

AO (Rev. 5/85) Criminal Complaint

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

FILED

2011 OCT 31 PM 5:02

US DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO, FLORIDA

UNITED STATES OF AMERICA

CRIMINAL COMPLAINT

vs.

CASE NUMBER: 6:11-mj-1496

ROBIN MIGUEL CORRALES CASTRO
SILVIO LEON
IVAN MALAGON
LAZARO J CORRALES CASTRO
FEDERICO MARTINEZ

I, the undersigned complainant, being duly sworn, state the following is true and correct to the best of my knowledge and belief. Beginning on a date unknown to the United States, but no later than in or about in or about January 2011, and continuing to in or about October 2011, in Orange County, in the Middle District of Florida, and elsewhere, the defendants did,

conspire to produce, use, or traffic in one or more counterfeit access devices, such production, use, or trafficking affecting interstate or foreign commerce

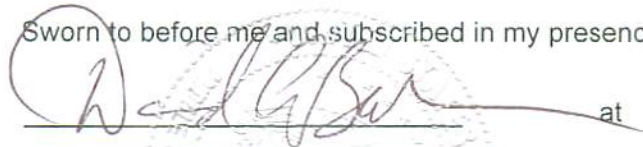
in violation of Title 18, United States Code, Section(s) 371. I further state that I am a(n) Special Agent with United States Secret Service, and that this Complaint is based on the following facts:

SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof: Yes No


Signature of Complainant
Ernest Wrenn

Sworn to before me and subscribed in my presence,


_____ at

Orlando, Florida 10/31/11

THE HONORABLE DAVID A. BAKER
United States Magistrate Judge
Name & Title of Judicial Officer

Signature of Judicial Officer

State of Florida
County of Orange

6:11-mj-1496, 1497, 1498, 1499,
1500, 1501, 1502, 1503

MASTER AFFIDAVIT

I, Ernest Wrenn, being duly sworn, state as follows:

Introduction

1) I am a Special Agent (SA) with the United States Secret Service (USSS) assigned to the Orlando Field Office. Among my duties as a Special Agent, I am charged with the investigation of financial crimes, including bank fraud, wire fraud, identity fraud, credit card fraud, and the manufacturing, possession, and passing of counterfeit private securities, counterfeit United States currency, and counterfeit and fraudulent access devices, such as credit cards, debit cards, and gift cards.

2) The information in this affidavit is based on my personal knowledge, information obtained from other law enforcement personnel, information obtained from corporate investigators, and information obtained from financial and other banking institutions. The information set forth herein is provided solely for the purpose of establishing probable cause in support of the requested arrest warrants, search warrants, and seizure warrants. Because this affidavit is submitted for the limited purpose of establishing such probable cause, it does not include all of the details of this investigation of which I am aware.

Arrest Warrants Requested

3) This affidavit is made in support of an application for arrest warrants for **ROBIN MIGUEL CORRALES CASTRO (R. CASTRO), SILVIO LEON (LEON), IVAN MALAGON (MALAGON), LAZARO J CORRALES CASTRO (L. CASTRO), and FEDERICO MARTINEZ (MARTINEZ)** for violations of Title 18, United States Code,

Sections 371 (conspiracy) and 1029 (fraud and related activity in connection with access devices).

Search Warrants Requested

4) This affidavit is also made in support of a warrant to search the business of **R. CASTRO** and **LEON**, located at **7612 Sun Vista Way, Orlando, FL (SIMPLE MOBILE)**, more specifically described in attachment A, and the residence of **R. CASTRO**, located at **4251 Anthony Lane, Orlando, FL (R. CASTRO RESIDENCE)**, more specifically described in attachment B, which is incorporated herein by reference, for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 371 (conspiracy) and 1029 (fraud and related activity in connection with access devices), which evidence, fruits, and instrumentalities are described more specifically in Attachment C, which is incorporated herein by reference. Based on information I obtained during this investigation, **R. CASTRO** and **LEON** are the co-owners of **SIMPLE MOBILE**, a business incorporated as R.S. Telecommunications, Inc.

5) This affidavit is also made in support of an application to search five vehicles: (a) a **2007 Nissan Armada**, FL license plate **AHSY36**, VIN #**5N1AA08AX7N703435**, registered to **Yanisleivy Morejon Valdes** (Valdes is the wife of **R. CASTRO**), more specifically described in Attachment D; (b) a **2007 Cadillac Escalade**, FL license plate **AHSX58**, VIN #**1GYFK63887R289038**, registered to Valdes, more specifically described in Attachment E; (c) a **2005 Nissan Titan**, FL license plate **S819NA**, VIN #**1N6BA06A55N537945**, registered to **MARTINEZ**, more specifically described in Attachment F; and (d) a **2006 Ford F150**, FL license plate **800NJL**, VIN #**1FTRX12526FA54665**, registered to **Katia Suarez** (Suarez is the

girlfriend of LEON), more specifically described in Attachment G, (e) a 2007 BMW, FL license plate AUHC53, VIN #WBAIN83557DT68622, registered to Lisset Martinez (Martinez is the wife of MARTINEZ), more specifically described in Attachment H. for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 371 (conspiracy) and 1029 (fraud and related activity in connection with access devices), which evidence, fruits, and instrumentalities are described more specifically in Attachment C.

Seizure Warrants Requested

6) This affidavit is also made in support of an application for seizure warrants for the 2007 Nissan Armada, 2007 Cadillac Escalade, 2005 Nissan Titan, 2006 Ford F150, and 2007 BMW, described more fully above. All of the above-listed vehicles were used to commit the violations of Title 18, United States Code, Sections 371 (conspiracy) and 1029 (fraud and related activity in connection with access devices) described in this affidavit.¹

Initiation of the Investigation by the USSS Orlando Field Office

7) In June 2011, I was contacted by Chase Bank Investigator Jeremy Geisel. Investigator Geisel informed me that he had discovered access device fraud that was occurring in Central Florida. According to Investigator Geisel, a Chase account holder reported fraudulent charges to their account, totaling \$73,577.27, at Orlando area Target stores on June 18, 2011, using Chase Visa card ****2309. The subjects of these arrest warrants, search warrants, and seizure warrants are those persons in Central Florida that agents have identified as using credit card account numbers to make hundreds of thousands of dollars in fraudulent credit card

¹ The United States requests seizure warrants in order to assure the availability of the vehicles for trial. Due to the fact that the assets to be seized are easily movable, the United States contends a seizure warrant is the only means which assure that the vehicles will be available for trial.

transactions at Target and other retail stores. Thus, when in this affidavit a credit card account is said to be used "fraudulently," it means that the credit card account number and related data was stolen via a data breach (i.e. the use of skimming device), and used without the authorization of the account holder. Further, based upon information provided by credit card companies and other law enforcement agencies, I believe that the suspects are obtaining compromised credit card numbers via skimming devices that are installed on gas pumps at gas stations in Central Florida, and the suspects are then using device-making tools to manufacture the fraudulent credit cards, debit cards, gift cards, and other access devices that allow them to perpetrate the fraud.

Information Obtained from Credit Card Companies and Retailers

8) On July 15, 2011, I met with Melissa Trahan (Trahan), a Lead Investigator with Target Asset Protection, and reviewed copies of surveillance videos of fraudulent transactions at several Target locations throughout Central Florida. Trahan provided surveillance videos of **R. CASTRO, LEON, L. CASTRO, MALAGON, and MARTINEZ** using fraudulent access devices inside several Target stores in Central Florida. Trahan also provided the suspects' vehicle information, including Florida license plate numbers. Trahan told me that Target stores in Central Florida are familiar with the suspects and have been documenting fraudulent charges at each of the affected stores. According to the information provided by Target, the suspects used the following vehicles during the course of their fraudulent activity: a **2007 white Nissan Armada**, FL license plate AHSY36, registered to Valdes; a **2007 Cadillac Escalade**, FL license plate AHSX58, registered to Valdes; a **2005 Nissan Titan**, FL license plate S819NA, registered to **MARTINEZ**; a **2006 Ford F150**, FL license plate 800NJL, registered to Suarez; and a **2007 BMW**, FL license plate AUHC53, registered to Lisset Martinez. Further, Trahan provided

agents with receipts listing the credit card numbers used by **R. CASTRO, LEON, L. CASTRO, MALAGON, and MARTINEZ**, along with surveillance videos of the fraudulent transactions. Those surveillance videos, examples of which are discussed in the following paragraphs, also show **R. CASTRO, LEON, L. CASTRO, MALAGON, and MARTINEZ** using the **2007 Nissan Armada, 2007 Cadillac Escalade, 2005 Nissan Titan, 2006 Ford F150, and 2007 BMW** to facilitate the fraud.

9) In July 2011, I contacted Kristin Kenerson (Kenerson) of American Express about the fraud committed in this case. I provided Kenerson with a spreadsheet of purchases and corresponding American Express credit card numbers used fraudulently at Target by **R. CASTRO, LEON, L. CASTRO, MALAGON, and MARTINEZ**. Kenerson researched the listed purchases and confirmed that the credit card numbers were used fraudulently, i.e. without the authorization of the actual account holders, to make those purchases. Kenerson further confirmed that, to date, and solely in relation to American Express credit cards, there currently is \$125,564.60 of identified fraud related to this investigation. Kenerson also determined a point of compromise to be Hess gas station (store #09369), in Winter Springs, FL.

10) In July 2011, I contacted Sam Fadel (Fadel) of Discover about the fraud committed in this case. I provided Fadel with a spreadsheet of purchases and corresponding Discover credit card numbers used fraudulently at Target by **R. CASTRO, LEON, L. CASTRO, MALAGON, and MARTINEZ**. Fadel researched the listed purchases and confirmed that the credit card numbers were used fraudulently, i.e. without the authorization of the actual account holders, to make those purchases. Fadel further confirmed that, to date, and solely in relation to Discover credit cards, there currently is \$30,220.91 of identified fraud

related to this investigation.

11) Based upon the information and video surveillance provided by Target, and the information provided by American Express and Discover, between January 2011 and October 2011, more than 175 credit card numbers were used fraudulently by the suspects at retail stores in Central Florida. The following are examples of the fraudulent credit card activity committed by the subjects of this investigation; these transactions are a small sample of the total number of fraudulent transactions documented by Target, Best Buy, Home Depot, and Wal-Mart, and it does not include all of the details of the investigation of which I am aware:

- a) Surveillance video provided by Target shows that on January 10, 2011, at approximately 6:35 p.m., **MALAGON** went inside of the Target store #2032, located at 3770 N. Goldenrod Road, Winter Park, FL 32792. There, **MALAGON** fraudulently used the following Visa and MasterCard credit card account numbers to make purchases: ****1762 (MC, declined), and ****3772 (Visa, approved).
- b) Surveillance video provided by Target shows that on February 7, 2011, at approximately 10:30 a.m., the 2007 Nissan Armada pulled into the parking lot of the Target store 1760, located at 325 N. Alafaya Trail, Orlando, FL 32828. **R. CASTRO** and **LEON** got out of the 2007 Nissan Armada and went into the Target. There, **R. CASTRO** and **LEON** fraudulently used the following Visa and MasterCard credit card account numbers to make purchases: ****6402 (Visa, declined), ****3423 (MC, declined), ****8817 (MC, declined), and ****9264 (MC, approved).

- c) Surveillance video provided by Target store #0649 shows that on May 6, 2011, at approximately 12:00 p.m., a black 2007 4-door Nissan Titan, FL tag AHSX58.² pulled into the parking lot of the Target located at 718 Maguire Blvd, Orlando, FL 32803. **R. CASTRO, LEON, and MALAGON** got out of the 2007 4-door Nissan Titan and went into the Target. There, **R. CASTRO, LEON, and MALAGON** fraudulently used the following Visa and MasterCard credit card account numbers to make purchases: ****1028 (MC, approved for some charges, and then declined), ****4408 (Visa, approved for some charges, and then declined), ****6689 (Visa, declined), and ****1956 (MC, approved for some charges, and then declined).
- d) Surveillance video provided by Total Wine shows that on June 4, 2011, at approximately 5:15 p.m., **MALAGON** went into Total Wine, located at 2712 E. Colonial Drive, Orlando, FL 32803. There, **MALAGON** fraudulently used the following Visa credit card account number to make purchases: ****8294 (Visa, approved). Upon completion of the transaction the cashier noticed that last four (4) digits of the credit card number did not match the last four (4) digits of the credit card number on the receipt. Upon questioning, **MALAGON** fled the scene in a vehicle registered to **MALAGON**. An examination of the credit card left behind by **MALAGON** revealed that the credit card had been re-encoded with a fraudulently obtained credit card number.
- e) Surveillance video provided by Target store #0650 shows that on July 21, 2011, at approximately 1:00 p.m., the 2007 4-door Nissan Titan, FL tag AHSX58, pulled into the

² The government is not seeking to seize this vehicle because, as explained more fully in this affidavit, this vehicle was traded for the 2007 Cadillac Escalade that the government is seeking to seize.

parking lot of the Target located at 880 Sand Lake Road. Orlando, FL 32809. **R. CASTRO, LEON, and L. CASTRO** got out of the 2007 4-door Nissan Titan and went into the Target. There, **R. CASTRO, LEON, and L. CASTRO** fraudulently used the following Visa and MasterCard credit card account numbers to make purchases: ****6220 (Visa, approved), ****3295 (MC, approved for some charges, and then declined), ****4610 (Visa, declined), and ****0694 (MC, approved).

- f) Surveillance video provided by Target store #0647 shows that on July 22, 2011, at approximately 11:55 p.m., the 2007 4-door Nissan Titan, FL tag AHSX58, pulled into the parking lot of the Target located at 886 W. State Road 436, Altamonte Springs, FL 32714. **R. CASTRO, LEON, and L. CASTRO** got out of the 2007 4-door Nissan Titan and went into the Target. There, **R. CASTRO, LEON, and L. CASTRO** fraudulently used the following Visa and MasterCard credit card account numbers to make purchases: ****4780 (Visa, declined), ****3818 (Visa, declined), ****6458 (Visa, declined), ****8567 (Visa, declined), ****0895 (Visa, approved for some charges, and then declined), and ****2024 (Visa, approved). Upon completion of the transactions **R. CASTRO, LEON, and L. CASTRO** were seen by Loss Prevention personnel, which caused the suspects to flee the store. Before leaving the parking lot, the suspects placed a cardboard cover over the license tag, completely blocking the view of the tag. The suspects stopped at a nearby bus stop and discarded nine (9) counterfeit credit cards bearing the names of **R. CASTRO, LEON, and L. CASTRO**. All nine counterfeit credit cards were recovered by the Seminole County Sheriff's Office.

