UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

United States of America
v.
NASCHANCY JOHNNY COLBERT

Case No. 3:14mj16

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of June 13, 2012 - December 4, 2013 in the county of Mecklenburg in the Western District of North Carolina, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1349	Conspiracy to Commit Mail Fraud (18 USC 1341), Wire Fraud (18 USC 1343) and Bank Fraud (18 USC 1344)

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT

☑ Continued on the attached sheet.

Randy Berkland
Complainant's signature

Postal Inspector Randy Berkland
Printed name and title

Sworn to before me and signed in my presence.

Date: 1-17-14

Judge's signature

City and state: Charlotte, North Carolina

David S. Cayer, United States Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA

STATE OF NORTH CAROLINA :
: ss
COUNTY OF MECKLENBURG :

RANDY BERKLAND, being duly sworn, deposes and says:

1. I am an Inspector with the United States Postal Inspection Service and have served in that position for approximately ten years. I have been trained in various aspects of law enforcement, including the investigation of access device fraud, bank fraud, mail fraud, wire fraud, identity theft, and computer crimes. In addition, I have received training regarding investigating the use of the United States mail and other overnight and rapid delivery services to facilitate the distribution of contraband. During my employment, I have been involved in over two hundred investigations, including those involving the execution of searches and controlled deliveries. During my tenure, I have participated in over fifty searches.

2. This Affidavit is submitted in support of a Criminal Complaint and Arrest Warrant for **NASHANCY JOHNNY COLBERT ("COLBERT")** for conspiracy, in violation of Title 18, United States Code, Section 1349, to commit mail fraud (18 USC § 1341), wire fraud (18 USC § 1343) and bank fraud (18 USC § 1344). Since this Affidavit is submitted for the limited purpose of establishing probable cause in support of a criminal complaint, I have not included each and every fact known to me concerning this investigation.

3. I am thoroughly familiar with the information contained in this Affidavit based upon my personal involvement in this criminal investigation, information relayed to me by other law enforcement officers and other witnesses, and my review of various documents and records.

THE CRIMINAL INVESTIGATION

A. Stolen Payment Card Data – Initiation of Federal Investigation

4. In December 2012, I received information from the Rutherfordton Police Department ("RPD") regarding the arrest of two individuals on state charges involving stolen payment card account numbers and counterfeit credit and debit cards. Based on this information, the United States Postal Inspection Service-Charlotte Office ("USPIS-Charlotte") and the United States Secret Service-Charlotte Office ("USSS-Charlotte") commenced a federal criminal investigation which has led to the identification and takedown of a domestically-operated Internet website that trafficked in counterfeit credit and debit cards, and authentication features for false identification documents, along with the arrests of the website's operator and its employees in the Middle District of Florida. As set forth more fully below, **NASHANCY JOHNNY COLBERT ("COLBERT")** was a member and customer of the illegal Internet website (the "Fake Plastic Website") and purchased approximately 231 counterfeit payment cards from the Fake Plastic Website beginning only sixteen (16) days after his release from state jail in September 2013 for **COLBERT**'s prior conviction for state charges involving the use of stolen payment card account information.

5. Information obtained from the RPD revealed that on December 6, 2012, a Food Lion grocery store clerk in Rutherfordton, North Carolina, observed a store customer, identified herein as L.B., attempt to pay for pre-paid gift and pre-paid debit cards by "swiping" approximately eight (8) magnetic-stripe plastic credit or debit payment cards (later determined to be encoded with stolen credit or debit card numbers) through the store's point-of-sale (POS) payment card terminal. Each of L.B.'s initial card "swipes" on Food Lion's POS terminal was declined for payment during the payment authorization process. L.B then swiped two (2) magnetic-stripe plastic credit or debit cards on Food Lion's POS terminal that resulted in successful payment authorizations for the

purchase of approximately $1,200's worth of pre-paid gift and pre-paid debit cards. Food Lion's POS payment system transmits and causes to be transmitted by wire communications in interstate commerce writings, signs, signals and sounds in connection with payment card transactions, including payment card account information and payment authorization or payment declination by the card payment networks (i.e. VISA, MasterCard, American Express and Discover) and payment card issuer, typically a financial institution or financial services company.

6. After L.B. departed the store, a Food Lion employee reported the suspicious declined payment transactions to the RPD, which later stopped a vehicle occupied by L.G. and a driver, identified herein as Confidential Witness Number 1 (CW1). During the vehicle stop, the RFD recovered forty-five (45) genuine unused pre-paid gift cards totaling $12,000 contained in original packaging; nine (9) Nordstrom gift cards totaling $1,800; thirteen (13) magnetic-stripe embossed payment cards that appeared to be counterfeit or altered and included the name of L.B; and a counterfeit Ohio driver's license bearing the name and photograph of L.B.

7. On December 18, 2012, USSS-Charlotte Special Agent (S/A) R. Matt Hayes and I examined the thirteen (13) magnetic-stripe credit and debit cards seized by RPD from the vehicle occupied by L.B. and CW1. The examination revealed that the magnetic stripes of the seized payment cards were encoded with thirteen different 16-digit debit or credit card numbers, and that at least nine (9) of the thirteen (13) account numbers on the payment cards were found to be stolen or compromised debit or credit card numbers. The nine (9) true payment card account holders advised S/A Hayes that they each still possessed their genuine credit or debit cards and that their respective payment card issuers had advised them of unauthorized card usage by unknown persons to purchase pre-paid gift or pre-paid debit cards. L.B.'s name contained on L.B's seized counterfeit Ohio driver's license bearing L.B.'s photograph was embossed on ten (10) of the

thirteen (13) magnetic-stripe counterfeit plastic debit or credit cards containing multiple stolen or compromised payment card account numbers. Based on my training and experience and information gathered in this investigation, the thirteen (13) plastic counterfeit payment cards each contained at least one counterfeit mark identical with or substantially indistinguishable from marks in use and registered to one or more of the various payment association networks (i.e., Visa, MasterCard, American Express, Discover) in the principal register of the United States Patent and Trademark Office.

