

that LOUIS ABAD, MATHEWS ANGEL, PRINCETTA DORISMA, LESLY ESQUEA, FRANCIS LOPEZ, LUIS ORRIOLS, PEDRO RODRIGUEZ, JOHNNY SANTANA, and JACKLIN VOLNY, a/k/a "Jeff Volny," the defendants, and others known and unknown, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, to wit, ABAD, ANGEL, DORISMA, ESQUEA, LOPEZ, ORRIOLS, RODRIGUEZ, SANTANA, and VOLNY, and others known and unknown used a telephone service provider's national intranet networks to obtain unique cellular telephone identifiers assigned to cellular telephones of the service provider's customers without authorization of the customers or the service provider, which identifiers were then used to make over \$15 million in unauthorized cellular telephone calls, in violation of Title 18, United States Code, Section 1343.

Overt Acts

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

a. On or about April 29, 2010, LOUIS ABAD, the defendant, accessed at least 16 cellular telephone service accounts and obtained unique identifiers assigned to the account holders' cellular telephones without the authorization or knowledge of the account holders.

b. On or about February 19, 2010, MATHEWS ANGEL, the defendant, accessed at least 21 cellular telephone service accounts and obtained unique identifiers assigned to the account holders' cellular telephones without the authorization or knowledge of the account holders.

c. On or about February 18, 2010, PRINCETTA DORISMA, the defendant, accessed at least 15 cellular telephone service accounts and obtained unique identifiers assigned to the account holders' cellular telephones without the authorization or knowledge of the account holders.

d. On or about April 7, 2010, LESLY ESQUEA, the defendant, accessed the cellular telephone service account of a resident of the Bronx, New York and obtained without the

authorization or knowledge of that account holder a unique identifier assigned to that account holder's cellular telephone.

e. On or about March 3, 2010, FRANCIS LÓPEZ, the defendant, accessed at least 19 cellular telephone service accounts and obtained unique identifiers assigned to the account holders' cellular telephones without the authorization or knowledge of the account holders.

f. On or about February 16, 2010, LUIS ORRIOLS, the defendant, accessed the cellular telephone service account of a resident of Mount Vernon, New York and obtained without the authorization or knowledge of that account holder a unique identifier assigned to that account holder's cellular telephone.

g. On or about March 11, 2010, PEDRO RODRIGUEZ, the defendant, accessed the cellular telephone service account of a resident of the Bronx, New York and obtained without the authorization or knowledge of the account holder a unique identifier assigned to that account holder's cellular telephone.

h. On or about February 22, 2010, JOHNNY SANTANA, the defendant, accessed at least 43 cellular telephone service accounts and obtained unique identifiers assigned to the account holders' cellular telephones without the authorization or knowledge of the account holders.

i. On or about May 8, 2010, JACKLIN VOLNY, a/k/a "Jeff Volny," the defendant, accessed the cellular telephone service account of a resident of the Bronx, New York and obtained without the authorization or knowledge of that account holder a unique identifier assigned to that account holder's cellular telephone.

(Title 18, United States Code, Section 1349.)

COUNT TWO

4. From at least in or about January 2010 through in or about June 2010, in the Southern District of New York and elsewhere, LUIS ABAD, MATHEWS ANGEL, PRINCETTA DORISMA, LESLY ESQUEA, FRANCIS LOPEZ, LUIS ORRIOLS, PEDRO RODRIGUEZ, JOHNNY SANTANA, and JACKLIN VOLNY, a/k/a "Jeff Volny," the defendants, unlawfully, willfully, knowingly and with intent to defraud, did possess fifteen or more devices which were counterfeit and unauthorized access devices, which conduct did affect interstate and foreign commerce, to wit, ABAD, ANGEL, DORISMA, ESQUEA, LOPEZ, ORRIOLS, RODRIGUEZ, SANTANA, and VOLNY possessed without

authorization fifteen and more unique cellular telephone identifiers of a cellular telephone service provider's customers.

(Title 18, United States Code, Section 1029(a)(3)).

COUNT THREE

5. From at least in or about January 2010 through in or about June 2010, in the Southern District of New York and elsewhere, LUIS ABAD, MATHEWS ANGEL, PRINCETTA DORISMA, LESLY ESQUEA, FRANCIS LOPEZ, LUIS ORRIOLS, PEDRO RODRIGUEZ, JOHNNY SANTANA, and JACKLIN VOLNY, a/k/a "Jeff Volny," the defendants, during and in relation to the conduct described in Counts One and Two of this Complaint, unlawfully, willfully, and knowingly did transfer, possess, and use, without lawful authority, a means of identification of another person, to wit, ABAD, ANGEL, DORISMA, ESQUEA, LOPEZ, ORRIOLS, RODRIGUEZ, SANTANA, and VOLNY did transfer, possess, and use the unique cellular telephone identifiers assigned to the cellular telephones of a cellular telephone service provider's customers without the authorization of the cellular telephone service provider or the customers.

(Title 18, United States Code, Section 1028A)

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

6. I am a Special Agent with the USSS, and I have been involved personally in the investigation of this matter. I have been a Special Agent with the USSS for approximately two years and have participated in numerous investigations of wire fraud and access device fraud. I am familiar with the facts and circumstances set forth below from my personal participation in the investigation, my examination of reports and records, and my conversations with other law enforcement officers investigating this matter. 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.

7. I have spoken to a technical representative ("Technical Representative-1") employed by a cellular telephone

service provider ("Provider-1"). From these conversations, I learned, among other things, that:

a. In order to provide its cellular telephone subscribers with the ability to place calls and access data, Provider-1 operates a network of cellular telephone towers (the "Provider-1 Network"). The Provider-1 Network recognizes cellular telephones and other mobile devices (collectively referred to herein as "cell phones") used by Provider-1's customers by two unique identifiers that are programmed into every cell phone that is given access to the Provider-1 Network: (i) a Mobile Station ID ("MSID") and (ii) an Electronic Serial Number ("ESN"). When a Provider-1 customer attempts to place a call using the Provider-1 Network, the cell phone tower receiving the signal from the particular cell phone identifies the MSID and ESN of the device sending the signal, and will only carry the call if the Provider-1 Network recognizes the MSID and ESN as belonging to a Provider-1 customer.

b. The MSID and ESN are unique identifiers associated with specific cell phones. Provider-1 tracks its customers' use of the Provider-1 Network by their assigned MSID and ESN numbers and then bills its customers based on their use of the Provider-1 Network. The MSID and ESN assigned to a particular cell phone can be changed by reprogramming the cell phone.

c. Cell phone cloning is a form of fraud that has been recognized by cell phone service providers since the infancy of the cell phone industry, and refers to the process by which an individual seeking to illegally place calls on a cellular telephone service provider's network steals or fraudulently obtains the necessary information to place calls on the network.

d. Cloning a cell phone used by one of Provider-1's customers by reprogramming another cell phone with the MSID and ESN of the Provider-1 customer's cell phone enables the user of the cell phone reprogrammed with the customer's MSID and ESN to make cell phone calls over the Provider-1 Network that appear to the Provider-1 Network to be made by the Provider-1 customer's cell phone.

8. I have spoken to a member of Provider-1's Corporate Security Department ("Corporate Security Employee-1"). From these conversations, I learned, among other things, that:

a. In the latter half of 2009, Provider-1 was contacted by several of its customers who stated that they were being billed for international calls that they did not make. Provider-1 employees confirmed that these calls were not made by these customers. Provider-1 employees learned, among other things, that many of the calls were made from hundreds of miles away from the states in which the customers resided and within minutes of calls made from within the state in which the Provider-1 customer resided, which would not be possible if only one cell phone was making the calls.

b. Provider-1 employees subsequently used Provider-1's computer networks to identify accounts of Provider-1 customers whose cell phones had been cloned. Provider-1 employees determined that MSIDs and/or MSNs assigned to tens of thousands of its customers had been used to make cell phone calls (the "suspect calls") that could not have been made from the customers' cell phones. These MSIDs and/or MSNs (a) had been used to make multiple calls simultaneously and/or (b) had been used to make calls from two different geographic locations within a short enough time period that it would not be physically possible to travel between those two locations during that time period. Provider-1 employees concluded that the phones belonging to these victims (the "Defrauded Customers") had been cloned and that the cloned phones had been used to make the suspect calls.

