this investigation, I, along with other Secret Service Agents, have, on several occasions, conducted physical surveillance of RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants. During the surveillance, I have observed KHANDAKAR and SAELIM traveling in SAELIM'S MERCEDES-BENZ. Among other places, KHANDAKAR and SAELIM drove to the Myrtle Avenue Address to pick up packages that had been delivered there.

44. From speaking with another Secret Service agent who participated in the surveillance, I have learned, in substance and among other things:

a. Some of the packages delivered to the Myrtle Avenue Address were in plain view because they were too large to fit into the mailbox rented by KHANDAKAR.

b. Certain of those packages were addressed to individuals other than the defendants. During surveillance, however, KHANDAKAR was observed picking up those packages.

45. I believe that the packages shipped to the Myrtle Avenue Address are goods that were fraudulently purchased using stolen credit/debit card accounts. As noted above, the Government obtained a search warrant for certain of the Enabling Email Accounts. From reviewing the emails in certain of those accounts, I know that they contain, among other things, receipts from various merchants, indicating that goods were being delivered to the Myrtle Avenue Address. Among other merchandise shipped to the Myrtle Avenue Address were materials that, based on my training and experience, can be used to create counterfeit credit cards and/or false identification documents. Those items included specialized printers, RFID chips and reader/writers, and magnetic strip readers.

46. In addition, during surveillance, I observed USAWAN SAELIM, the defendant, enter a drugstore. I watched SAELIM attempt to purchase an item using at least four separate credit cards, each of which was declined by the cashier. Eventually, SAELIM left the drugstore without completing the purchase. Based on my training and experience, SAELIM's attempt to purchase an item using four separate credit cards that were all declined is consistent with behavior associated with credit/debit card fraud. That is because although fraudsters may initially succeed in processing fraudulent charges using compromised accounts, once the fraud is reported to the credit/debit card issuer, the account often is closed, and no further charges can be processed using the account.

47. The investigation also has revealed that several of the Stolen AMEX Accounts were also fraudulently charged for meals that were delivered to the Lafayette Avenue Apartment where RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, currently live.

48. From speaking with a Special Agent of the Social Security Administration, I have learned, in substance and among other things, that, at all times relevant to this Complaint, the Social Security Administration has no record of earnings or

employment for either RANA KHANDAKAR, a/k/a "Rick Shinwat," or USAWAN SAELIM, the defendants, other than one instance in which they reported \$5,000 from self-employment. Based on this information, as well as my surveillance of the defendants, my review of bank records and other documents obtained during the investigation, and my training and experience, it appears that the defendants have no legitimate sources of income.

WHEREFORE, deponent prays that warrants be issued for the arrest of RANA KHANDAKAR, a/k/a "Rick Shinwat," and USAWAN SAELIM, the defendants, and that they be imprisoned or bailed, as the case may be.



TIMOTHY G. DESROCHERS
Special Agent
United States Secret Service

Sworn to before me this
26th day of March, 2012



THE HONORABLE HENRY B. PITMAN
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK