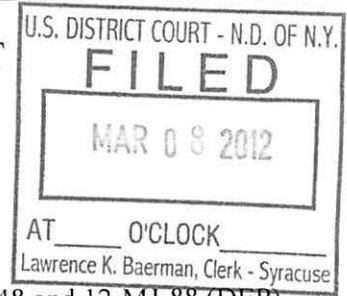


UNITED STATES DISTRICT COURT

for the Northern District of New York



In the Matter of the Search of (Briefly describe the property to be searched or identify the person by name and address)

Aspire Notebook Computer, SN: LUSEV0D01310440A121601; HTC Mobile Phone SN: SH175T505051; iPhone SN: 861324NWA4S; iPhone SN: 7U042CA2A4S; and Blackberry Cell Phone ESN#: 80DC5D47.

Case No. 12-MJ-48 and 12-MJ-88 (DEP)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Aspire Notebook Computer, SN: LUSEV0D01310440A121601; HTC Mobile Phone SN: SH175T505051; iPhone SN: 861324NWA4S; iPhone SN: 7U042CA2A4S; and Blackberry Cell Phone ESN#: 80DC5D47. Please see Attachment A. located in the Northern District of New York, there is now concealed (identify the person or describe the property to be seized): Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- X evidence of a crime; X contraband, fruits of crime, or other items illegally possessed; X property designed for use, intended for use, or used in committing a crime; a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Table with 2 columns: Code Section, Offense Description. Rows include Title 18, U.S.C. Section 1028A (Aggravated Identity Theft) and Title 18, U.S.C. Section 1029 (Fraud and Related Activity in Connection with Access Devices).

The application is based on these facts:

- X Continued on the attached sheet. Delayed notice of days (give exact ending date if more than 30 days: ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

John A. Szydluk, Special Agent Printed name and title

Sworn to before me and signed in my presence.

Date: Mar 8, 2012

Judge's signature

City and state: Syracuse, NY

Hon. David E. Peebles, U.S. Magistrate Judge Printed name and title

AUSA Ransom P. Reynolds

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF AN APPLICATION FOR A  
SEARCH WARRANT AUTHORIZING THE  
SEARCH OF:

- (1) **Aspire Notebook Computer, SN:  
LUSEV0D01310440A121601;**
- (2) **HTC Mobile Phone SN: SH175T505051;**
- (3) **IPhone SN: 861324NWA4S;**
- (4) **IPhone SN: 7U042CA2A4S; and**
- (5) **Blackberry Cell Phone ESN#: 80DC5D47.**

Case No. 12-MJ-48 (DEP)  
12-MJ-88 (DEP)

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Special Agent John A. Szydlik of the United States Secret Service, being duly sworn under oath, do hereby depose and state:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent with the United States Secret Service. I have been so employed since December 2007. I am currently assigned to the Syracuse Resident Office in Syracuse, New York. Among my duties are investigating electronic crimes specifically related to access device and identity theft violations pursuant to Title 18, United States Code, Sections

1028, 1028A, 1029, 1030 and similar sections. I have participated in investigations of persons suspected of committing fraud utilizing false information, identification documents, access devices, and computers. I presently serve on an Electronic Crimes Task Force (ECTF) designed to collaborate with other law enforcement agencies for the purpose of gathering intelligence and combating crimes committed utilizing computers and electronic media.

2. As a federal agent, your affiant is authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. This affidavit is being made in support of an application for a search warrant authorizing the search of the following items which together comprise the ("TARGET MEDIA"):

- a. Aspire Notebook Computer, SN: LUSEV0D01310440A121601;
- b. HTC Mobile Phone SN: SH175T505051;
- c. iPhone SN: 861324NWA4S;
- d. iPhone SN: 7U042CA2A4S; and
- e. Blackberry Cell Phone ESN#: 80DC5D47.

These items are set forth in Attachment A, and to seize and/or photograph any items set forth in Attachment B attached hereto, which constitute evidence, fruits and/or instrumentalities of access device fraud, in violation of Title 18, United States Code, Section 1029, and aggravated identity theft, in violation of Title 18, United States Code, Section 1028A.

4. The statements in this affidavit are based in part on my investigation of this matter and on information provided by other law enforcement agents, and others, as well as my personal observations and knowledge. Where statements of others are related herein, they are



related in substance and in part. Because this affidavit is being submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of a violation of 18 U.S.C. §§ 1028A and 1029 is located in located in the TARGET MEDIA.

**BACKGROUND ON ACCESS DEVICE FRAUD AS IT RELATES  
TO "CARDING" AND RE-ENCODED CARDS**

5. Through my training and experience I know that a common access device fraud scheme known as "Carding" involves the trade and use of illegally obtained personal identification information (PII) and stolen account numbers through online websites or via instant messenger services. These account numbers are both a Means of Identification as defined by 18 U.S.C. § 1028(d)(7)(D), and when fraudulently obtained are Unauthorized Access Devices as defined by 18 U.S.C. § 1029(e)(3)(D). "Carders" include hackers and their distributors who serve as vendors, as well as the consumers who purchase the stolen PII and account numbers and use them.

6. Through my experience I know that sellers and buyers of PII and stolen account numbers often interact and conduct transactions through instant messenger services or through websites created for the specific purpose of selling account numbers and PII. The price of account numbers varies by type and characteristics of the account and what type of corresponding PII accompanies it. Account numbers can cost as little as \$1.00 a piece or more than \$80.00 for desirable account types with full corresponding information. A popular commodity traded by Carders is known as a "Dump," which is the electronic copy of a credit or

debit card's magnetic stripe. Dumps often cost approximately \$20.00.<sup>1</sup> Once the buyer provides payment, vendors are able to directly transfer stolen account information and corresponding PII to consumers directly through the instant messenger service or website. Payment is generally conducted through Western Union money transfer or a similar service known as Liberty Reserve. These methods of payment are often preferred because they readily permit international transfers.

7. In my experience, once Carders purchase account numbers and PII they often save the information on their computer's hard drive or other electronic media because they may need to edit and organize it prior to use and distribution. They also often save the information because they don't want to risk losing it if their computer crashes and be forced to buy more.

8. Once Carders obtain the stolen account numbers and PII they are able to convert them to their specific illegal use. Carders use Dumps to create counterfeit credit or debit cards. This is often accomplished through a process known as re-encoding. Re-encoding occurs when a carder obtains a stored value gift card "gift card" or credit card with a magnetic stripe and uses a device known as an "encoder," which attaches to a computer via USB or other connection, and erases or overwrites the card's magnetic stripe transferring the Dump from the computer to the card's magnetic stripe. In my experience, gift card re-encoding is often preferred to counterfeiting or altering credit cards because gift cards generally lack several security features contained on normal credit and debit cards, making it easier to alter them and yet still appear to be an authentic looking access device.

9. The credit card industry has created common standards which govern what it calls, the "Payment System." The Payment System prescribes standards for how credit and

---

<sup>1</sup> Due to the black market nature of Carding, prices and the quality of product often vary widely.

debit cards are processed by merchants and what information is contained on the physical card itself. On standard credit cards, account information, including the account holder's name, account number and expiration date, are often embossed onto the front of the credit card. Most gift cards which are processed the same as credit cards, only have an account number and expiration date printed onto the front.

10. The Payment System terms "Card Present" transactions as those that are conducted face to face between a customer and merchant and a physical card is used to complete the transaction. A merchant processes a Card Present transaction by swiping the magnetic stripe of a customer's card through a card reader attached to a Point of Sale ("POS") Terminal. The magnetic stripe on the card contains two commonly used "Tracks" that contain machine readable information. The account name is usually only listed on Track 1 and the account number is usually listed on both Tracks 1 and 2. According to credit card industry specifications, the embossed or printed account number listed on the front of the card must match the account numbers encoded on the magnetic stripes. As a result, a card with mismatching account numbers constitutes a Counterfeit Access Device as defined by 18 U.S.C. § 1029(e)(2). Formatting and other discretionary data is also present on both Tracks. Only Track 2 is needed to process transactions through the electronic Payment System. Some POS Terminals may read Track 1 and print the account name to the receipt. When the card is swiped, most POS systems mask all of the account information except for the last four digits of the account number, which is often printed on the receipt as well. After the payment is approved, the merchant is then required to have the customer sign an authorization slip to complete the transaction. Several merchants have established anti-fraud policies. For example,



requiring customers to present a photo identification which matches the name listed on the card and verifying that the last four digits on the receipt match the last four digits printed on the card.

11. Many financial institutions have sophisticated fraud detection policies and mechanisms that allow them to rapidly identify compromised accounts and close them. This prevents further transactions to be processed on an account once fraud has been detected. In response to this countermeasure, Carders often use counterfeit access devices to purchase gift cards. In effect, the funds are removed from victim's account by the merchant selling the gift card to a gift card account usually operated by a separate financial institution. This added layer prevents victim financial institutions from tracing and reclaiming their funds.

12. As a result of the prevalence of re-encoded gift card fraud, many merchants have become suspicious of certain types of gift card transactions and have on occasion created their own safeguards to prevent fraud. To counter this, I have learned that Carders often attempt to spread their gift card purchases across multiple stores to avoid detection. They also generally limit the amount of gift cards they purchase at one store and may attempt to purchase other items to camouflage their actions. Carders have also been known to make multiple back to back purchases of gift cards using different re-encoded cards each time. They are also known to travel long distances, going from town to town along expressways, seeking out stores they are familiar with that sell gift cards. Carders also engage in this practice because it is difficult for store chains and law enforcement to recognize patterns in fraudulent activity when it is spread across many stores and jurisdictions. Through my experience, I know carders often use rental cars as a mode of transportation during these trips because they believe it is more difficult for law enforcement to track them.

### **BACKGROUND OF INVESTIGATION**

13. On December 17, 2011, an employee of Walgreens, in Cortland, New York, contacted the Cortland County 911 Center and reported that two males had attempted to purchase gift cards with other cards. During the transaction, the employee requested identification from both of the males, but they said they did not have any and left the store. The employee identified one of the cards used during the transaction as stolen and took down the license plate information on the male's vehicle as they departed. The vehicle, a Chevy Malibu bearing Arizona license plate AD4653 was later determined to have been registered by Hertz and rented to KAREEM HIGHSMITH for a period of one week.

14. Shortly thereafter, a Cortland County Sherriff's Deputy and a New York State Trooper located the Chevy Malibu in the parking lot at Tops in Cortland, New York. The officers then approached the vehicle and identified the occupants as KAREEM HIGHSMITH, MH, NT and GLENN FRANCIS. During a conversation with the occupants, the occupants stated that they had attempted to purchase gift cards at Walgreens. During the conversation, the officers asked the occupants if they had entered Tops. In response, the occupants stated that they had not entered Tops. However, the officers observed a Tops bag in plain view inside the vehicle. Thereafter, the officers entered Tops and spoke to the store manager. The officers learned that GLENN FRANCIS and KAREEM HIGHSMITH had purchased gift cards at Tops. After obtaining a copy of the receipt, the officers confronted the occupants of the vehicle with the receipt and informed them that Tops video surveillance captured KAREEM HIGHSMITH and GLENN FRANCIS purchasing gift cards. After being confronted with this information, FRANCIS removed three \$100.00 MasterCard gift cards from the driver door and handed them to the officers along with a receipt. The officers then asked FRANCIS where the credit card was that he used to purchase the gift cards. In response, FRANCIS stated that he paid cash and did



not use a credit card. The officers then informed FRANCIS that the Tops transaction receipt reflected that he had purchased the gift cards with a credit card, not cash. FRANCIS then admitted that he had used a credit card to purchase the gift cards but did not know which credit card he used or what he did with the credit card after the transaction. At this point, the officers asked GLENN FRANCIS to exit the vehicle and decided to interview the occupants separately.

15. The officers then interviewed KAREEM HIGHSMITH who was seated in the front passenger seat. During the interview, HIGHSMITH admitted that he had purchased gift cards and provided the officers with two \$100.00 gift cards that had been concealed in the glove box. The officers then asked HIGHSMITH where the credit card was that he used to purchase the gift cards. He stated that he did not know where it was. The officers asked HIGHSMITH to step out of the vehicle. Upon exiting the vehicle, HIGHSMITH handed the officers his wallet. During a search of HIGHSMITH's wallet, the officers located two credit cards that had his name embossed on them and neither of the two credit cards matched the credit card used to purchase the gift cards in Tops. The officers then asked HIGHSMITH if he had any other credit cards in his possession and HIGHSMITH consented to a search of his person. During a search of HIGHSMITH, the officers located 18 gift cards in HIGHSMITH's boot. Additionally, HIGHSMITH told police his address was 135 Didama Street, Syracuse, New York, 13224, and that his phone number was (315) 575-7592.

16. The officers did not search the vehicle. However, the officers did compare the recovered cards to the account number listed on the Tops receipt, but could not find any cards ending with same last four digits. The four subjects were then transported to the New York State Police barracks in Homer, New York, to be interviewed. At the conclusion of the interviews, all

four subjects departed and no charges were filed. The New York State Police maintained custody of all of the cards seized from the individuals.

17. On December 19, 2011, I examined the eighteen cards found in KAREEM HIGHSMITH's boot, as well as the two embossed cards located in his wallet with the name KAREEM HIGHSMITH. I determined that the account numbers encoded on the magnetic stripes of all twenty cards did not match any of the account numbers printed on the front of the twenty cards and that they were all counterfeit access devices. I have also determined the following:

- a. Six of the eighteen gift cards recovered from KAREEM HIGHSMITH's boot were issued by American Express, and the account numbers encoded on the magnetic stripes were also American Express account numbers. I provided this information to American Express investigator Alfred Cavuto. He stated that all of the account numbers encoded on the magnetic stripes belonged to individuals other than KAREEM HIGHSMITH.
- b. One of the two cards embossed with the name KAREEM HIGHSMITH was also an American Express card with a different American Express account encoded on it. Alfred Cavuto forwarded me the "Gift Card Order" detail records for the American Express card embossed in KAREEM HIGHSMITH's name. It was ordered on October 21, 2011, by KAREEM R HIGHSMITH at address 135 Didama St. Syracuse, New York, 13224, with a phone number listed as (315) 575-7592 (note: this is the same phone number he provided to the police on December 17, 2011).
- c. Alfred Cavuto was unable to identify the exact point of compromise for all of the account numbers in KAREEM HIGHSMITH's possession. However, he stated that it

appeared to be Carder activity because all of the victim account holders reside in different geographical areas.

- d. Additionally, after querying gift card servicer websites, I learned that one of the re-encoded gift cards had been purchased on August 18, 2011, at Wegman's in Erie, Pennsylvania, and another had been purchased the same day at a Wegman's in Amherst, New York.
- e. A card used by FRANCIS at Tops to purchase gift cards in two transactions for a total of \$217.85 contained the account number ending in 9728 and was determined to be issued to a person with initials H.A. by Capital One N.A. who provided a fraud affidavit to Capital One N.A. claiming not to have authorized the transactions and that he/she had retained possession of the Capital One card ending in 9728.

18. Thereafter, I searched archived video surveillance of unidentified suspected Carders that I had previously received from local merchants and law enforcement sources which contained photos of individuals making suspicious card transactions. During my video search, I searched for any video surveillance that depicted any of the four occupants of the vehicle. As a result of my search, I was able to identify KAREEM HIGHSMITH as the subject previously known only as "Prestige the CEO," that had been under investigation by the Electronic Crimes Task Force in Syracuse, New York, for card re-encoding since June 2011.

19. In December 2011, I learned that the Manlius Police Department (MPD) had an open criminal investigation involving KAREEM HIGHSMITH, GLENN FRANCIS, MAURICE PUGH, ET, MH and others which began in May of 2011. The MPD's investigation began after receiving a complaint from a person with initials T.M. who reported that he had lost his wallet on May 4, 2011, which contained three credit/debit cards. After losing his wallet, T.M. noticed



unauthorized charges on his accounts statement that were posted by Target, Walmart and other merchants in the Syracuse area. After receiving the complaint, MPD questioned the veracity of T.M.'s statement because they had information that he may have previously given others access to his accounts for the purpose of purchasing illegal drugs. During the investigation, officers from the MPD reviewed purchase logs and video surveillance from several of these stores pertaining to the charges made on T.M.'s accounts. After reviewing the logs and videos, MPD learned that the same group of individuals that had been using T.M.'s accounts to purchase gift cards also made other purchases using numerous accounts that did not belong to T.M. to also purchase gift cards and merchandise. Additionally, MPD learned from Target asset protection that the same group of individuals had been conducting similar activity at several other Target stores in the Syracuse area. From reviewing surveillance video, comparing it to MPD reports, and Facebook information I determined that:

- a. On May 4, 2011, at the Target located in Camillus, NY, KAREEM HIGHSMITH, FRANCIS, ET, PUGH, MH and one other person, entered the store.
  - i. Inside the store, FRANCIS used cards containing American Express (AMEX) account number's ending in 5268, 5511, and 4418 to make six separate transactions for gift cards. Francis also attempted to purchase a gift card using an account ending in 2503, but the transaction was declined. At Target, FRANCIS purchased a total of \$1,000.00 worth of gift cards.
  - ii. At Target, PUGH was observed on video using a card containing T.M.'s account ending in 2726 to purchase a gift card with a value of \$180.00. According to T.M., this was an unauthorized transaction.

iii. At Target, ET was observed using a card containing the AMEX account number ending in 8740 for two separate gift card transactions totaling \$200.00. At Target, ET attempted to use cards containing AMEX account number 2051, and T.M.'s accounts ending in 2796 and 7752, but the transactions were declined. At this point the full account numbers of the AMEX cards have not been obtained from Target and it is unknown if they were unauthorized transactions.

b. On May 5, 2011, PUGH was observed on video attempting to purchase gift cards at Walmart in Camillus, NY using T.M.'s accounts ending in 2726, 2796, and 7752, however the transactions were declined. According to T.M., all of these transactions were unauthorized.

20. On July 7, 2011, American Express reported that a card ending in 1005 issued to a person with initials O.M. who resides in Connecticut had \$5,158.00 worth of unauthorized charges posted to it, many of which occurred in the Syracuse area. KAREEM HIGHSMITH, who at the time was unidentified, was observed through store video surveillance using a card containing this account number to purchase gift cards on seven (7) separate occasions at various Price Chopper and Wegman's locations in the Syracuse, NY area from June 9, 2011 to June 13, 2011.

21. A source of information within the U.S. Postal Service has advised me that Change of Address forms for KAREEM HIGHSMITH and AW were filed on December 16, 2011. The forms indicate that they changed their address from 135 Didama St. Syracuse, NY, 13224, to 685 Hazelwood Avenue, Syracuse, NY, 13224.

22. On January 20, 2012, I observed a Nissan Maxima with Pennsylvania license plate HSS5061 parked in the driveway at 685 Hazelwood, Syracuse, NY 13224. A source at Hertz stated that the vehicle had been rented to KAREEM HIGHSMITH on January 19, 2012, and was due to return on January 26, 2012. The source stated HIGHSMITH'S address was listed as 135 Didama Street and that it appeared he had been renting vehicles through Hertz for one week at a time since at least December 2011.

23. On January 21, 2012, a Target receipt for the Webster, NY location from January 19, 2012, was located in a trash bag removed from the container located on the curb of 685 Hazelwood Ave. Syracuse, NY 13224. The receipt listed a purchase of a dvd using an AMEX account ending in 9001. A source of information at Target provided video surveillance and related transaction information. The video for this transaction depicts KAREEM HIGSMITH, along with an individual closely resembling PUGH, and a third unidentified individual at Target.

- a. According to transaction logs, HIGHSMITH used cards containing Visa accounts ending in 3926 and 9821, which were declined.
- b. The video depicts an individual closely resembling PUGH using a card containing an AMEX account ending in 4008 to purchase a gift card for \$106.00 and then attempting to purchase a \$50.00 gift card using cards containing the AMEX accounts ending in 4008, 8198, and 5064, all of which were declined.

24. On January 26, 2012, I observed a 2012 White Yukon with New York plate FAD7460 parked in the driveway of 685 Hazelwood Avenue, Syracuse, New York, 13224. A source of information from Hertz stated that this vehicle had been rented on January 26, 2012, by KAREEM HIGHSMITH with an address listed of 135 Didama Street, Syracuse NY, 13224.



25. On February 1, 2012, the trash along the curb of 685 Hazelwood Ave, Syracuse NY, 13224 was removed and examined. The contents included a counterfeit access device in the form of a Vanilla Visa gift card re-encoded with a Visa account number issued by FIA Card Services N.A. "(FIA)." Several empty Target gift card wrappers, an empty American Express gift card wrapper and a Victoria's Secret gift card were also found along with a torn up Western Union money transfer receipt was also found in the trash.

- a. According to a source of information at FIA, FIA had previously declared the account encoded on the Vanilla Visa gift card to be compromised and also stated that preceding the compromise the account was issued to a person with initials D.F. who lives in Maryland. FIA also provided a list of fraudulent transaction attempts on D.F.'s account (which was encoded on the back of the Vanilla Visa gift card) which occurred on January 19, 2012, including two attempts at a Wal-Mart in Victor, NY, and one attempt each at a Wegmans in Webster, NY and Penfield, NY.
  - i. A source of information at Wal-Mart provided video surveillance screen shots of KAREEM HIGHSMITH, PUGH, and an unidentified individual entering the store. Inside Wal-Mart, one of the individuals attempted to use a card containing the account issued to D.F to purchase an IPAD. However, the transaction was declined.
  - ii. A source of information at Wegman's was able to provide a surveillance video depicting the same three individuals inside Wegman's. The video shows the unidentified individual attempting to use the card containing D.F.'s account number to make a purchase, but it was declined. At the

same time, the video surveillance shows PUGH attempting to purchase gift cards, but the transaction was declined.

- b. The Western Union money order receipt located in the trash detailed a transfer conducted at a Price Chopper store in Syracuse, NY on January 23, 2012. The transfer amount was \$530.00 and was sent from "Mister Swagg" to an individual in Russia. A source of information at Price Chopper was able to determine a similar transaction occurred on January 17, 2012 with the same amount, sender and recipient. The source examined video surveillance of the transactions and provided footage showing KAREEM HIGHSMITH making the transfers. For the January 23, 2012, Western Union transaction, HIGHSMITH was transported to the Price Chopper in a vehicle resembling a dark colored Chevy Malibu. During that transaction, the driver remained in the vehicle and waited while HIGHSMITH conducted the transaction. Approximately one hour prior to the transfer, a Chevy Malibu bearing Massachusetts plate, 969PH5 registered to Hertz was observed parked outside 685 Hazelwood Ave. Syracuse, NY 13324. A source of information at Hertz stated the vehicle had been rented to a person with initials D.S. of Syracuse, NY.

26. On February 1, 2012 the tracking device affixed to the 2012 White Yukon (rented by KAREEM HIGHSMITH), reported that the vehicle was in the vicinity of the same Price Chopper in Syracuse, NY. Thereafter, the source at Price Chopper was able to determine through video surveillance that KAREEM HIGHSMITH and another occupant met PUGH who arrived at the store in a dark car matching the description of the 2011 Chevy Malibu observed on January 23, 2012. According to the source, one of the occupants of the Yukon received a

Western Union wire transfer sent to KAREEM HIGHSMITH from an individual in Brooklyn, NY. PUGH and the other Yukon occupant sent Western Union wire transfers to two different individuals in Russia. PUGH and the other Yukon occupant sent the two separate wire transfers using the names SW and SC. One transfer was for \$180.00 and the other was for \$430.00.

27. On February 2, 2012, KAREEM HIGHSMITH was observed parking the 2012 White Yukon in the lot at Skyline apartments located at 753 James St. Syracuse, NY 13203 and entering with a back pack. Approximately one hour later, HIGHSMITH (without the backpack) and PUGH emerged from the building and drove away in the 2012 white Yukon. Approximately one hour later, HIGHSMITH and PUGH returned to Skyline in the Yukon. Thereafter, PUGH exited the Yukon and drove off in a Chevy Malibu bearing Massachusetts plate 969PH5 which was parked in the parking lot. HIGHSMITH then departed in the white Yukon.

28. A source of information at the U.S. Postal Service stated that PUGH receives mail at Skyline Apartment # 232 located at 753 James St. Syracuse, NY 13203. A manager at Skyline Apartments confirmed that PUGH rents apartment 232 and is the only one listed on the lease.

29. On February 6, 2012, KAREEM HIGHSMITH was observed at a Price Chopper in Syracuse, NY purchasing a Western Union money order/wire transfer for \$990.00 to the same individual in Russia as the money orders on January 17<sup>th</sup> and 23<sup>rd</sup>. HIGHSMITH listed his name as SC on the money order form.

30. On February 13, 2012, GLENN FRANCIS was apprehended pursuant to a Federal Arrest Warrant, inside of Room 355, United Inn 1308 Buckley Rd. Syracuse, NY. FRANCIS was asked for his identification and he stated it was in his wallet in his pant pocket. Upon retrieving the ID, nine gift cards were immediately visible in the wallet. One of the cards



was found to be counterfeit as the account number listed on the front did not match the one encoded on the back.

31. On February 13, 2012, during the execution of a Federal Arrest Warrant on GLENN FRANCIS at Room 355, United Inn 1308 Buckley Rd. Syracuse, NY. KERVON WARRICK was also located in the room. KERVON WARRICK was asked for identification and stated his wallet was in his pants pocket. Upon retrieving the ID, numerous gift cards and credit cards were visible in WARRICK's wallet. The account numbers listed on 11 of the cards in Warrick's wallet did not match the account number on the magnetic stripe. A genuine AMEX reloadable gift card ending in \*7672 was also located in the wallet. During a sweep of Room 357, which was connected to 355 with an open door, 16 Target gift cards and various receipts were found in an open bag. The receipts showed the following purchases:

- a. Purchase at True Religion in Garden City, NY on February 11, 2012 for \$954.42. According to the receipt an AMEX gift card with the last for \*7672
- b. Purchase at Polo Ralph Lauren in Tannersville, PA on February 6, 2012 for \$149.99. According to the receipt an AMEX gift card with the last for \*7672

32. When agents arrived FRANCIS and WARRICK were laying on separate twin beds in the hotel room. On the night stand between them was a HTC Mobile Phone bearing SN: SH175T505051 and a iPhone bearing SN: 7U042CA2A4S. A Blackberry Cell Phone bearing ESN#: 80DC5D47 was also located on the floor. FRANCIS told agents the HTC Phone was his. WARRICK stated the Blackberry and the iPhone were his.

33. KERVON WARRICK gave consent for the search of his Chrysler 300 rental car that he drove with GLENN FRANCIS and one other from Brooklyn, NY to Syracuse NY in. A jacket was found in the trunk of the car that KERVON WARRICK later stated was his. In the

jacket four counterfeit cards that had different account numbers listed on the front and magnetic stripe of each card were found. Three of the cards had the name KERVON WARRICK printed on them. An Aspire Notebook Computer, bearing SN: LUSEV0D01310440A121601 was found in the trunk of the vehicle. FRANCIS stated the computer belonged to him. An iPhone bearing SN: 861324NWA4S with a damaged screen was located by on the center console area of the passenger compartment; WARRICK stated this Iphone was his.