- g) Surveillance video provided by Best Buy shows that on July 27, 2011, at approximately 7:45 p.m., the **2005 Nissan Titan** and the **2007 BMW** pulled into the parking lot of the Best Buy store #157, located at 845 N. Alafaya Trail, Orlando, FL 32828. **MALAGON** got out of the **2005 Nissan Titan**, while **MARTINEZ** got out of the **2007 BMW**. Both suspects entered the Best Buy. There, **MALAGON** and **MARTINEZ** fraudulently used the following Visa credit card account number to make purchases: ****4995 (Visa, approved). Upon leaving store #157, both **MALAGON** and **MARTINEZ** relocated to store #571, located on E. Colonial Drive, Orlando, FL, where they made purchases using a Visa card ending in ****9018 (Visa, approved).
- h) Surveillance video provided by Target store #1760 shows that on August 16, 2011, at approximately 12:10 p.m., the **2007 Cadillac Escalade** pulled into the parking lot of the Target located at 325 N. Alafaya Trail, Orlando, FL 32828. **R. CASTRO** and **LEON** got out of the **2007 Cadillac Escalade** and went into the Target. There, **R. CASTRO** and **LEON** fraudulently used the following Visa and MasterCard credit card account numbers to make purchases: ****7400 (Visa, approved), ****5422 (Visa, declined), and ****7043 (Visa, approved).
- i) Surveillance video provided by Target, Best Buy, and ABC Fine Wine/Spirits shows that on September 17, 2011, at approximately 5:40 p.m., the **2007 BMW** pulled into the parking lot of the Target store #1760 located at 325 N. Alafaya Trail, Orlando, FL 32828. **MARTINEZ** got out of the **2007 BMW** and went into the Target. **MARTINEZ** fraudulently used the following Visa credit card account number to make purchases: ****4290 (Visa, approved). On the same date, surveillance video shows **MARTINEZ**

making additional purchase with the same credit card number at Best Buy and ABC Fine Wine/Spirits. While at Best Buy, **MARTINEZ** signed up for a Best Buy Rewards card under the name "Fred Martinez," with a fictitious address of 2525 Forethy, Orlando, FL 32807, with an email address of FRED25252@gmail.com.

- j) Surveillance video provided by Target store #0649 shows that on September 21, 2011, at approximately 12:00 p.m., the 2006 Ford F150 pulled into the parking lot of the Target located at 718 Maguire Blvd, Orlando, FL. **R. CASTRO** and **LEON** got out of the 2006 Ford F150 and went into the Target. There, **R. CASTRO** and **LEON** fraudulently used the following Visa and American Express credit card account numbers to make purchases: ****2001 (AMEX. declined), ****2002 (AMEX. approved), and ****6066 (Visa, approved).

Information Obtained from Local Law Enforcement Confidential Source

12) In September 2011, I received information from Organized Crime Unit Detectives with the Orange County Sheriff's Office (OCSO) concerning **R. CASTRO** re-encoding credit cards at the **R. CASTRO RESIDENCE**, using those re-encoded cards fraudulently, and selling gift cards that he obtained fraudulently for a fraction of the actual value of each gift card. In particular, SA Edward Thompson (USSS), along with OCSO Detectives conducted multiple interviews with a Confidential Source (CS). The CS has been charged with the use of stolen credit card numbers to purchase gasoline and diesel fuel, and the sale of that diesel fuel for a fraction of its value. The CS is cooperating in the on-going state investigation in hopes of receiving a reduction in his state sentence related to his state charge. Information provided by the CS has been corroborated by this USSS investigation, and I believe that the CS is providing

accurate and reliable information concerning the suspects in this investigation.

13) According to the CS, in 2011, the CS went to the **R. CASTRO RESIDENCE** and saw **R. CASTRO** inside the **R. CASTRO RESIDENCE** using a card reader/encoder to “swipe” cards. According to the CS, **R. CASTRO** was re-encoding cards with stolen credit card numbers for the purpose of using the re-encoded cards fraudulently to make purchases. The CS also stated that the card reader/encoder was attached to a computer that **R. CASTRO** was using during the manufacturing process. Further, the CS stated that in 2011 the CS had seen approximately 1,000 Target gift cards on a single visit inside the **R. CASTRO RESIDENCE**. The CS also verified the address of the **R. CASTRO RESIDENCE**.

14) In addition, the CS told the Organized Crime Unit Detectives with the OCSO and SA Thompson that **R. CASTRO** sells gift cards that he obtained fraudulently for a fraction of the actual value of each gift card. According to the CS, in 2011 the CS saw fraudulently obtained gift cards being sold at **SIMPLE MOBILE**. In 2011, the CS also stated that he had seen **R. CASTRO** purchase items, such as televisions, at retail stores using re-encoded cards, and then sell those items at a discount at **SIMPLE MOBILE**.

Initial Surveillance by the USSS

15) Between July 2011 and October 2011, I conducted surveillance approximately once a week at the **R. CASTRO RESIDENCE**. During that time, I consistently saw the 2007 Nissan Armada, the 4-door 2007 Nissan Titan, and the 2007 Cadillac Escalade parked at the **R. CASTRO RESIDENCE**. Several times, I witnessed **R. CASTRO** and his wife, Valdes, leave the residence and get into those vehicles. The vehicles at the residence matched the vehicles identified by Target. In addition, other agents and I watched **R. CASTRO** drive back and forth

between the **R. CASTRO RESIDENCE** and the **SIMPLE MOBILE** store. On occasion, agents saw **L. CASTRO** riding a bike between the **R. CASTRO RESIDENCE** and **SIMPLE MOBILE**. The residence and the store are approximately one-half mile from each other. From June 2011 through August 2011, Florida license plate AHSX58 was displayed on, and registered to, the 4-door Nissan Titan, which was also registered to Valdes. From August 2011 to the present, the same tag has been displayed on the 2007 Cadillac Escalade. Further, I have conducted mail checks with the U.S. Postal Service and discovered that mail is being sent to the **R. CASTRO RESIDENCE** in the name of **R. CASTRO**, Valdes, and the business name of RS Telecommunications Inc (i.e. **SIMPLE MOBILE**).

16) Between June 2011 and September 2011, I conducted surveillance on several occasions at the residence of **LEON**, located at 1921 S. Kirkman Road, Apt 221, Orlando, FL. The surveillances occurred weekly to monitor traffic in and out of the residence. I consistently saw the 2006 Ford F150 at the residence. On several occasions, I also saw the 2007 4-door Nissan Titan parked at the residence.

USSS Two-Day Surveillance of the Suspects

17) On August 16, 2011 and August 17, 2011, other USSS agents and I, as well as Detectives from Seminole County Sheriff's Office Financial Crimes Task Force, conducted surveillance of the suspects. During the surveillance, agents saw **R. CASTRO**, **LEON**, and **MALAGON** engaging in fraudulent credit card transactions similar to the transactions at Target and other stores already described in this affidavit. During the two days that agents followed the suspects, the suspects made approximately \$1,129.42 in successful fraudulent credit card purchases, and attempted to make an additional \$2,644.33 in credit purchases that were declined.

During those two days, the suspects used approximately two (2) fraudulent MasterCard credit card numbers and eight (8) fraudulent Visa credit card numbers.

Surveillance - August 16, 2011

18) On August 16, 2011, agents of the Secret Service and other law enforcement officers conducted surveillance of **SIMPLE MOBILE**. **R. CASTRO** and **LEON** arrived at the store at approximately 11:30 a.m. **R. CASTRO** arrived driving the **2007 Cadillac Escalade**. **LEON** arrived in the **2006 Ford F150**.

19) At about 11:45 a.m., **R. CASTRO** and **LEON** left **SIMPLE MOBILE** in the **2007 Cadillac Escalade** and drove to Target store #1760, located at 325 N. Alafaya Trail, Orlando, FL 32828. **R. CASTRO** and **LEON** then used the following Visa credit cards numbers fraudulently to make purchases of gift cards at Target: ****7400 (Visa, approved), ****7400 (Visa, declined), ****5422 (Visa, declined), ****7043 (Visa, approved), ****7043 (Visa, declined), ****5422 (Visa, declined), ****7043 (Visa, declined), and ****7400 (Visa, declined). **R. CASTRO** and **LEON** then drove back to **SIMPLE MOBILE**, and agents saw **CASTRO** go into **SIMPLE MOBILE** carrying the gift cards that he and **LEON** had just purchased fraudulently at the Target.

20) At about 1:35 p.m., **R. CASTRO**, **LEON**, and Ernesto Ayon (Ayon) left **SIMPLE MOBILE** in the **2007 Cadillac Escalade** and drove to the Home Depot located at 7007 Narcoossee Road, Orlando, FL 32822. Agents then watched as **R. CASTRO**, **LEON**, and Ayon attempted to make credit card purchases. However, all the credit card transactions were declined. **R. CASTRO**, **LEON**, and Ayon then drove back to **SIMPLE MOBILE**.

21) At approximately 4:00 p.m., **R. CASTRO** and his wife, Valdes, left **SIMPLE MOBILE** in the **2007 Nissan Armada**. Agents watched as the vehicle stopped at Murphy's gas station located at 201 South Chickasaw Trail, Orlando, FL. Agents then watched as **R. CASTRO** and Valdes attempted to use multiple credit cards to purchase gas. However, all of the credit cards were declined. **R. CASTRO** and Valdes then returned to **SIMPLE MOBILE**.

Surveillance - August 17, 2011

22) On August 17, 2011, agents of the Secret Service and other law enforcement officers continued their surveillance of **SIMPLE MOBILE**.

23) At about 11:55 p.m., **MALAGON** left **SIMPLE MOBILE** and drove a red Dodge truck to Target store #2032, located at 3770 N. Goldenrod Road, Winter Park, FL 32792. There, agents watched as **MALAGON** purchased gift cards fraudulently by using the following Visa and MasterCard credit card numbers: ****8408 (MC, declined), ****1959 (Visa, approved), and ****1959 (Visa, approved).

24) At about 12:15 p.m., **R. CASTRO** and **LEON** left **SIMPLE MOBILE** and drove to a truck/boat storage yard located at the intersection (Northeast corner) of Forsyth Road and Memory Lane in Orlando, FL. Through my knowledge of this investigation and through discussion with other law enforcement officers, I know that this lot is a common location visited by individuals who are involved in the use of skimming devices to fraudulently obtain credit card numbers. This lot is also used to store trucks that are used to obtain large amounts of gasoline by purchasing the gasoline using fraudulently obtained credit card numbers. In particular, as part of on-going and past investigations, OCSO's Organize Crime Unit has tracked several vehicles to this location that had large fuel bladders added to the vehicle to increase the capacity for fuel. In

some cases, additional fuel cells were added to the beds of trucks. During OCSO's investigations, these vehicles were seen during multiple surveillances coming and going from this lot. While away from the lot, OCSO Detectives have watched the suspects in this case purchase large amounts of gasoline with fraudulently obtained credit card numbers. OCSO Detectives confirmed that this location is currently being used to store these vehicles on a weekly basis. In addition, OCSO confirmed with several credit card companies that the fraudulently obtained credit card numbers used to purchase gasoline were obtained at the same Central Florida gas stations where it is believed that skimmers have been utilized to capture the card numbers. During this USSS surveillance, **R. CASTRO** and **LEON** parked their vehicle behind a yellow building with the sign, "OFFICE," posted next to the front door. Agents then watched as **R. CASTRO** and **LEON** walked inside the yellow building and also walked around the lot. **R. CASTRO** and **LEON** then drove back to **SIMPLE MOBILE**.

25) At about 2:40 p.m., **R. CASTRO** and **LEON** left **SIMPLE MOBILE** in the 2007 Cadillac Escalade and drove to Target store #2032, located on 3770 N. Goldenrod Road, Winter Park, FL 32792. There, agents watched as **R. CASTRO** and **LEON** fraudulently purchased Visa gift cards by using the following credit card numbers: ****5510 (Visa, declined), ****7229 (MC, declined), ****4015 (Visa, declined), ****3027 (Visa, declined), ****5683 (Visa, declined), ****7229 (MC, approved), ****7229 (MC, declined), ****7229 (MC, declined), ****4015 (Visa, approved), ****4015 (Visa, declined), ****5510 (Visa, approved), ****5510 (Visa, approved), ****5510 (Visa, declined), ****3027 (Visa, declined), and ****5683 (Visa, declined). As the suspects left Target and walked across the parking lot, agents saw **R. CASTRO** placing a large number of credit cards into his wallet.

26) At about 4:00 p.m., **R. CASTRO** and **LEON**, after leaving Target in the 2007 **Cadillac Escalade**, stopped at the CITGO gas station located at 5698 Lake Underhill Road, Orlando, FL 32807. There, agents saw **R. CASTRO** and **LEON** attempt to use fraudulently the following credit card numbers to purchase gasoline: ****7229 (MC, declined), ****5510 (Visa, declined), ****4015 (Visa, declined), ****3027 (Visa, declined), and ****5683 (Visa, declined). Once the suspects left the gas station, agents contacted the store manager to obtain the above-mentioned credit card numbers. In addition to obtaining the credit card numbers, agents retrieved a Target bag from the trash can next to the gas pump used by **R. CASTRO** and **LEON**. That discarded Target bag contained receipts that corresponded with the Target purchases described in the foregoing paragraph.

27) At about 4:10 p.m., after leaving the CITGO gas station, **R. CASTRO** and **LEON** stopped at several pawn stores in the southeast Orlando area. While at Pawn America, I saw **R. CASTRO** pull between eight and ten credit cards from his wallet and look through them as he was standing next to the 2007 **Cadillac Escalade**. After going through the cards several times he placed them back into his wallet. Agents then saw **R. CASTRO** and **LEON** enter and exit each pawn shop. On all occasions, both **R. CASTRO** and **LEON** entered the stores with nothing in their hands. When they left each store, **R. CASTRO** and **LEON** were not carrying anything in their hands. After they visited the last pawn shop, **R. CASTRO** and **LEON** drove back to **SIMPLE MOBILE**. Agents then watched as **R. CASTRO** and **LEON** went into **SIMPLE MOBILE** carrying a small stack of gift cards in their hands.

Delivery of Device-Making Equipment to SIMPLE MOBILE

28) On or about October 19, 2011, I received notification from Secret Service SA Oliver Grant (SA Grant), JFK Resident Office, that U.S. Customs officers had intercepted a package en route for delivery to **SIMPLE MOBILE**. The package was addressed to **R. CASTRO** at the street address of **SIMPLE MOBILE**. SA Grant told me that U.S. Customs officers inspected the package according to standard operating procedures and determined that the package contained a Wonder embossing machine, S/N 20101126. SA Grant supplied information that the embosser was shipped via U.S. Postal Service Express Mail, originating from China.

29) Embossers are commonly used in manufacturing credit cards, including in the production and use of counterfeit and unauthorized access devices. The Wonder embossing machine en route to **SIMPLE MOBILE** allows the user of the embosser to determine what credit card or account number is embossed on the front of a card. Based upon my knowledge and experience in this investigation, I know that such an embosser would allow the user of counterfeit and unauthorized access devices to create credit, debit, or gift cards on which the embossed number on the front of the card matched the stolen credit, debit, or account number re-encoded on the magnetic strip on the back of the card. Indeed, as already discussed in this affidavit, on June 4, 2011, **MALAGON** fraudulently used a Visa credit card account numbers to make purchases. Upon completion of the transaction, the cashier noticed that the last four (4) digits of the credit card number did not match the last four (4) digits of the credit card number on the receipt, which reflected the numbers re-encoded on the magnetic strip of the card. Upon questioning, **MALAGON** fled the scene. The use of the Wonder embossing machine to match

the embossed numbers to the re-encoded card would have prevented the store clerk from noticing the fraudulent use of the Visa number. The use of only a re-encoding machine, as described by the CS earlier in this affidavit, results in counterfeit and unauthorized cards on which the credit, debit, or account numbers re-encoded on the magnetic strip on the back of the card do not match the number embossed on the front of the card.