B. Use of the U.S. Mail for Trafficking in Counterfeit Payment Cards

8. On February 14, 2013, federal search warrants were executed at the residences of L.B. and CW1. The search of CW1's residence yielded approximately twenty-two (22) counterfeit payment cards that were embossed with CW1's name, but which did not contain any payment card account numbers encoded on the magnetic stripes of the counterfeit payment cards.

9. Evidence seized from CW1's residence included an opened and discarded Express Mail envelope with a pre-printed postal mailing label addressed to CW1's residence in the name of L.B. and bearing a unique USPS tracking number. The label also contained a return address located in Melbourne, Florida.

10. CW1 agreed to cooperate at the time of the search and advised me that the twenty-two (22) counterfeit payment cards seized from CW1's residence had been delivered in the discarded Express Mail envelope. CW1 had ordered the seized counterfeit payment cards from the Internet after having purchased stolen payment card accounts numbers and corresponding payment account data from unknown individuals on the Internet using an instant messaging computer program known as ICQ. CW1 advised that the unknown individuals selling stolen payment card

account information on ICQ also referred CW1 to a website that sold fake plastic credit and debit cards, hereinafter referred to as the "Fake Plastic Website."

11. According to CW1, the Fake Plastic Website sold unembossed or custom-embossed counterfeit magnetic-stripe credit and debit cards for use with the stolen and compromised credit card and debit card account numbers.

12. Using CW1's computer, CW1 showed me the Fake Plastic Website that CW1 had used to order and purchase counterfeit credit and debit cards. In my presence and at my request, CW1 logged onto the Fake Plastic Website using CW1's unique user ID and password. I then reviewed the Fake Plastic Website and established an undercover user ID and password to later access the Fake Plastic Website during the investigation.

13. During the investigation, I reviewed various web pages on the Fake Plastic Website and observed several web pages that displayed numerous photographs of various credit card styles and backgrounds containing one or more trademarks of bank payment networks (i.e. Visa, MasterCard, American Express and Discover) and card-issuing banks, such as Bank of America. **See EXHIBIT A.** I also observed a customer order web page on the Fake Plastic Website that enabled customers to enter credit card and debit card account numbers, cardholder names and card expiration dates to be custom embossed onto counterfeit credit and debit cards offered for sale on the Fake Plastic Website. **See EXHIBIT B.** I also observed a web page that enabled Fake Plastic Website customers to order counterfeit holograms for use on counterfeit payment cards. **See EXHIBIT C.**

C. <u>Counterfeit Payment Cards Sold Through the Fake Plastic Website</u>

14. In March 2013, I learned that the USPIS-New Jersey and the Federal Bureau of Investigation in New Jersey ("FBI-New Jersey") had an open investigation on the Fake Plastic

Website. Since that time, USPIS-Charlotte, USSS-Charlotte, USPIS-New Jersey and FBI-New Jersey have worked together to conduct a joint criminal investigation of the Fake Plastic Website, its operator and its employees. The joint criminal investigation revealed that the Fake Plastic Website was a large-scale seller of (i) customized counterfeit credit and debit cards (referred to herein as counterfeit "payment cards"), and (ii) authentication features for false identification documents.

15. As a result of the multi-agency federal investigation, the Fake Plastic Website's operator and its employees were arrested by federal law enforcement agents on December 4, 2013. Additionally, federal law enforcement agents executed multiple search warrants that, in pertinent part, resulted in the seizure of equipment and materials used to manufacture counterfeit payment cards and a large stock of false authentication features for application to false identification documents, such as counterfeit state driver's licenses. **See EXHIBIT D.**

16. The Fake Plastic Website was a one-stop shop for various "carding" or "cash out" crews across the country. Based on my training and experience and that of other law enforcement agents involved in this investigation, these crews obtain stolen payment card track data,[1] or "dumps," through a number of varied schemes, including various payment card skimming operations[2] and hacking, designed to illegally acquire other people's payment card numbers and related data. Once the stolen payment card track data is acquired, criminals seeking to monetize

---

1 "Track data" refers to data that is encoded on the magnetic stripe on the back of a credit or debit card. Track data contains certain information relating to a particular debit or credit account, including the account number and other personal identifying information.

2 Skimming operations involve the theft of payment card numbers and related data through the surreptitious installation of specialized equipment at ATMs or point-of-sale terminals, which are designed to steal the track data on the back of a payment card once it is used at the ATM or point-of-sale terminal.

such stolen information re-encode the stolen track data on to plastic magnetic-stripe cards with the same dimensions as a legitimate payment card, then use those re-encoded cards to execute unauthorized transactions for goods, services, cash, pre-paid gift or debit cards and other items of value. Re-encoding counterfeit payment cards with stolen track data requires the use of specialized equipment (e.g. magnetic-stripe reader/writer) and software that is readily available for sale to the general public.

17. Based on my training and experience, stolen track data can be re-encoded onto any magnetic stripe plastic card, including gift cards and prepaid debit cards. Use of such generic magnetic stripe cards, however, increases the risk that cautious retail clerks, like the Rutherfordton Food Lion grocery store clerk, may notice that the payment card information printed on a receipt after the card is swiped does not match the account number appearing on the face of the magnetic stripe payment card presented for payment. Generic gift cards, prepaid cards or re-used credit or debit cards containing different account numbers embossed on such plastic payment cards expose cash-out operations and criminals to the risk of detection by store clerks and arrest by law enforcement authorities. For this reason, an increasing number of more sophisticated cash-out operations and criminals have started to use genuine-looking counterfeit credit cards when using stolen payment card account numbers.

18. During its operation from 2012 until December 4, 2013, the Fake Plastic Website offered genuine-looking counterfeit payment cards to more sophisticated cash-out operations and criminals who wanted to increase their chances of successfully using stolen track data without being detected by store clerks and law enforcement. Such cash-out operations and criminals could do so by using the Fake Plastic Website's genuine-looking, custom-made counterfeit payment cards with

embossed account numbers matching stolen account numbers that the cash-out operations and criminals would encode on the magnetic stripe on the back of the counterfeit payment cards.

19. The Fake Plastic Website's operator and employees used equipment, supplies and software **(See EXHIBIT D)** seized by federal law enforcement agents on December 4, 2013, to manufacture the high-end, realistic-looking counterfeit payment cards desired by cash-out operations and criminals.

20. Criminals seeking to obtain counterfeit payment cards to be encoded with stolen track data or authentication features for false identification documents could do so by making online purchases through the Fake Plastic Website. In order to access the Fake Plastic Website's counterfeit payment cards and authentication features for false identification documents, individuals were required to be members with user login names and user passwords provided by the administrator of the Fake Plastic Website.

21. Members of the Fake Plastic Website seeking to purchase authentication features for false identification documents were able to browse through the Fake Plastic Website's offerings of holographic overlays for various state identification cards that could be ordered and then used to create legitimate looking state identification cards.

22. Members seeking to purchase counterfeit payment cards also were able to browse through the Fake Plastic Website's voluminous fake payment card inventory of designs that appeared to be and were substantially indistinguishable from legitimate, genuine credit and debit cards. **See EXHIBIT A.** Members had the ability to select the design and look of the fake payment cards that they wanted to order from a selection of legitimate looking payment card templates, bearing the trademarks of various payment card issuers and card-issuing banks. Members could even select and order various holographic stickers designed to look like and substantially

indistinguishable from the holograms appearing on legitimate, genuine payment cards. **See EXHIBIT C.**

23. Members also could input an account number, name, expiration date, and CVV or CID number, which were embossed by the Fake Plastic Website conspirators, or printed on the cards with raised print-type, onto the counterfeit cards.[3] **See EXHIBIT B.** For those members with access to their own embossing equipment, counterfeit payment cards could be purchased as "blanks," *i.e.* cards that were not embossed with account numbers, names, and expiration dates.

24. Once an order was placed on the Fake Plastic Website, the Website member was provided with a tracking number for delivery of the ordered contraband directly through the Fake Plastic Website, which appeared on a page displaying that member's order history.

25. According to the Fake Plastic Website, its members could make purchases using BitCoin, a cryptographic-based digital currency service. Until in or around May 2013, the Fake Plastic Website also allowed its members to make purchases using Liberty Reserve online currency. Liberty Reserve, its founders, and certain of its officers were indicted by the Southern District of New York, 13-cr-368 for, among other things, money laundering. The charges against Liberty Reserve were made public in or around May 2013. Shortly thereafter, the Fake Plastic Website stopped accepting Liberty Reserve currency.

---

3 CVV stands for "Card Verification Value" and CID stands for "Card Identifier" or "Card Identification Number." Both are 3- to 4- digit codes embossed on the front or back of legitimate payment cards. Online merchants often require customers to enter a card's CVV or CID code along with other payment card information prior to entering into online transactions. The purpose of requiring the entry of these codes is to provide some proof that the user of the payment card account information has physical possession of the card.

C. **Post-Seizure Operation by Law Enforcement of the Fake Plastic Website**

26. The joint multi-agency, multi-district criminal investigation revealed that since in or around the middle of 2012, in the Middle District of Florida, the Fake Plastic Website was owned and operated by a person identified herein as S.R. Since in or about January 2013, a person identified herein as V.G. was primarily responsible for physically manufacturing the counterfeit payment cards, packaging the counterfeit payment cards for shipment by U.S. Express Mail to the Fake Plastic Website's members, and placing the U.S. Express Mail packages in the U.S. mail for delivery to the Fake Plastic Website's members.

27. As referenced above, law enforcement agents executed multiple search warrants on December 4, 2013, including a search warrant executed at the warehouse where the Fake Plastic Website's orders were processed, manufactured and prepared for shipment by U.S. mail to the Fake Plastic Website's members. Law enforcement agents seized the equipment, materials, supplies, inventory of holographic overlays and holographic stickers, computers, software and packaging materials used to manufacture and ship by mail counterfeit payment cards to the Fake Plastic Website's customers. **See EXHIBIT D.**

28. Since on or about December 5, 2013, law enforcement assumed control of the Fake Plastic Website as well as an associated email account used to communicate with a number of the Fake Plastic Website's customers.