34. KERVON WARRICK waived his Miranda Rights and agreed to be interviewed. He stated that a month ago GLENN FRANCIS told him that he could get gift cards for him if WARRICK provided FRANCIS with his credit cards. WARRICK stated he gave Francis a total of five credit cards which FRANCIS returned to him. WARRICK said he used the gift cards to purchase clothing and Target gift cards. WARRICK denied knowing the cards were counterfeit.

**SPECIFICS REGARDING THE SEIZURE AND SEARCHING OF COMPUTER SYSTEMS**

35. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, cellular phones, magnetic tapes, memory chips and other portable and removable media. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

- a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer

hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

- b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted or password protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.
- c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of a premises. A single megabyte of storage space is the equivalent of 500 double spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double spaced pages of text. Storage devices capable of storing 160 gigabytes (“GB”) of data are now commonplace in desktop computers. Consequently, each non networked, desktop computer found during a search can easily contain the equivalent of 80



million pages of data, which, if printed out, would result in a stack of paper over four miles high.

- d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.
- e. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is

overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – 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. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

36. In light of these concerns, I hereby request the Court’s permission to search, copy, image and seize the electronic media and computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an offsite search of the image or hardware for the evidence fruits and instrumentalities of violations of the Specified Federal Offenses.

**THE APPLICATION FOR A SEARCH WARRANT**

37. Based on all of the foregoing facts, I submit that there is probable cause to believe that a search of the TARGET MEDIA will lead to the discovery of the items described in

Attachment B (incorporated by reference herein), all of which constitute evidence, fruits, and/or instrumentalities of a violation of Title 18, United States Code, Section 1029, and aggravated identity theft, in violation of Title 18, United States Code, Section 1028A.

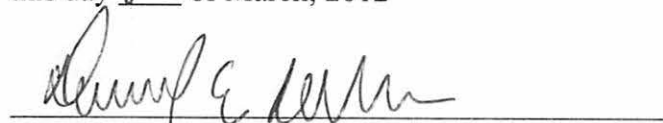
38. WHEREFORE, deponent requests that a warrant be issued, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, to search the TARGET MEDIA for the items and information set forth in Attachment B.

Respectfully submitted,



JOHN A. SZYDLIK  
Special Agent  
United States Secret Service

Subscribed and sworn to before me  
this day 8<sup>th</sup> of March, 2012

  
HON. DAVID E. PEEBLES  
UNITED STATES MAGISTRATE JUDGE



**ATTACHMENT A**  
**TARGET MEDIA to be searched**

This warrant applies to the following devices currently held by the US Secret Service, in Syracuse NY:

- (1) **Aspire Notebook Computer, SN: LUSEV0D01310440A121601;**
- (2) **HTC Mobile Phone SN: SH175T505051;**
- (3) **IPhone SN: 861324NWA4S;**
- (4) **IPhone SN: 7U042CA2A4S; and**
- (5) **Blackberry Cell Phone ESN#: 80DC5D47.**

## ATTACHMENT B

ITEMS TO BE SEIZED, ALL OF WHICH CONSTITUTE EVIDENCE, FRUITS AND INSTRUMENTALITIES OF ACCESS DEVICE FRAUD, FROM THE TARGET MEDIA:

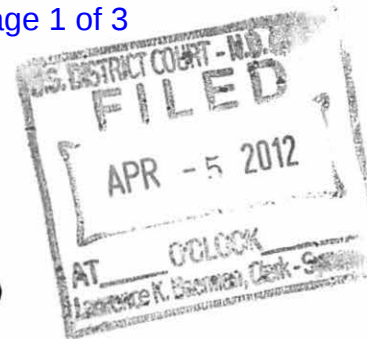
1. The evidence, fruits and instrumentalities of access device fraud, that may be seized from the TARGET MEDIA are the following:
  - a. Any Access Device, or Means of Identification of another ;
  - b. Any access device manufacturing implements or materials, to include encoders, embossers and cards;
  - c. Any receipt or document in any form showing the use of access devices to purchase goods or services;
  - d. Any receipt, document or card in any form used for the purpose of or documenting the transfer of funds;
  - e. Any packaging or correspondence used to transfer items between
  - f. Any geo-locational information;
  - g. Any stored communication in any form between pertaining to the use of unauthorized access devices or other supporting activities;
  - h. Any photograph, calendar entry, or other item in any format that directly or indirectly relates to the use of unauthorized access device or other supporting activities.;
  - i. Any electronic or optical storage devices capable of storing credit, debit or other account information or numbers;
  - j. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or data stored on the digital device.
  
2. The evidence, fruits and instrumentalities of access device fraud, that may be contained in the TARGET MEDIA are the following:
  - a. Computer hardware and "smart phones", meaning any and all computer equipment or "smart phones" including all electronic devices which are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar

computer impulses or data. Included within the definition of computer hardware is a laptop computer;

- b. Computer software, meaning any and all information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software includes data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components;
  - c. Computer passwords and data security devices, meaning any devices, programs, or data – whether themselves in the nature of hardware or software – that can be used or are designed to be used to restrict access to, or facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, without limitation, data security hardware or information (such as encryption devices, chips, and circuit boards); passwords, data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into useable forms;
  - d. Any electronic information or data, stored in any form, which has been used or prepared for us either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), or any computer or computer system. The form such information might take includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, video cassettes, and other media capable of storing magnetic or optical coding.
3. In searching for data capable of being read, stored or interpreted by a wireless phone or computer, law enforcement personnel executing this search warrant will employ the following procedures:
- a. Surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
  - b. Opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
  - c. Scanning storage areas to discover and possibly recover recently deleted files;



- d. Scanning storage areas for deliberately hidden files;
- e. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation;
- f. In conducting the search of any computer, electronic storage device, closed, or locked container authorized by this Search Warrant, the government shall make reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information which are identified in the Search Warrant itself.



IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF NEW YORK

IN RE ORDER REQUIRING APPLE, INC.  
TO ASSIST IN THE EXECUTION OF A  
SEARCH WARRANT ISSUED BY THIS  
COURT

Case No. **12- MJ-48 (DEP)**

APPLICATION

**INTRODUCTION**

The United States of America, by and through Richard Hartunian, United States Attorney, and Ransom Reynolds, Assistant United States Attorney, hereby moves this Court under the All Writs Act, 28 U.S.C. § 1651, for an order requiring Apple, Inc. to assist the United States Secret Service in the execution of a federal search warrant by bypassing the lock screen of two iOS devices, specifically, two iPads.

**FACTS**

The United States Secret Service currently has in its possession two iOS devices that were seized pursuant to a search warrant issued by this Court on March 8, 2012. An initial inspection of the iOS devices revealed that that they are locked. Because the iOS devices are locked, law enforcement agents are not able to examine the iOS devices as commanded by the search warrant.

The iOS devices are two iPads with the following identifiers:

1. Model #A1337, serial number HW107EANETV, and FCC ID#BCG-E2328A;  
and
2. Model #A1397, serial number DLXFC1SYDJHH, and FCC ID#BCGA1397.

Apple, Inc., the creator of the iOS operating system and producer of the iOS device, may have the capability of bypassing the iOS devices' locks. This Application seeks an Order requiring Apple to use any such capability, so as to assist agents in complying with the search warrant.

### DISCUSSION

The All Writs Act provides that “[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.” 28 U.S.C. § 1651(a). As the Supreme Court explained, “[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute.” *Pennsylvania Bureau of Correction v. United States Marshals Service*, 474 U.S. 34, 43 (1985). “The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice... and encompasses even those who have not taken any affirmative action to hinder justice.” *United States v. New York Tel. Co.*, 434 U.S. 159, 174 (1977). Specifically, in *United States v. New York Tel. Co.*, the Supreme Court held that the All Writs Act permitted district courts to order a telephone company to effectuate a search warrant by installing a pen register. Consequently, this Court has the authority to order Apple, Inc., to use any capabilities it may have to unlock the iOS devices.


The government is aware, and can represent, that in other cases, courts have ordered the unlocking of an iPhone under this authority. Additionally, Apple has routinely complied with such orders, and has suggested specific language for such orders.



This Court should issue the Order because doing so would enable agents to comply with this Court's warrant commanding that the iOS devices be examined for evidence identified by the warrant. Examining the iOS devices without Apple's assistance, if at all possible, would require significant resources and may harm the iOS devices. Moreover, the Order is not likely to place any unreasonable burden on Apple.

Respectfully submitted this 5<sup>th</sup> day of April, 2012

RICHARD S. HARTUNIAN  
United States Attorney



---

Ransom P. Reynolds  
Assistant United States Attorney  
Bar Roll No. 512035

IN THE UNITED STATES DISTRICT COURT  
FOR NORTHERN DISTRICT OF NEW YORK

IN RE ORDER REQUIRING APPLE, INC.  
TO ASSIST IN THE EXECUTION OF A  
SEARCH WARRANT ISSUED BY THIS  
COURT

Case No. 12- MJ-48 (DEP)

**ORDER**



Before the Court is the Government's Application for an Order requiring Apple, Inc. to assist law enforcement agents in the search of two Apple iOS devices. Upon consideration of the motion, and for the reasons stated therein, it is hereby

ORDERED that Apple Inc. assist law enforcement agents in the examination of:

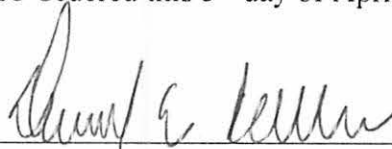
1. iPad with Model #A1337, serial number HW107EANETV, and FCC ID#BCG-E2328A,  
and
2. iPad with Model #A1397, serial number DLXFC1SYDJHH, and FCC ID#BCGA1397  
(the "iOS devices"); and it is hereby

FURTHER ORDERED that Apple shall provide reasonable technical assistance to enable law enforcement agents to obtain access to unencrypted data ("Data") on the iOS devices, and to bypass the passcode; and it is hereby

FURTHER ORDERED that, to the extent that data on the iOS devices is encrypted, Apple may provide a copy of the encrypted data to law enforcement, but Apple is not required to attempt to decrypt, or otherwise enable law enforcement's attempts to access any encrypted data; and it is hereby

FURTHER ORDERED that although Apple shall make reasonable efforts to maintain the integrity of data on the iOS Device, Apple shall not be required to maintain copies of any user data as a result of the assistance ordered herein; all evidence preservation shall remain the responsibility of law enforcement agents.

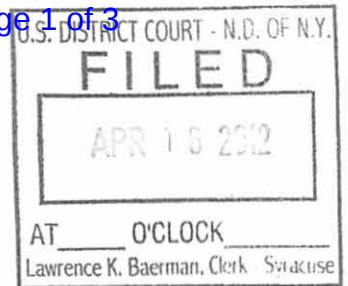
So Ordered this 5<sup>th</sup> day of April, 2012.

A handwritten signature in black ink, appearing to read "David E. Peebles", written over a horizontal line.

Hon. David E. Peebles

United States Magistrate Judge





IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF NEW YORK

IN RE ORDER REQUIRING APPLE, INC.  
TO ASSIST IN THE EXECUTION OF A  
SEARCH WARRANT ISSUED BY THIS  
COURT

Case No. **12- MJ-48 (DEP)**

**APPLICATION**

**INTRODUCTION**

The United States of America, by and through Richard Hartunian, United States Attorney, and Ransom Reynolds, Assistant United States Attorney, hereby moves this Court under the All Writs Act, 28 U.S.C. § 1651, for an order requiring Apple, Inc. to assist the United States Secret Service in the execution of a federal search warrant by bypassing the lock screen of two iPads.

**FACTS**

The United States Secret Service currently has in its possession two iPads that were seized pursuant to a search warrant issued by this Court March 8, 2012. An initial inspection of the iPads revealed that that they are locked. Because the iPads are locked, law enforcement agents are not able to examine the iPads as commanded by the search warrant.

The two iPads have the following identifiers:

1. iPad, Black, Model #A1337, FCC ID#BCG-E2328A and IC: 579C-E2328A, IMEI: 012438003440250, serial HW107EANETV, and;
2. iPad, Black, Model #A1397, FCC ID#BCGA1397, MEID: A100001CB088EA, and serial DLXFC1SYDJHH, (the "iPads").

Apple, Inc., the creator of the iPads operating system and producer of the iPad device, may have the capability of bypassing the iPads' locks. This Application seeks an Order requiring Apple to use any such capability, so as to assist agents in complying with the search warrant.

### DISCUSSION

The All Writs Act provides that “[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.” 28 U.S.C. § 1651(a). As the Supreme Court explained, “[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute.” *Pennsylvania Bureau of Correction v. United States Marshals Service*, 474 U.S. 34, 43 (1985). “The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice... and encompasses even those who have not taken any affirmative action to hinder justice.” *United States v. New York Tel. Co.*, 434 U.S. 159, 174 (1977). Specifically, in *United States v. New York Tel. Co.*, the Supreme Court held that the All Writs Act permitted district courts to order a telephone company to effectuate a search warrant by installing a pen register. Consequently, this Court has the authority to order Apple, Inc., to use any capabilities it may have to unlock the iPads.

The government is aware, and can represent, that in other cases, courts have ordered the unlocking of an iPad under this authority. Additionally, Apple has routinely complied with such orders, and has suggested specific language for such orders.

This Court should issue the Order because doing so would enable agents to comply with this Court's warrant commanding that the iPads be examined for evidence identified by the warrant. Examining the iPads without Apple's assistance, if at all possible, would require significant resources and may harm the iPads. Moreover, the order is not likely to place any unreasonable burden on Apple.

Respectfully submitted this 16<sup>th</sup> day of April, 2012

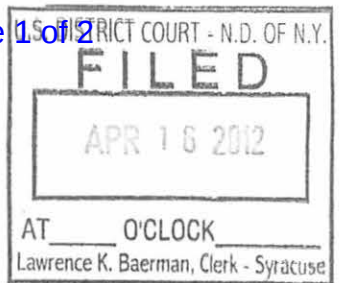
RICHARD S. HARTUNIAN  
United States Attorney



---

Ransom P. Reynolds  
Assistant United States Attorney  
Bar Roll No. 512035





IN THE UNITED STATES DISTRICT COURT  
FOR NORTHERN DISTRICT OF NEW YORK

IN RE ORDER REQUIRING APPLE, INC.  
TO ASSIST IN THE EXECUTION OF A  
SEARCH WARRANT ISSUED BY THIS  
COURT

Case No. **12- MJ-48 (DEP)**

**ORDER**

Before the Court is the Government's motion for an Order requiring Apple, Inc. to assist law enforcement agents in the search of two Apple iPads. Upon consideration of the motion, and for the reasons stated therein, it is hereby

ORDERED that Apple Inc. assist law enforcement agents in the examination of:

1. one iPad, Black, Model #A1337, FCC ID#BCG-E2328A and IC: 579C-E2328A, IMEI: 012438003440250, serial HW107EANETV; and
2. one iPad, Black, Model #A1397, FCC ID#BCGA1397, MEID: A100001CB088EA, and serial DLXFC1SYDJHH, (the "iPads"); and it is hereby

FURTHER ORDERED that Apple shall provide reasonable technical assistance to enable law enforcement agents to obtain access to unencrypted data ("Data") on the iPads; and it is hereby

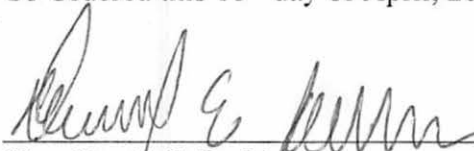
FURTHER ORDERED that, to the extent that data on the iPads are encrypted, Apple may provide a copy of the encrypted data to law enforcement but Apple is not required to attempt to decrypt, or otherwise enable law enforcement's attempts to access any encrypted data; and it is hereby

FURTHER ORDERED that, Apple's reasonable technical assistance may include, but is not limited to, bypassing the iPads users' passcode so that the agents may search the iPads,

extracting data from the iPads and copying the data onto an external hard drive or other storage medium that law enforcement agents may search, or otherwise circumventing the iPads' security systems to allow law enforcement access to Data and to provide law enforcement with a copy of encrypted data stored on the iPads; and it is hereby

FURTHER ORDERED that, although Apple shall make reasonable efforts to maintain the integrity of data on the iPads, Apple shall not be required to maintain copies of any user data as a result of the assistance ordered herein; all evidence preservation shall remain the responsibility of law enforcement agents.

So Ordered this 16<sup>th</sup> day of April, 2012.

A handwritten signature in black ink, appearing to read "David E. Peebles", written over a horizontal line.

Hon. David E. Peebles

United States Magistrate Judge