c. Provider-1 employees also found that many of the Defrauded Customers' accounts had been accessed using Provider-1's internet website and the Defrauded Customers' online account information had been changed. These changes included changing account passwords, adding calling features such as international calling, and adding entirely new cell phones (with new MSIDs and ESNs) to the Defrauded Customers' accounts. Provider-1's investigators have reviewed calling records for the cell phones assigned to the Defrauded Customers and discovered that unusually large volumes of international calls were being placed on the Provider-1 Network using MSIDs and ESNs assigned to the Defrauded Customers. Provider-1 employees and agents attempted to contact all of the Defrauded Customers and succeeded in speaking with nearly all of them. All, or nearly all, of the Defrauded Customers who spoke with Provider-1 employees or agents denied placing the suspect calls that the Provider-1 Network had identified as made from their cell phone.

d. LUIS ABAD, MATHEWS ANGEL, PRINCETTA DORISMA, LESLY ESQUEA, FRANCIS LOPEZ, LUIS ORRIOLS, PEDRO RODRIGUEZ, JOHNNY SANTANA, and JACKLIN VOLNY, a/k/a "Jeff Volny," the defendants, all were employees of Provider-1 from at least January 2010 through early June 2010. During this time period, RODRIGUEZ and SANTANA worked at Provider-1 stores located in the Bronx, New York; ABAD, ANGEL, LOPEZ, and ORRIOLS worked at a Provider-1 store located in North Bergen, New Jersey; and DORISMA, ESQUEA, and VOLNY worked at a Provider-1 store located in Tampa, Florida.

e. From January 2010 through early June 2010, ABAD, ANGEL, DORISMA, ESQUEA, LOPEZ, ORRIOLS, RODRIGUEZ, SANTANA, and VOLNY, the defendants, all had access to computer databases maintained by Provider-1, which they could access using unique identification codes provided to them by Provider-1. These codes are referred to, among other things as "System User IDs" or "ELIDs" (which is short for "Employee Login ID"). One of the programs used to access these databases is known as "E-Ticket." ABAD, ANGEL, DORISMA, ESQUEA, LOPEZ, ORRIOLS, RODRIGUEZ, SANTANA, and VOLNY could use these computer databases to obtain account information concerning customers of Provider-1, including the ESN and MSID numbers assigned to customers' cell phones. According to Provider-1 records, the unique identification codes assigned to ABAD, ANGEL, DORISMA, ESQUEA, LOPEZ, ORRIOLS, RODRIGUEZ, SANTANA, and VOLNY during this time period, include the following:

Provider-1 Employee	ID Code
LUIS ABAD	ut340673
MATHEWS ANGEL	ma154610
PRINCETTA DORISMA	pr301698
LESLY ESQUEA	lye9966
FRANCIS LOPEZ	fr247328
FRANCIS LOPEZ	fx13889
LUIS ORRIOLS	lu307373
PEDRO RODRIGUEZ	zp476473
JOHNNY SANTANA	jls6688
JACKLIN VOLNY	jjv0428

f. Corporate Security Employee-1 has reviewed electronic records of contact with Provider-1 customer accounts made using these unique identification codes assigned to ABAD, ANGEL, DORISMA, ESQUEA, LOPEZ, ORRIOLS, RODRIGUEZ, SANTANA, and VOLNY, the defendants. Among other things, Corporate Security Employee-1 learned that each of these unique identification codes were used to access many accounts of Defrauded Customers and that often within a few days suspect calls were made from cloned cell phones using the MSIDs and ESNs assigned to Defrauded Customers'

cell phones. Corporate Security Employee-1 also learned that the value of the unauthorized calls made over the Provider-1 Network using ESNs and MSIDs assigned to Defrauded Customers whose accounts were accessed using the unique identification codes assigned to ABAD, ANGEL, DORISMA, ESQUEA, LOPEZ, ORRIOLS, RODRIGUEZ, SANTANA, and VOLNY is \$15,417,064.45. Provider-1 has credited the Defrauded Customers for the value of these calls.

g. The unique identification codes of ABAD, ANGEL, DORISMA, ESQUEA, LOPEZ, ORRIOLS, RODRIGUEZ, SANTANA, and VOLNY, the defendants, also were used to access Provider-1 customer accounts in patterns that were inconsistent with servicing customers in their stores. For example, these codes were used rapidly over a short period of time to access accounts of Defrauded Customers with out-of-state billing addresses. It would be highly unusual for large groups of out-of-state customers to all enter a store at the same time and request account services from the same Provider-1 employee. Another example is that these codes were used to access accounts in an order corresponding to the numerical order of the phone numbers assigned to the accounts. It would be highly unusual for a group of Provider-1 customers with nearly identical phone numbers to all seek service at the same Provider-1 store from the same Provider-1 employee at the same time. Some data concerning these patterns of activity are set forth in paragraph 10 below.

h. On or about June 8, 2010 and June 9, 2010, members of Provider-1's Corporate Security Department spoke with ABAD, ANGEL, DORISMA, ESQUEA, LOPEZ, RODRIGUEZ, SANTANA, and VOLNY after these defendants agreed to speak with them. Members of Provider-1's Corporate Security Department scheduled an interview with ORRIOLS, but he did not show up for the interview.

i. Corporate Security Employee-1 has personally reviewed videotapes from the stores in which ABAD, ORRIOLS, and RODRIGUEZ worked. The videotapes contain video recordings made inside the stores during the specific times when these defendants' unique identification codes were used to access the accounts of Defrauded Customers. Corporate Security Employee-1, who personally interviewed ABAD, concluded that ABAD appeared to be the person depicted in the videotape from the store in which he worked. Similarly, Corporate Security Employee-1 had personally interviewed RODRIGUEZ and concluded that RODRIGUEZ appeared to be the person depicted in the videotape from the store in which he worked. Corporate Security Employee-1 reviewed the video recordings of the store at which ORRIOLS worked with a Provider-1 district manager ("District Manager-1") who supervised the store at which ORRIOLS worked. District Manager-1 told

Corporate Security Employee-1 that the male depicted in the videotape was ORRIOLS.

j. On or before June 11, 2010, ABAD, ANGEL, DORISMA, ESQUEA, LOPEZ, ORRIOLS, RODRIGUEZ, SANTANA, and JACKLIN VOLNY all either resigned or were fired from Provider-1.

9. I have reviewed written summaries of statements made by LUIS ABAD, MATHEWS ANGEL, PRINCETTA DORISMA, LESLY ESQUEA, FRANCIS LOPEZ, PEDRO RODRIGUEZ, JOHNNY SANTANA, and JACKLIN VOLNY, a/k/a "Jeff Volny," the defendants, during their interviews with members of Provider-1's Corporate Security Department prepared by members of Provider-1's Corporate Security Department who were present during the interviews. Based on these summaries, I learned, among other things:

a. LUIS ABAD was interviewed on or about June 9, 2010. During his interview, he stated, in substance and in part, that:

i. My system user ID is ut340673.

ii. I never access a customer's account unless the customer is present or I have assisted the customer in the past and I recognize their voice and telephone number when they call on the phone.

iii. I cannot explain why a report of activity of ID ut340673 shows thirteen accounts, all of which have billing addresses in Idaho, accessed on February 25, 2010 within the span of approximately 20 minutes. I can't understand how all these accounts were accessed in such a short amount of time.

b. MATHEWS ANGEL was interviewed on or about June 9, 2010. During his interview, he stated, in substance and in part, that:

i. My user ID is mal54610. I understand we shouldn't share passwords and I don't share my password with anyone

ii. We can go onto a customer's account when they request information and are in the store. We are not allowed to make any changes to customers' telephone numbers or to their plan. I never gave customers any information over the telephone. I service people who have the PIN and access to the account in the store. For the most part I service customers from

this area. I get some travelers and truck drivers, but for the most part the customers are from this area. I usually access about 200 customer accounts a month; it's a busy store.