30) On November 1, 2011, agents with the USSS and United States Postal Service intend to conduct a controlled delivery of the above-mentioned Wonder embosser to **SIMPLE MOBILE**. Following the delivery of the embosser to **SIMPLE MOBILE**, agents intend to execute the search, seizure, and arrest warrants requested in this affidavit.

Use of Computer Equipment in the Manufacture of Fraudulent Access Devices

31) Through my experience and training, my knowledge of this investigation, and information provided to me by other law enforcement personnel and corporate investigators, I have learned that the access devices that have been utilized by the suspects in this investigation were compromised via the use of skimming devices. Through my experience and training, I have learned that skimming devices are temporarily attached to the interior of gas station pumps, which will read and record all credit card numbers that are "swiped" by that particular card reader. Further, the skimmers are later removed from the gas pump and then downloaded on a computer to retrieve the credit card numbers that have been fraudulently obtained.

32) Based on my training and experience, I know that when an individual uses a computer to obtain unauthorized access to a victim's credit card account information via downloading from skimmers, when an individual re-encodes cards with fraudulently obtained credit card numbers, or when an individual sells or purchases that information, or otherwise

transfers or acquires that information for use or dissemination, the computers involved will generally serve both as instrumentalities for committing the crime and also as a storage device for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage device for evidence of crime. Based upon my training and experience, I believe that a computer used to commit a crime of this type may contain records, data, and information relating to or reflecting, among other things, the following: how the computer was used, information that was sent or received, the manner in which crimes were committed using access devices, credit cards, and debit cards, ATM transactions, purchases, money withdrawals, money transfers, and other financial transactions, account information and the opening of accounts, passwords, access codes, user names, and other identifiers, ownership or use of the computers, and unauthorized access to accounts, websites, and computers.

33) Particularly, in the access device fraud scheme at issue in this affidavit, the participants in the scheme likely produced the access devices using credit card information obtained via skimmers. Once acquired, the information is entered into a credit card encoding machine. Computer software and files related to the encoding process remain on computers and computer storage devices for extended periods of time and are often recoverable using forensic techniques even if they are deleted by the users of the computer equipment.

34) As described above and in Attachment C, this application seeks permission to search for records that might be found at the **R. CASTRO RESIDENCE** and **SIMPLE MOBILE**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for

would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

35) I submit that if a computer or storage medium is found at the **R. CASTRO RESIDENCE** and **SIMPLE MOBILE**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c) Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from

operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."
- e) Based on actual inspection of other evidence related to this investigation, i.e. the access devices used to perpetuate the fraud in this case, I am aware that computer equipment was used to manufacture and use the counterfeit and unauthorized access devices used in the access device fraud scheme. There is reason to believe that there is a computer system currently located at the **R. CASTRO RESIDENCE** and **SIMPLE MOBILE**.

36) As further described in Attachment C, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the at the **R. CASTRO RESIDENCE** and **SIMPLE MOBILE** because:

- a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store

configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b) Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.
- c) A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d) The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend

on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e) Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

37) In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a) The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that

information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b) Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations.

Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

38) Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

39) **SIMPLE MOBILE** is a functioning company that agents believe conducts some legitimate business. The seizure of **SIMPLE MOBILE**'s computers may limit **SIMPLE MOBILE**'s ability to conduct its legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of **SIMPLE MOBILE** so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of **SIMPLE MOBILE**'s legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.³

Legal Authority for Seizure of Vehicles

38) As set forth in this affidavit, there is probable cause to believe that the **2007 Nissan Armada**, the **2007 Cadillac Escalade**, the **2006 Ford F150**, the **2005 Nissan Titan**, and the **2007 BMW** facilitated violations of 18 U.S.C. § 1029 and are, therefore, subject to criminal forfeiture by the United States, pursuant to 18 U.S.C. § 1029(c)(1)(C).

39) The Court's authority to order criminal forfeiture of property for violations of 18 U.S.C. § 1029 is found in 18 U.S.C. § 1029(c)(1)(C). Section 1029(c)(1)(C) provides for the criminal forfeiture of "any personal property used or intended to be used to commit" violations

³ To the extent that any computer equipment was used to facilitate the access device fraud scheme described in this affidavit, that computer equipment is subject to criminal forfeiture by the United States, pursuant to 18 U.S.C. § 1029(c)(1)(C).

of 18 U.S.C. § 1029. The Court may issue a seizure warrant for violations of 18 U.S.C. § 1029 pursuant to 21 U.S.C. § 853(f), as incorporated by 1029(c)(2).

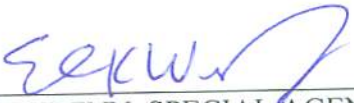
Conclusion

40) Through my experience and training, my knowledge of this investigation, and information provided to me by other law enforcement personnel and corporate investigators, I believe that **R. CASTRO, LEON, MALAGON, L. CASTRO, and MARTINEZ** are using illegally obtained credit card numbers and using those numbers fraudulently to purchase gift cards and other merchandise. **R. CASTRO**, along with **LEON, MALAGON, L. CASTRO, and MARTINEZ** has been observed making hundreds of transactions using fraudulently obtained credit card numbers. Further, I believe that **R. CASTRO** is using the illegally obtained credit card numbers to manufacture counterfeit credit cards at the **R. CASTRO RESIDENCE** and **SIMPLE MOBILE**. Moreover, **R. CASTRO, LEON, MALAGON, L. CASTRO, and MARTINEZ** have used the above-mentioned vehicles to commit this access device fraud.

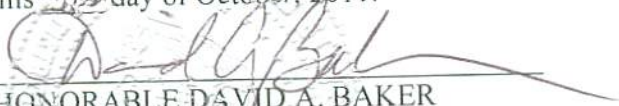
41) WHEREFORE, I attest that there is probable cause for a warrant to arrest, **R. CASTRO, LEON, L. CASTRO, MALAGON, and MARTINEZ**, and I believe that the items listed in Attachment C are located at **SIMPLE MOBILE** and the **R. CASTRO RESIDENCE**, more specifically described in Attachments A and B, respectively, and inside the **2007 Nissan Armada, the 2007 Cadillac Escalade, the 2006 Ford F150, 2005 Nissan Titan, and the 2007 BMW**, identified more fully in Attachments D,E, F,G, and H, respectively, and respectfully request that a search warrant be issued commanding myself or any other duly authorized law enforcement official to search those locations and vehicles and to seize such items as evidence and analyze them at another location, as they are evidence, fruits, and instrumentalities of

criminal violations of Title 18, United States Code, Sections 371 and 1029.

This concludes my affidavit.


ERNEST WRENN, SPECIAL AGENT
UNITED STATES SECRET SERVICE

Sworn and subscribed before me
this ~~31st~~ day of October, 2011.


HONORABLE DAVID A. BAKER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Description of Property to be Searched

SIMPLE MOBILE is a retail store located at 7612 Sun Vista Way, Orlando, FL. 32822. It is a single story business located in a retail shopping center at the southeast corner of the intersection of S. Goldenrod Road and Sun Vista Way, Orlando, FL. The business to be searched has a red brick front with a green sign immediately above the entry door that reads, "Simple Mobile Authorized Retailer, Unlimited Starting at \$40." The roof of the building is red. The numbers "7612" (black numbering with white background) are centered at the top of the entry door. There are additional cell phone advertisements affixed to the window and door.

ATTACHMENT B

Description of Property to be Searched

The **R. CASTRO RESIDENCE** is a single family home located at 4251 Anthony Lane, Orlando, FL 32822. It is a single-story, ranch style home, located on the northeast corner of the intersection of Anthony Lane and Yount Drive. The residence is tan with white borders around the windows and doors, and a gray roof. The numbers "4251" are affixed to a white boarder on the front right of the residence. There are two (2) single windows to the left of the door (facing from the street), and one (1) double window to the right of the front door. The back yard is covered by a 6' white vinyl privacy fence. The front yard is enclosed in a white vinyl picket fence, including a gate that covers the driveway.

ATTACHMENT C

Items to be Seized

All records and information that constitutes evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 371 (conspiracy) and 1029 (fraud and related activity in connection with access devices), including:

1. All credit, debit, and gift cards and all credit, debit, and gift card numbers, and any other items, records, or information that constitute evidence, fruits, or instrumentalities, of the production, manufacture, distribution, storage, transportation, and uttering, and of the conspiracy to do any of the fore-going, of counterfeit or unauthorized credit, debit, and gift cards and credit, debit, and gift card numbers:

2. Any computers or electronic media that were or may have been used as a means to commit the offenses described on the warrant, including to produce, manufacture, distribute, store, transport, and utter counterfeit or unauthorized credit, debit, and gift cards and credit, debit, and gift card numbers.

3. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;

- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks, cellular telephones, or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

ATTACHMENT D

Description of Vehicle to be Searched and Seized

White 2007 Nissan Armada. Florida License Plate AHSY36, Vehicle Identification Number 5N1AA08AX7N703435. The vehicle has tinted windows and after-market rims.

ATTACHMENT E

Description of Vehicle to be Searched and Seized

White 2007 Cadillac Escalade. Florida License Plate AHSX58. Vehicle Identification

Number 1GYFK63887R289038.

ATTACHMENT F

Description of Vehicle to be Searched and Seized

Black 2005 Nissan Titan, Florida License Plate S819NA. Vehicle Identification Number N6BA06A55N537945. The vehicle has after-market rims and a bed cover.

ATTACHMENT G

Description of Vehicle to be Searched and Seized

White 2006 Ford F150. Florida License Plate 800NJL, Vehicle Identification Number 1FTRX12526FA54665. The vehicle has after-market rims, bed cover, and spoiler.

ATTACHMENT H

Description of Vehicle to be Searched and Seized

**Black 2007 BMW, Florida License Plate AUHC53. Vehicle Identification Number
WBAHN83557DT68622.**