29. The investigation revealed that the conspirators involved in the Fake Plastic Website operation used a number of different methods to mail out orders placed on the Fake Plastic Website. The Fake Plastic Website conspirators used a number of different United States Postal Service ("USPS") Click-N-Ship Web Tools ("Click-N-Ship") accounts (the "Fake Plastic Click-N-Ship

Accounts") to create tracking numbers and shipping labels for delivery of the orders made through the Fake Plastic Website.

30. Because law enforcement controlled the Fake Plastic Website and various related email accounts after December 5, 2013, law enforcement has been able to review the order history of the members of the Fake Plastic Website. Additionally, every new order placed on the Fake Plastic Website after December 5, 2013, has been and continues to be sent exclusively to law enforcement.

31. The post-December 5, 2013 orders place by the Fake Plastic Website's members have been accessible to law enforcement either by accessing the Fake Plastic Website as the sole administrator, or through emails generated by the Website (the "Website Order Emails") that have been automatically forwarded to an email account also controlled by law enforcement.

32. The Fake Plastic Website Order Emails follow a uniform format. Each of these emails has a subject line beginning with the words "Website Order," followed by an order number and date and time. The bodies of the emails contain the details of orders placed on the Fake Plastic Website and follow the same basic structure. The Fake Plastic Website Order Emails each contain: (a) a shipping method for the order; (b) the username of the Fake Plastic Website user placing the order; (c) an address and "Drop Name" to send the order to; and (d) the actual order. The order itself indicates the quantity and type of each order. As an example, a Fake Plastic Website Order Email ordering "blanks" will indicate the amount of each type of counterfeit card ordered by the user (for example, 5 "Amex Citi Advantage" cards indicates an order of five unembossed cards bearing American Express and Citibank trademarks). If, for example, a member orders embossed cards, the Fake Plastic Website Order Email includes, not only the template counterfeit card to be

used, but also the account number, name, expiration date, and CVV or CID number to be embossed onto the ordered cards.

33. Since December 5, 2013, once law enforcement received an order from the Fake Plastic Website, USPIS inspectors prepared a parcel with a tracking number and shipping label made to appear as though it was generated through one of the Fake Plastic Click-N-Ship Accounts.

34. The investigation revealed that Fake Plastic Website members typically received their orders within one or two days of placing their orders on the Fake Plastic Website. In order not to raise any suspicion about law-enforcement changes to the *modus operandi* of the Fake Plastic Website, law enforcement notified the Fake Plastic Website's members, through a blog appearing on its welcome page, that Fake Plastic Website orders would be delayed due to technical issues, and that all orders will be fulfilled as soon as possible.

35. Once a Fake Plastic Website member placed on order for counterfeit payment cards, USPIS prepared U.S. Express Mail envelopes without any contraband contained inside other than a number of holographic stickers bearing infringing trademarks.

D. Fake Plastic Website Orders Mailed to 3531 Creeping Flora Ln, Charlotte, NC

36. A review of USPS records revealed that twenty-two (22) individual parcels of counterfeit payment cards were mailed from the Fake Plastic Website's Florida operation to a townhouse residence located at the **3531 Creeping Flora Lane** address from June 13, 2012, and December 2, 2013. The mailings included: (a) 2 parcels mailed on 6/13/12, (b) 1 parcel mailed on 6/20/12, (c) 1 parcel mailed on 6/26/12, (d) 1 parcel mailed on 7/17/2012, (e) 1 parcel mailed on 7/23/12, (f) 1 parcel mailed on 7/31/12, (g) 1 parcel mailed on 8/14/12, (h) 2 parcels mailed on 9/5/12, (i) 1 parcel mailed on 9/26/12, (j) 1 parcel mailed on 9/20/13, (k) 1 parcel mailed on 9/24/13, (l) 1 parcel mailed on 9/30/13, (m) 1 parcel mailed on 10/8/13, (n) 1 parcel mailed on

10/10/13, (o) 1 parcel mailed on 10/15/13, (p) 1 parcel mailed on 10/23/13, (q) 1 parcel mailed on 11/1/13, (r) 1 parcel mailed on 11/18/13, (s) 1 parcel mailed on 11/21/13, and (t) 1 parcel mailed on 12/2/13.

37. Significantly, as discussed more fully below, eleven (11) parcels had been mailed to the **3531 Creeping Flora Lane** townhouse residence from June 13, 2012, and September 26, 2012, no parcels were mailed to the **3531 Creeping Flora Lane** townhouse residence from May 2013, through August 2013, and **eleven (11) parcels had been mailed to the 3531 Creeping Flora Lane townhouse residence from September 20, 2013, and December 2, 2013**. The name of the addressee of the mailings from June 2012 to September 2012 was "Debbie Young." The name of the addressee of the mailings from September 20, 2013, to December 2, 2013 was "Carlton Drayton" on one of the mailings, and "Akeem Drayton" on the remaining mailings.

38. A review of USPS records revealed that movement of several of the eleven parcels mailed in late 2013 from the Fake Plastic Website for delivery to the townhouse residence located at **3531 Creeping Flora Lane, Charlotte, NC,** had been tracked on the Internet from IP address 75.181.140.247. Based on a court order obtained by Charlotte-Mecklenburg Police Department, Time Warne Cable records were obtained for said IP address that included subscriber information for Internet service to IP address 75.181.140.247 in the name of Debbie Young, **3531 Creeping Flora Lane, Charlotte, NC**. Said records also reflected that Internet Service had been active at **3531 Creeping Flora Lane, Charlotte, NC** since September 1, 2013.

E. NASHANCY JOHNNY COLBERT and the Fake Plastic Website

39. On or about December 20, 2013, law enforcement received the following order from a member of the Fake Plastic Website: **User ID: cbreeze**; **Drop name: Akeem Drayton**; **Drop**

address: 3531 Creeping Flora Ln, Charlotte, NC 28216; Specific order: 19 piece embossed credit card order bearing 16-digit credit cards numbers (suspected at the time of being stolen).

40. Pursuant to an anticipatory search warrant issued on December 23, 2013, to search the townhouse residence at **3531 Creeping Flora Lane** address, a control package (which did not contain any counterfeit credit cards) was prepared for delivery in a U.S. Express mail envelope addressed to "Akeem Drayton, 3531 Creeping Flora Ln, Charlotte, NC 28216-6614" with a return address of "Roger Townshend, 1155 Malabar RD NE, Palm Bay, FL 32907-3245" bearing tracking number 9470112699350002194327. In executing the federal anticipatory search warrant on the same date, an undercover law enforcement officer posing as a USPS letter carrier made a controlled delivery of an undercover Fake Plastic Website parcel on December 23, 2013, to a locked mailbox for the **3531 Creeping Flora Lane** townhouse residence. Post-delivery law enforcement surveillance of the locked mailbox and the townhouse residence of **3531 Creeping Flora Lane** was conducted from approximately 1:00 p.m. to 5:00 p.m. Law enforcement did not observe anyone access the locked mailbox to retrieve said parcel. Thereafter, USPIS Postal Inspectors knocked on the front door of the **3531 Creeping Flora Lane** townhouse in an effort to make contact with any occupants of said premises. USPIS Postal Inspectors retrieved said parcel from the locked mail box after no one answered the door of the **3531 Creeping Flora Lane** townhouse residence.

41. USPS database records revealed that on the following day, December 24, 2013, that a person accessing the Internet from IP address 75.181.140.247 checked the tracking the status of the control parcel that had been delivered to and retrieved by law enforcement on December 23, 2013. The information displayed to the inquiring online customer accessing the USPS website reflected that said parcel had been delivered to **3531 Creeping Flora Lane** on December 23, 2013.

42. I obtained a federal search warrant for the townhouse residence located at **3531 Creeping Flora Lane, Charlotte, NC,** on January 2, 2014, and executed it on January 3, 2014, along with other law enforcement agents.

43. Present in the **3531 Creeping Flora Lane** townhouse residence at the time of the search on January 3, 2014, were **NASHANCY JOHNNY COLBERT** and a female identified herein as D.Y. **COLBERT** and D.Y. each stated that they both lived at said townhouse residence and shared a bedroom. **COLBERT** acknowledged that he used the **User ID: cbreeze** on the Fake Plastic Website. It should be noted that all of the orders placed on and shipped from the Fake Plastic Website, set forth in paragraph 36, were made on the user ID account **cbreeze**.

44. **COLBERT** also acknowledged that **COLBERT** had been convicted in state court of state offenses related to stolen credit cards, that **COLBERT** went to jail in May 2013 for his state conviction, that **COLBERT** had been released from jail in September 2013, and that **COLBERT** has been on and continues to be on state probation for his state convictions. **COLBERT**, who was not under arrest and who was free to leave, refused to answer any more questions in connection with the Fake Plastic Website or evidence that law enforcement recovered from **COLBERT's** residence during the search on January 3, 2014.

45. Evidence recovered during the search of **COLBERT**'s residence included approximately forty-one (41) counterfeit payment cards, thirty-seven (37) of which were encoded with payment card information. Seventeen (17) of the forty-one (41) counterfeit payment cards had the name "**NASHANCY COLBERT**" embossed on them, and the remaining counterfeit payment cards had the names of other individuals embossed on them. Of the seventeen (17) counterfeit payment cards in **COLBERT**'s name, thirteen (13) of those counterfeit payment cards were encoded with payment card account numbers. To date, three (3) of the encoded counterfeit payment

cards in **COLBERT**'s name have been confirmed as being compromised or stolen payment card account numbers. The status of the remaining payment card numbers on **COLBERT**'s embossed and encoded counterfeit payment cards has not yet been provided by the card-issuing banks to law enforcement. Of the forty-one (41) seized counterfeit payment cards, thirty-seven (37) had payment card account information encoded on the magnetic stripe, and of those cards, eighteen (18) payment cards account numbers (including three (3) counterfeit payment cards in **COLBERT**'s name) have been confirmed to be compromised or stolen. The status of the remaining payment card numbers has not yet been provided by the card-issuing banks to law enforcement

46. Additional evidence recovered from **COLBERT**'s residence during the search also included a magnetic stripe reader/writer and a laptop computer. I know from my training and experience that the computer and magnetic stripe reader/writer can be used to encode stolen payment card account information onto magnetic- stripe cards, including counterfeit magnetic-stripe payment cards like those found in **COLBERT**'s residence during the search and previously ordered from the Fake Plastic Website since June 2012 under the user ID name **cbreeze**.

47. Additional evidence recovered during the search of **COLBERT**'s residence included a discarded U.S. Express Mail envelope from the Fake Plastic Website that had been mailed on December 2, 2013, consistent with USPS records for said mailing under e user ID name **cbreeze**.

48. I have reviewed **COLBERT**'s criminal history and discovered that, according to jail records, **COLBERT** was convicted on May 7, 2013, in state court in Mecklenburg County, North Carolina, for Obtaining Property by False Pretenses. Jail records reveal that **COLBERT** received a five-month jail sentence for said state offense, that **COLBERT** began his jail sentence on May 10, 2013, and that **COLBERT** was released from jail on September 4, 2013. Jail records also reflect that **COLBERT** was convicted of Uttering Forged Instruments on May 7, 2013, in state court in

Mecklenburg County, North Carolina, and was sentenced to twenty-four (24) months' probation, with a supervision release date of May 7, 2015.

49. As noted above, no parcels from the Fake Plastic Website were mailed to the **3531 Creeping Flora Lane** townhouse residence during the time that **COLBERT** was in jail from May 2013, through August 2013. However, on sixteen (16) days following **COLBERT**'s release from state jail, eleven (11) parcels of counterfeit payment cards were ordered from and mailed from the Fake Plastic Website to the **3531 Creeping Flora Lane** townhouse residence, beginning on September 20, 2013, and ending on December 2, 2013, two days before the government's seizure and takedown of the Fake Plastic Website. It should be noted that the U.S. Express Mail envelope from the order placed by user ID **cbreeze** on December 2, 2013, was recovered in the search of **COLBERT**'s residence on January 3, 2014.

50. Records from the Fake Plastic Website reflect that 231 counterfeit payment cards were ordered and shipped from the Fake Plastic Website to the **3531 Creeping Flora Lane** townhouse residence from September 20, 2013, to December 2, 2013. All orders had placed under the user ID name **cbreeze**. To date, at least twelve (12) payment card account numbers embossed on the customized counterfeit payment cards have been determined to be compromised or stolen payment cards account numbers. The status of the remaining payment card numbers that were ordered to be embossed on the counterfeit payment cards manufactured by the Fake Plastic Website conspirators has not yet been provided by the card-issuing banks to law enforcement.

Randy Berkland

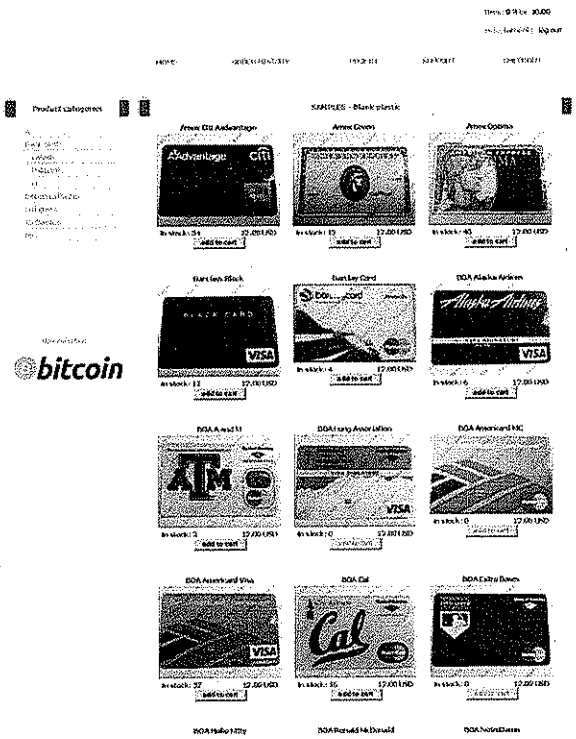
RANDY BERKLAND
United States Postal Inspector

Sworn to and Subscribed before me
this 17 day of January, 2014

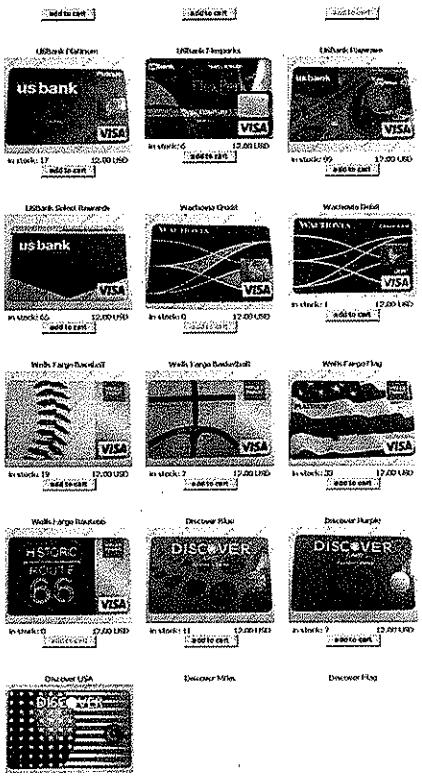
D. J. Cayer

DAVID S. CAYER
United States Magistrate Judge

EXHIBIT "A"


Product categories
SAMPLES - Blank plastic
bitcoin


HSBC Business
HSBC Black
HSBC Classic
HSBC Corporate
HSBC Lemans
HSBC Platinum
HSBC Sphere
Metro
PNC Cashbuilder
Regions Black
Suntrust Platinum
Suntrust Signature
TD Bank Gold
TD Bank Green
USAA Tuskegee
add to cart


add to cart
USBank Platinum
USBank Prosperia
USBank Visa
us bank
USBank Select Rewards
Wachovia Credit
Wachovia Debit
Wells Fargo Business
Wells Fargo Business
Wells Fargo Flag
Wells Fargo Business
Discover Blue
Discover Purple
DISCOVER
Discover USA
Discover Miles
Discover Flag


Miles

EXHIBIT "B"

Items: 0 Price: $0.00

Hello, tarheel | log out

HOME ORDER HISTORY PROFILE SUPPORT CHECKOUT

Product categories

- All
- Blank plastic
  - Canada
  - Philippines
  - UK
- Embossed Plastics
- Holograms
- ID Overlays
- Misc

Now Accepting ...

bitcoin

SAMPLES - Embossed Plastics

Format:
account number, exp date(YYMM), first and last name, custom cvv(optional)
The following characters may be used as delimiters: , or | or =
Example: 4147507512345678=1412, john smith or 4147507512345678,1412,john smith,345

ACCOUNT NUMBER
Input the 16 digit account number or 15 digit account number for amex.
For a random AMEx account number use only the number 3 in the first field.
For a random VISA account number use only the number 4 in the first field.
For a random MC account number use only the number 5 in the first field.
For a random DISCO account number use only the number 6 in the first field.

EXPIRATION FIELD
Input the exp date to be embossed in the year year month month format just like your dumps.
For a random exp date, leave the field blank. To NOT emboss the exp date, use spaces instead.

FULL NAME
Input first name first then the last name to emboss.
If you want this field to be blank and not embossed, then leave blank or use spaces instead.

CVV or CID (AMEX)
For random cvv numbers, then do not enter this field or leave it blank.
If you choose to have NO cvv printed, then use spaces after the last delimiter.

Paste Embossing Data Here

Check Embossing Info

Please double check all info is correct.
This will be the data used for embossing orders.

E-mail: info@fakeplastic.biz / Phone: +123 543-56-67

EXHIBIT "C"

Items: 0 Price: $0.00

Hello, tarheel | log out

HOME ORDER HISTORY PROFILE SUPPORT CHECKOUT

Product categories

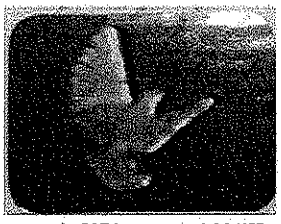
- All
- Blank plastic
  - Canada
  - Philippines
  - UK
- Embossed Plastics
- Holograms
- ID Overlays
- Misc

Now Accepting ...

bitcoin

SAMPLES - Holograms

Visa Stickers - Small Silver



in stock: 3074 1.00 USD

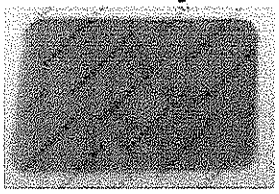
add to cart

Visa Stickers - Large Silver

in stock: 0 1.00 USD

add to cart

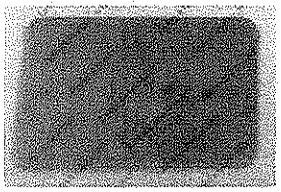
Visa Stickers - Large Gold



in stock: 1697 1.00 USD

add to cart

Visa Stickers - Small Gold



in stock: 10940 1.00 USD

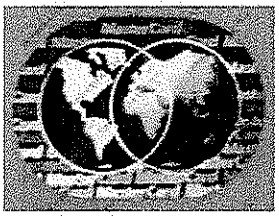
add to cart

Master Card Stickers - Silver

in stock: 0 1.00 USD

add to cart

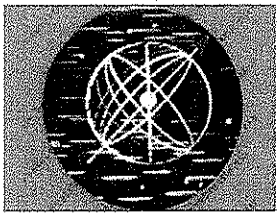
Master Card Stickers - Gold



in stock: 7408 1.00 USD

add to cart

Discover Stickers - Silver

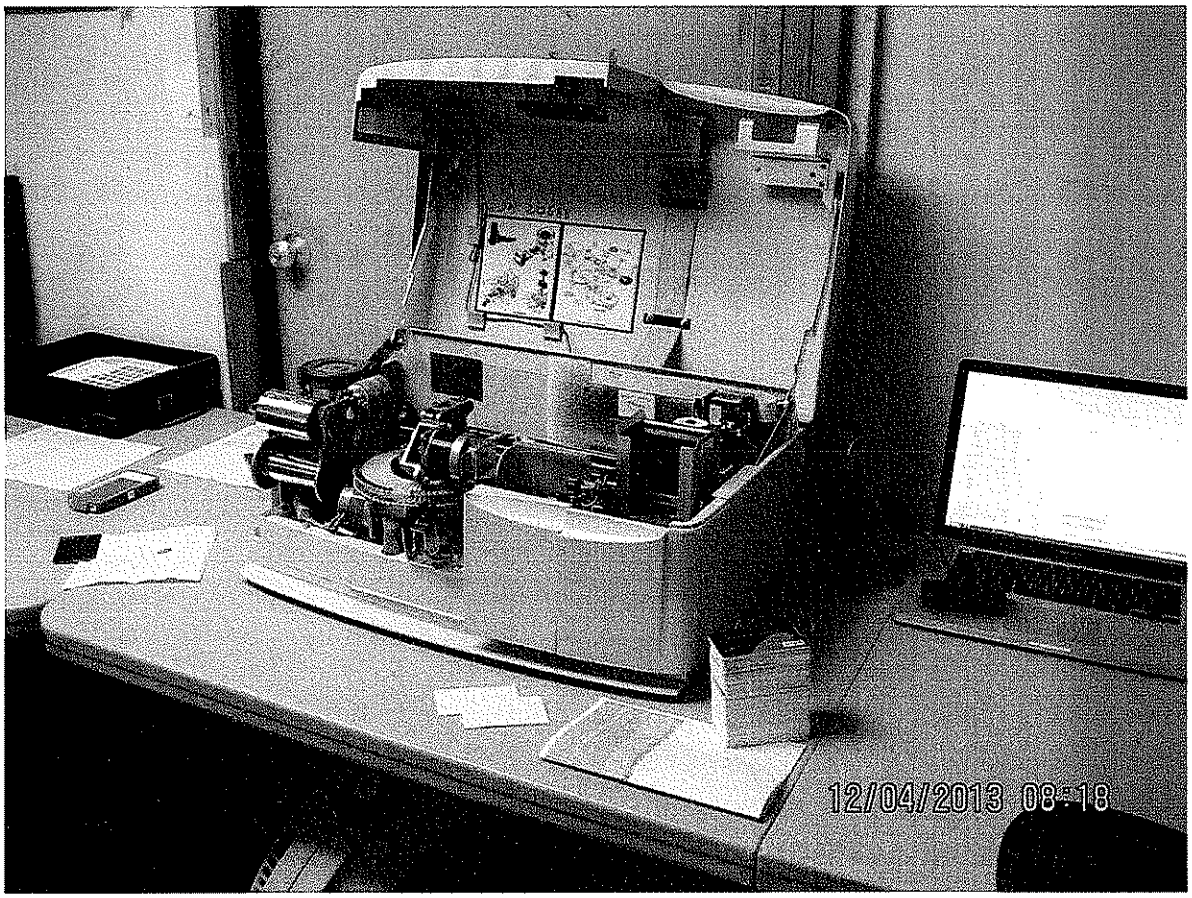


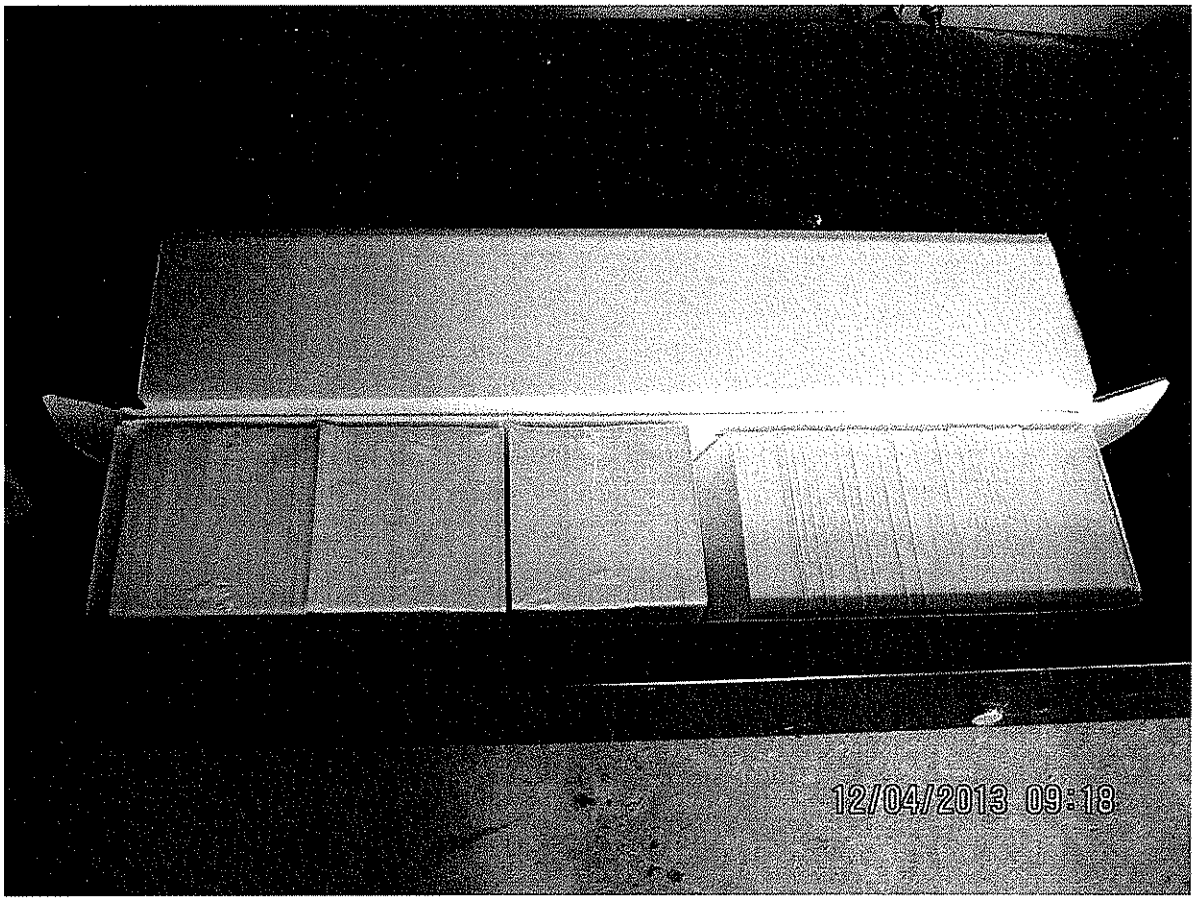
in stock: 25672 1.00 USD

add to cart

E-mail: info@fakeplastic.biz / Phone: +123 543-56-67

EXHIBIT "D"


12/04/2013 08:18


12/04/2013 09:18


barclaycard
rewards
PLATINUM PLUS
CHASE FREEDOM
VISA
REGIONS
12/04/2013 09:14


12/04/2013 09:27


12/04/2013 09:31