c. PRINCETTA DORISMA was interviewed on or about June 8, 2010. During her interview, she signed a written statement stating, in substance and in part, that:

i. My user ID is pr301698. I have not shared my password with anyone at the store.

ii. What is required to access a customer's account if the customer is in the store is verification of the customer's account. There would be no reason to access a customer's account without having a customer in the store. Once in a blue moon, I will access a customer's account if I am following up on a previous issue.

iii. A co-worker approached me and asked me if I wanted to make some extra money. She provided me with phone number ranges to review and I just went through them numerically in E-Ticket. She asked me to get information from these accounts and send them to an email address that she provided me. I would write the customer's name, cell phone number and ESN down and then send them to the email address.

iv. The co-worker who gave me the phone number ranges paid me \$1000 for sending customer account information to the email address. She paid me \$500 twice. At the time I started doing this, I was having some financial issues. I stopped doing this a couple months ago because I felt that this was not right.

d. LESLY ESQUEA was interviewed on or about June 8, 2010. During her interview, she signed a written statement stating, in substance and in part, that:

i. My user ID is lye9966. I have not shared my password with anyone at the store, however, over the past few months, I feel other employees have been using my login for themselves.

ii. What is required to access a customer's account if the customer is in the store is verification of the customer's account through a PIN code or security question. If they are not able to provide this information, they need to provide some form of identification. The only time I have accessed a customer account without having a customer in the

store is if one of my customers contacts me by phone and asks to determine when they will be eligible for an upgrade or exchange.

iii. The reason why a report of activity of my user ID shows that I used E-Ticket to access accounts of customers with billing addresses in Hawaii one right after another, is that sometimes when the store is slow, I just punch in numbers in E-Ticket to see what comes up. I did not have the customer's permission to view the accounts. Accessing these accounts did not follow the established company policy.

e. FRANCIS LOPEZ was interviewed on or about June 8, 2010. During his interview, he stated, in substance and in part, that:

i. My system user ID is fx13889 and my ELID is fr247328. I did not share my codes with any other employee.

ii. The customer is always present when I access their account. I always obtain the authorization of an account holder prior to accessing their account. I cannot think of any occasions where the customer was not present during my access to their account.

iii. I cannot explain why a report of activity of my user ID shows that on February 15, 2010, within the span of twenty minutes, my user ID was linked to account activity through E-ticket to eleven distinct customer accounts based out of the state of Texas. It would not be possible for these eleven customers from Texas to be present in the store when their accounts were accessed.

f. PEDRO RODRIGUEZ was interviewed on or about June 8, 2010. During his interview, he signed a written statement stating, in substance and in part, that:

i. My ELID is zp476473 and I use the same ID to access my employer's systems and databases.

ii. Prior to accessing a customer's account, I always ask for picture identification, wireless phone number and the account PIN. If the customer cannot provide picture identification then I will not access their account without my management's approval. I always follow this process. The customer is always present when I access their account. I always obtain authorization of the account holder prior to accessing their account. I cannot think of any occasions where the customer was not present during my access to their account.

iii. Almost all of the customers that I assist are Bronx and/or Manhattan based customers. I do not really recall assisting and/or accessing the accounts of out of state customers.

g. JOHNNY SANTANA was interviewed on or about June 8, 2010. During his interview, he signed a written statement stating, in substance and in part, that:

i. My ELID is jo215638 and my system user ID is jls6688.

ii. I have a company laptop computer at home, and I continue to use it.

iii. I am an event promoter, and I have been working with people outside this company to gather information about wireless numbers that we can use in "Text Blast" promotions. I randomly enter phone numbers into E-Ticket to determine if they are valid and active phone numbers and then I pass on the phone numbers to another person. I haven't provided any information other than the phone number. I received some compensation in return for the information that I provided. I have received a few hundred dollars in return during the past few months. I estimate that I have provided two to three hundred phone numbers to people outside the company. I believe that my actions were in violation of company policy.

h. JACKLIN VOLNY was interviewed on or about June 8, 2010. During his interview, he stated, in substance and in part, that:

i. My IDs are jjv0428 and ja289760.

ii. There is no reason to access a customer account unless they were present at the store.

iii. I cannot explain why a report of activity of my user ID shows that my user ID was linked to account activity to customer accounts based out of the state of Hawaii. I don't know about logging into those accounts. There is no need for me to go into accounts of customers from Hawaii.

10. I have reviewed data provided to me by Provider-1 concerning the use of the unique identification codes of LUIS ABAD, MATHEWS ANGEL, PRINCETTA DORISMA, LESLY ESQUEA, FRANCIS LOPEZ, LUIS ORRIOLS, PEDRO RODRIGUEZ, JOHNNY SANTANA, and JACKLIN

VOLNY, a/k/a "Jeff Volny," the defendants, to access accounts of Defrauded Customers and learned the following:

a. The Defrauded Customers whose accounts were accessed using the unique identification codes of ABAD, ANGEL, DORISMA, ESQUEA, LOPEZ, ORRIOLS, RODRIGUEZ, SANTANA, and VOLNY, often had billing addresses located in states distant from the states in which they worked. More specifically:

i. ABAD worked at a store in North Bergen, New Jersey, but over 99% of the Defrauded Customers whose accounts were accessed using his unique identification code had an out-of-state billing address. The state in which the largest number of these Defrauded Customers had a billing address was Texas.

ii. ANGEL worked at a store in North Bergen, New Jersey, but over 99% of the Defrauded Customers whose accounts were accessed using his unique identification code had an out-of-state billing address. The state in which the largest number of these Defrauded Customers had a billing address was Texas.

iii. DORISMA worked at a store in Tampa, Florida, but over 96% of the Defrauded Customers whose accounts were accessed using her unique identification code had an out-of-state billing address. The state or territory in which the largest number of these Defrauded Customers had a billing address was Puerto Rico.

iv. ESQUEA worked at a store in Tampa, Florida, but over 99% of the Defrauded Customers whose accounts were accessed using her unique identification code had an out-of-state billing address. The state in which the largest number of these Defrauded Customers had a billing address was Hawaii.

v. LOPEZ worked at a store in North Bergen, New Jersey, but over 99% of the Defrauded Customers whose accounts were accessed using his unique identification codes had an out-of-state billing address. The state in which the largest number of these Defrauded Customers had a billing address was Texas.

vi. ORRIOLS worked at a store in North Bergen, New Jersey, but over 99% of the Defrauded Customers whose accounts were accessed using his unique identification code had an out-of-state billing address. The state in which the largest

number of these Defrauded Customers had a billing address was Texas.

vii. RODRIGUEZ worked at a store in the Bronx, New York, but over 95% of the Defrauded Customers whose accounts were accessed using his unique identification code had an out-of-state billing address. The state or territory in which the largest number of these Defrauded Customers had a billing address was Puerto Rico.

viii. SANTANA worked at a store in the Bronx, New York, but over 99% of the Defrauded Customers whose accounts were accessed using his unique identification code had an out-of-state billing address. The state in which the largest number of these Defrauded Customers had a billing address was Maine.

ix. VOLNY worked at a store in Tampa, Florida, but over 99% of the Defrauded Customers whose accounts were accessed using his unique identification code had an out-of-state billing address. The state in which the largest number of these Defrauded Customers had a billing address was Hawaii.

b. The unique identification codes of ABAD, ANGEL, DORISMA, ESQUEA, LOPEZ, ORRIOLS, RODRIGUEZ, SANTANA, and VOLNY were often used to access accounts of Defrauded Customers less than five days before calls were made from cloned cell phones using the MSIDs and ESNs assigned to Defrauded Customers' cell phones. The following chart summarizes for each of the defendants (i) the approximate time period during which each defendant's unique identification code was used to access accounts of Defrauded Customers, (ii) the minimum number of times during this time period that the unique identification code, or codes, assigned to the defendant was used to access accounts of Defrauded Customers, (iii) the minimum number of times that calls were made from cloned cell phones using MSIDs and ESNs assigned to a Defrauded Customer less than five days after the Defrauded Customer's account was accessed using the respective defendant's unique identification code, (iv) the minimum dollar amount of charges accruing to the accounts of Defrauded Customers due to unauthorized calls made using the ESNs and MSIDs of Defrauded

Customers whose accounts were accessed using the unique identification code, or codes, assigned to the defendant:

Defendant/Employee	Date Range During Which Defrauded Customer Accounts Were Accessed Using Defendant/Employee's Unique Code	Minimum Number of Times Defrauded Customer Accounts Were Accessed	Less Than 50 Days From Defrauded Customer Account Access to Cloned Phone Calling Using Defrauded Customer ESN/MSID	Minimum Fraudulent Charges
LUIS ABAD	15 Feb - 2 Jun 2010	2255	1655	\$798,305.64
MATHEWS ANGEL	15 Feb - 26 May 2010	1449	1143	\$887,256.79
PRINCETTA DORISMA	15 Feb - 14 Mar 2010	101	5	\$42,984.43
LESLY ESQUEA	20 Feb - 26 May 2010	921	323	\$1,484,266.94
FRANCIS LOPEZ	25 Jan - 1 Jun 2010	3906	2877	\$1,396,720.61
LUIS ORRIOLS	3 Jan - 1 Jun 2010	3727	2881	\$1,453,464.50
PEDRO RODRIGUEZ	14 Feb - 2 Jun 2010	1598	798	\$1,868,151.63
JOHNNY SANTANA	18 Feb - 5 May 2010	1566	557	\$6,996,106.07
JACKLIN VOLNY	15 Feb - 21 May 2010	580	232	\$687,807.84

c. The unique identification codes of ABAD, ANGEL, DORISMA, ESQUEA, LOPEZ, ORRIOLS, RODRIGUEZ, SANTANA, and VOLNY were used to access accounts of Defrauded Customers within a very short period of time and often the phone numbers for the Defrauded Customers whose accounts were accessed during that short time period were identical except for the last two digits. For example:

i. On or about April 29, 2010, between 13:45 (EST) and 14:09 (EST), the identification code assigned to ABAD was used to access 17 accounts of Defrauded Customers. All 17 belonged to account holders with billing addresses outside the state in which the Provider-1 store at which ABAD worked was located, including 16 account holders located in Illinois.

ii. On or about February 19, 2010, between 14:23 (EST) and 14:56 (EST), the identification code assigned to ANGEL was used to access 21 accounts of Defrauded Customers. All 21 of these accounts belonged to account holders with billing addresses in Maryland, which is not the state in which the Provider-1 store at which ANGEL worked was located. In addition, 7 of the Defrauded Customers' phone numbers were identical other than the last two digits.

iii. On or about February 18, 2010, between 18:15 (EST) and 19:11 (EST), the identification code assigned to DORISMA was used to access 15 accounts of Defrauded Customers. Of these accounts, 14 belonged to account holders with billing addresses outside the state in which the Provider-1 store at which DORISMA worked was located, including 13 account holders

located in Puerto Rico. In addition, 11 of the Defrauded Customers' phone numbers were identical other than the last two digits.

iv. On or about March 10, 2010, between 16:41 (EST) and 17:42 (EST), the identification code assigned to ESQUEA was used to access 63 accounts of Defrauded Customers. Of these accounts, 61 belonged to account holders with billing addresses outside the state in which the Provider-1 store at which ESQUEA worked was located, including 54 account holders located in Hawaii. In addition, 26 of the Defrauded Customers' phone numbers were identical other than the last two digits.

v. On or about March 3, 2010, between 14:35 (EST) and 16:01 (EST), a identification code assigned to LOPEZ was used to access 19 accounts of Defrauded Customers. All 19 belonged to account holders with billing addresses in Carlsbad, New Mexico, which is outside the state in which the Provider-1 store at which LOPEZ worked was located. In addition, 14 of the Defrauded Customers' phone numbers were identical other than the last two digits.

vi. On or about February 14, 2010, between 10:18 (EST) and 12:30 (EST), the identification code assigned to ORRIOLS was used to access 25 accounts of Defrauded Customers. All 25 accounts belonged to account holders with billing addresses outside the state in which the Provider-1 store at which ORRIOLS worked was located, including 22 account holders located in Texas. In addition, 19 of the Defrauded Customers' phone numbers were identical other than the last two digits.

vii. On or about March 18, 2010, between 10:53 (EST) and 12:47 (EST), the identification code assigned to RODRIGUEZ was used to access 11 accounts of Defrauded Customers. All 11 accounts belonged to account holders with billing addresses outside the state in which the Provider-1 store at which RODRIGUEZ worked was located, including 10 account holders located in Puerto Rico territory. In addition, 9 of the Defrauded Customers' phone numbers were identical other than the last two digits.

viii. On or about February 22, 2010, between 00:47 (EST) and 02:54 (EST), the identification code assigned to SANTANA was used to access 43 accounts of Defrauded Customers.¹

¹ This access time is not during business hours of the store in which SANTANA was working. As set forth in paragraph 9(g) above, SANTANA had a Provider-1 laptop at his home.

Of these accounts, 44 belonged to account holders with billing addresses outside the state in which the Provider-1 store at which SANTANA worked was located, including 43 account holders located in Connecticut. In addition, all 44 of the Defrauded Customers' phone numbers were identical other than the last four digits.

ix. On or about February 17, 2010, between 15:00 (EST) and 16:52 (EST), the identification code assigned to VOLNY was used to access 19 accounts of Defrauded Customers. Of these accounts, 17 belonged to account holders with billing addresses outside the state in which the Provider-1 store at which VOLNY worked was located, including 15 account holders located in Hawaii. In addition, 14 of the Defrauded Customers' phone numbers were identical other than the last two digits.

d. The unique identification codes of ABAD, ANGEL, DORISMA, ESQUEA, LOPEZ, ORRIOLS, RODRIGUEZ, SANTANA, and VOLNY all were used to access a Defrauded Customer account that was accessed using the unique identification code of at least one other defendant. For example, between in or about January 2010 through in or about June 2010:

i. ABAD's unique identification code was used to access an account of a Defrauded Customer with a billing address in Texas that was also accessed using the unique identification code of LOPEZ.

ii. ANGEL's unique identification code was used to access an account of a Defrauded Customer with a billing address in Georgia that was also accessed using the unique identification codes of LOPEZ and ORRIOLS.

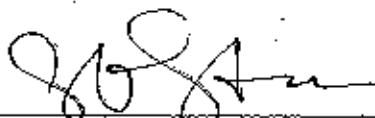
iii. DORISMA's unique identification code was used to access an account of a Defrauded Customer with a billing address in Puerto Rico that was also accessed using the unique identification code of RODRIGUEZ.

iv. ESQUEA's unique identification code was used to access an account of a Defrauded Customer with a billing address in Hawaii that was also accessed using the unique identification codes of VOLNY and RODRIGUEZ.

v. SANTANA's unique identification code was used to access an account of a Defrauded Customer with a billing address in Florida that was also accessed using the unique identification code of RODRIGUEZ.

11. Based on my training and experience and consultation with other Special Agents in the USSS, I know that when database users access a national database such as E-Ticket, this access usually involves interstate wire communications. In particular, changing a cell phone user's account information from a location outside the state where that cell phone user resides would be highly likely to involve interstate wire communications.

WHEREFORE, deponent prays that a warrant be issued for the arrest of LUIS ABAD, MATHEWS ANGEL, PRINCETTA DORISMA, LESLY ESQUEA, FRANCIS LOPEZ, LUIS ORRIOLS, PEDRO RODRIGUEZ, JOHNNY SANTANA, and JACKLIN VOLNY, a/k/a "Jeff Volny," the defendants, and that they be arrested and imprisoned, or bailed, as the case may be.



SAMUEL STORRER
SPECIAL AGENT
UNITED STATES SECRET SERVICE

Sworn to before me this
26 day of August 2010



HONORABLE GEORGE A. YANTHIS
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK