
**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA	:	Hon. Mark Falk
	:	
v.	:	Mag. No. 13-8354 (MCA)
	:	
SEAN ROBERSON	:	AMENDED CRIMINAL COMPLAINT

I, Eric Malecki, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Postal Inspector with the United States Postal Inspection Service, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.

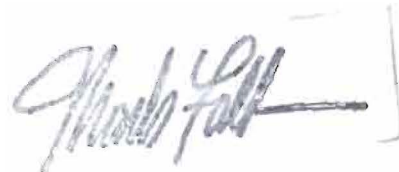


Eric Malecki, Postal Inspector
United States Postal Inspection Service

Sworn to before me, and
subscribed in my presence

January 21, 2014 at
Newark, New Jersey

HONORABLE MARK FALK
UNITED STATES MAGISTRATE JUDGE



Signature of Judicial Officer

ATTACHMENT A

Count One (Conspiracy to Commit Fraud by Wire)

From at least as early as in or around April 2011 through in or around December 2013, in the District of New Jersey and elsewhere, defendant

SEAN ROBERSON

knowingly and intentionally conspired and agreed with Vinicio Gonzalez, Hugo Rebaza, and others, to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communications in interstate commerce, certain writings, signs, signals, pictures, and sounds for the purpose of executing such scheme or artifice in a manner affecting a financial institution, contrary to Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Section 1349.

Count Two (Conspiracy to Traffic in Counterfeit Goods or Services)

From at least as early as in or around April 2011 through in or around December 2013, in the District of New Jersey and elsewhere, defendant

SEAN ROBERSON

knowingly and intentionally conspired and agreed with Vinicio Gonzalez, Hugo Rebaza, and others, to traffic and attempt to traffic in goods and services and knowingly used counterfeit marks on and in connection with such goods and services, and intentionally trafficked and attempted to traffic in labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, and packaging of any type and nature, knowing that counterfeit marks had been applied thereto, the use of which was likely to cause confusion, to cause mistake, and to deceive.

In violation of Title 18, United States Code, Section 2320(a).

Count Three
**(Conspiracy to Commit Fraud and Related Activity in
Connection with Authentication Features)**

From at least as early as in or around April 2011 through in or around December 2013, in the District of New Jersey and elsewhere, defendant

SEAN ROBERSON

knowingly and intentionally conspired and agreed with Vinicio Gonzalez, Hugo Rebaza, and others, to traffic in false and actual authentication features for use in false identification documents, document-making implements, and means of identification, contrary to Title 18, United States Code, Section 1028(a)(8).

In violation of Title 18, United States Code, Section 1028(f).

ATTACHMENT B

I, Eric Malecki, a Postal Inspector with the United States Postal Inspection Service (“USPIS”), having conducted an investigation and discussed this matter with other law enforcement officers who have participated in this investigation, have knowledge of the following facts. Because this Complaint is being submitted for the limited purpose of establishing probable cause, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts which I believe are necessary to establish probable cause. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part.

Background

1. At all times relevant to this Complaint, unless otherwise indicated:
 - a. Defendant SEAN ROBERSON was a resident of Palm Bay, Florida. ROBERSON was convicted in 2006, in the District of New Jersey, for fraud and related activity in connection with means of identification, in violation of Title 18, United States Code, Section 1028, for attempting to sell counterfeit driver’s licenses and health insurance cards over the Internet. In or around January 2013, ROBERSON formed Inksplat LLC (“Inksplat”), ostensibly a printing company that sold customizable T-shirts, mugs, and other items, bearing various logos and images. Beginning in or around April 2011, ROBERSON began selling counterfeit credit and debit cards (collectively, “payment cards”) and related contraband over the Internet. By June 2012, ROBERSON launched an online retail shop specializing in the sale of counterfeit payment cards, as well as holographic overlays used to make fake identification cards, known as fakeplastic.net (the “Fakeplastic Website” or “Website”). ROBERSON, *inter alia*, created the templates used to create the counterfeit payment cards, oversaw the process for creating counterfeit payment cards, set up the card manufacturing plant used to fulfill orders for counterfeit payment cards, and was the founder and administrator of the Website.
 - b. Vinicio Gonzalez was a resident of Palm Bay, Florida. Gonzalez was responsible for, *inter alia*, actually printing the counterfeit payment cards ordered by the Website’s customers, as well as creating the mailings used to deliver the cards and any other contraband ordered on through the Website.
 - c. Hugo Rebaza was a resident of Palm Bay, Florida. Rebaza assisted ROBERSON in, *inter alia*, opening “mail drops” using fake identification, which were primarily used to receive supplies needed to fulfill orders placed on the Website and, in some cases, to receive cash payment from some of ROBERSON’s customers.
 - d. Both Gonzalez and Rebaza have been charged in the Western District of North Carolina for their involvement in the scheme alleged herein.
 - e. “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 credit or debit account, including the credit or debit account number and the name on the account. Criminals often refer to stolen track data as “dumps.”

f. “Embossing” is the act of printing certain information on credit and debit cards. Embossed print is the raised print typically appearing on the face of legitimate payment cards that displays information associated with a particular card, such as the name of the accountholder, the account number for the account, and expiration date for the card.

g. “CVV” stands for “Card Verification Value” and “CID” refers to “Card Identifier” or “Card Identification Number.” Both are 3- to 4- digit codes printed 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.

h. “Authentication features” refer to any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that either individually or in combination with another feature is used by the issuing authority on an identification document, document-making implement, or means of identification to determine if the document is counterfeit, altered, or otherwise falsified.

i. “IP address” refers to an Internet Protocol address. An IP address is a unique number assigned to an internet connection. This number is used to route information between devices. Two computers or devices must know each other’s IP addresses to exchange even the smallest amount of information. Accordingly, when one computer requests information from a second computer, the requesting computer specifies its own IP address so that the responding computer knows where to send its response.

j. “Proxy services” are services that allow individuals to hide their true IP address when accessing the Internet.

k. “Bitcoin” is a cryptographic-based digital currency, which can be used to pay for goods or services over the Internet, and can be exchanged into United States currency through, *inter alia*, the use of Bitcoin exchangers.

l. “Liberty Reserve” is an online currency, which, until in or around May 2013, could be used to pay for goods or services over the Internet, and could be exchanged into United States currency.

m. “Counterfeit payment card plants” are operations using specialized equipment, such as specialized printers, embossers, card readers, and encoders, to create counterfeit payment cards.

The Investigation

A. The Fakeplastic Website

Overview

2. Since in or around January 2013, the Federal Bureau of Investigation (“FBI”) and USPIS have been investigating a large-scale seller of (i) authentication features for false identification documents, namely holographic overlays used on various state-issued driver’s licenses, and (ii) customized counterfeit payment cards. The authentication features and cards were sold through the Fakeplastic Website.

3. The Fakeplastic Website was a one-stop shop for various “carding” or “cash out” crews across the country. These crews obtain stolen track data, or “dumps,” through various online “vendors” who typically obtain the data through a number of varied schemes, including skimming operations¹ and hacking, designed to illegally acquire other people’s payment card numbers and other related information.

4. Once the stolen track data is acquired, criminals seeking to monetize the stolen information re-encode the stolen track data on to cards with the same dimensions as legitimate payment cards, then use those re-encoded cards to enter into unauthorized transactions. Once the stolen data is re-encoded onto these cards, they could be used at ATM machines or point-of-sale terminals to withdraw money or make unauthorized purchases.

5. Traditionally, these criminals would re-encode stolen track data onto the magnetic stripe appearing on the back of gift cards or prepaid credit cards. However, the use of such cards increased the risk that the criminals using them would raise the suspicion of wary retail clerks noticing that the payment card information actually used in the transaction, after the card is swiped, does not match the face of the card presented, which would appear to be a gift card or prepaid card with a different account number. Accordingly, more sophisticated cash out operations seeking to increase the likelihood of successfully using stolen track data without detection by law enforcement use custom-made counterfeit payment cards embossed with the same account numbers that have been encoded on the back of the card. These more sophisticated operations oftentimes acquire fake identification cards in order to increase the likelihood of successfully using stolen track data without detection from law enforcement.

6. The criminal underground for the purchase and sale of stolen track data has evolved from fractured, regional operations, to what is more accurately described as “e-commerce,” where buyers and sellers across the globe can advertise, purchase, and transmit, stolen track data through the Internet. The market for the physical tools required by these cash out operations, fake identification and custom-embossed counterfeit cards, has lagged behind the market for stolen track data, likely because the creation of fake identification and high-quality counterfeit payment cards require the use of expensive, specialized equipment. However, the

¹ “Skimming operations” refer to schemes involving the installation of specialized equipment at either ATM locations or point-of-sale terminals, designed to steal payment card information once it is used to enter into a transaction.

Fakeplastic Website brought the physical tools needed by these cash out operations to the world of e-commerce by providing an online retail shop for cash out operations seeking to purchase high-end, realistic looking counterfeit payment cards. These criminals could now order what they needed for their cash out operations directly from the Website, eliminating the need to invest in expensive hardware.

Making Purchases on the Website

7. Since in or around June 2012, criminals seeking to obtain high-quality 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 Fakeplastic Website. In order to access the Website's illegal offerings, an individual needed to be a member with a login and password provided by the administrator of the site. See Exhibit A (screenshot of the login page for the Website). As of December 2013, the Website had over 400 members.

8. Upon successful login, members of the Website were directed to a welcome page listing the Website's inventory of contraband, as well as a "current news" section. See Exhibit B (screenshot of welcome page).

9. Members of the Fakeplastic Website seeking to purchase authentication features for false identification documents were able to browse through the 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. See Exhibit C (screenshot of Website page displaying some of the holographic overlays members of the Website could purchase). These members typically had the ability to create their own fake identification cards, but not the holographic overlays used to make the cards appear legitimate.

10. Members seeking to purchase counterfeit payment cards were able to browse through the Website's many varied fake cards designed to look like legitimate payment cards. Members had the ability to select the design and look of the fake payment card they wished to order from a selection of legitimate looking payment card templates, bearing the trademarks of various payment card issuers and processors. See Exhibit D (screenshot of Website page displaying some of the counterfeit payment cards members of the Website could purchase); Exhibit E (blowout of Exhibit D). Indeed, members could even select and order various holographic stickers designed to look like the holograms appearing on legitimate payment cards. See Exhibit F (screenshot of Website page displaying various holographic stickers members of the Website could purchase).

11. The counterfeit cards made available through the Website contained at least one counterfeit mark identical to 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.

12. Fakeplastic Website members could also input an account number, name, expiration date, and CVV or CID number, directly through the Website, which were all then embossed onto the counterfeit cards. See Exhibit G (screenshot of Website page where members

ordering counterfeit payment cards could input information to be embossed on cards purchased from the Website; the information appearing in this exhibit does not relate to actual payment card accounts). For those members with access to their own embossing equipment, counterfeit payment cards could be purchased as “blanks,” *i.e.* cards designed to look legitimate and bearing one or more infringing mark, that had not been embossed with account numbers, names, and expiration dates.

Payment for Purchases on the Website

13. According to the Fakeplastic Website, its members could make purchases using Bitcoin, a cryptographic-based digital currency service. Until in or around May 2013, the 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 United States Attorney’s Office for 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 Fakeplastic Website stopped accepting Liberty Reserve currency. Indeed, notice of this change was posted in the “current news” section of the Website’s welcome page on or about May 27, 2013. See Exhibit B (screenshot of the “current news” section of the welcome page for the Website). The posting, which is excerpted below, noted the change from Liberty Reserve to Bitcoin and highlighted that Bitcoin was both safe and anonymous and had been previously used by other criminal websites:

So for anyone that has not heard. Liberty Reserve was shutdown indefinitely for Money Laundering. What does that mean for fakeplastic??? It means we are going to accept Bitcoin as our primary payment system

I strongly urge everyone who is working in our line of work to start using Bitcoin. Bitcoin cannot be shutdown by any person or government, it cannot track your ass down, it is anonymous and safe! It is why Sil[k]Road (largest drug buying marketplace) has always used Bitcoin as a payment processor.

The Co-Conspirators’ Roles

14. SEAN ROBERSON was the mastermind behind the Website and enlisted the assistance of Hugo Rebaza, Vinicio Gonzalez, and others known and unknown (collectively, the “Co-Conspirators”), to create and ship the contraband ordered from the Website.

15. As further detailed below, when Fakeplastic Website members ordered contraband from the Website, an email was automatically generated by the Website and sent to ROBERSON. These emails, referred to herein as “Website Order Emails,” contained detailed information regarding the order as well as names and addresses for delivery of the order.

16. Once ROBERSON received a Website Order Email, he provided the details of the order to his Co-Conspirators, including Gonzalez, who would put together the orders for

delivery. For orders of counterfeit payment cards, ROBERSON provided Gonzalez and others with a spreadsheet, referred to herein as the "Embossing Order Spreadsheets," designed to be used in conjunction with certain specialized printers to print out the counterfeit payment cards. Using the Embossing Order Spreadsheets and specialized software and hardware, the Co-Conspirators were able to create counterfeit payment cards embossed with information provided by the Fakeplastic Website member ordering the cards.

17. Additionally, ROBERSON took custom orders from some of his clients, where ROBERSON would not only provide embossed counterfeit payment cards, but would also encode stolen track data, provided by his customers, on the magnetic stripe on the back of the counterfeit payment cards. After putting together the contraband ordered by one or more of ROBERSON's customers, Gonzalez and others, mailed the orders out via United States Postal Service express mail.

18. The Co-Conspirators used a number of commercial mail receiving agents ("CMRAs") to receive cash payment for orders made through the Website, as well as to receive the Co-Conspirator's orders of holographic overlays that were resold through the Website. Although the Website primarily received payment through online currencies such as Bitcoin, in some instances ROBERSON accepted cash payment.

Pricing, Profit, and Loss

19. The Fakeplastic Website provided its members with bulk discounting in certain circumstances, and even provided some members with online "coupons" that could be entered in the Website when placing an order to get a discount. The listed price for the contraband sold through the Website was as follows:

- a. \$1 for each holographic overlay;
- b. \$1 for each holographic sticker;
- c. \$12 for each unembossed counterfeit card; and
- d. \$15 for each embossed counterfeit card.

20. The Fakeplastic Website was launched in or around June 2012. Prior to the creation of the Website, ROBERSON advertised his services and products through online criminal forums, and took orders for counterfeit payment cards by email and through online instant chat programs such as "ICQ." Between in or around April 2011 and December 2013, ROBERSON received and fulfilled orders, either by email, ICQ, or through the Website, for over 69,000 counterfeit payment cards (over 46,000 unembossed counterfeit payment cards and over 23,000 embossed cards), over 35,000 holographic stickers, and over 30,000 state identification holographic overlays. Indeed, the Co-Conspirators sent over 3,600 parcels through the United States mail since April 2011 in order to fulfill these orders.

21. The losses associated with the over 69,000 counterfeit payment cards ordered directly through ROBERSON or the Website are difficult to estimate in light of the fact that it is impossible to know specifically what stolen payment card numbers were used with the unembossed counterfeit payment cards trafficked by ROBERSON and his Co-Conspirators.

However, using an estimate of loss of \$500 associated with each counterfeit payment card, derived from the Sentencing Guidelines estimation of loss associated with stolen payment card information, law enforcement estimates the losses associated with just the counterfeit payment cards trafficked by ROBERSON and his Co-Conspirators at over \$34,500,000.

Proceeds of the Fraud

22. During the course of its operation, the Website generated over \$1,700,000 in gross receipts for ROBERSON, who re-invested much of the proceeds into the illegal business itself, which required the acquisition and maintenance of expensive printing equipment, as well as to make cash purchases of, *inter alia*, an approximately \$76,000 rental property and an approximately \$48,000 Yamaha speedboat, as well as approximately \$20,000 in cash down payments for a 2008 Black Hummer and 2013 GMC Yukon Denali.

23. Additionally, and in order to compound his illegal profits, ROBERSON used the criminal proceeds from his illegal activity to purchase approximately fifty Bitcoin mining processors, currently valued at approximately \$1,000 each, in order to generate or “mine” Bitcoins. See Exhibit H (photograph of Bitcoin mining equipment seized from Inksplat). Since in or around October 2013, ROBERSON set up these processors and was able to “mine” over 150 Bitcoins as a result of his investment. Although the value of Bitcoins is highly-volatile, a single Bitcoin is currently valued at over \$800 per Bitcoin.

B. Identification of the Fakeplastic Website and the Associated Mailing Account

24. On or about January 30, 2013, law enforcement interviewed a confidential informant (the “CI”), who provided information about the Fakeplastic Website. According to the CI, the Website was a resource for criminals who wished to create fake identification documents or to encode stolen track data onto plastic cards designed to look like legitimate payment cards.

25. The CI indicated that the only way to access the Fakeplastic Website was to have a membership. Membership required an already existing member to “vouch” a new member into the Website by creating a membership account for the new user.

26. The CI stated that the CI had a membership for the Website, and provided the CI’s access credentials to law enforcement.

27. On or about January 30, 2013, law enforcement, using the CI’s membership credentials, accessed the Fakeplastic Website and confirmed the accuracy of the CI’s description of the Website.

28. According to the CI, once a purchase was made on the website, the purchased contraband was sent to the purchaser through the United States mail. The CI indicated that the CI had already made a purchase on the website prior to the January 30, 2013 interview, and had it sent to an address in New York City (the “CI Purchase”). The CI also provided law enforcement with the tracking number for the CI Purchase.

29. Law enforcement corroborated the information provided by the CI regarding the CI Purchase. The investigation revealed that a parcel was sent through the United States Postal Service ("USPS"), by express mail, to the New York City address, with the tracking number provided by the CI.

30. The investigation also revealed that the tracking number associated with the CI Purchase was generated through an online USPS Click-N-Ship Web Tools ("Click-N-Ship") account (the "Fakeplastic Click-N-Ship Account"). Click-N-Ship is a service offered by the USPS that allows users to create and print shipping labels from their home. In order to register for a Click-N-Ship account, a user must provide their name, address, and email address.

31. Law enforcement confirmed that the Fakeplastic Click-N-Ship account used to generate the tracking number associated with the CI Purchase was registered to a "Sam Adams," with a mailing address for a university in Florida. The email address associated with this account was budlighthouse@gmail.com (the "Budlighthouse Gmail Account").

32. USPS confirmed that over approximately 1,400 parcels were sent using the Fakeplastic Click-N-Ship Account since January 2013. The investigation also revealed a number of other Click-N-Ship accounts used to fulfill orders received by ROBERSON since in or around September 2011. In total, law enforcement identified over 3,600 parcels sent from the various Click-N-Ship accounts associated with ROBERSON and the Website.

33. On or about July 24, 2013, an undercover FBI agent (the "UC") placed an order for holographic overlays and counterfeit payment cards from the Fakeplastic Website. On or about July 30, 2013, the UC received, by mail, a package from an address in Melbourne, Florida. Inspection of the contents of that package confirmed that it contained the contraband ordered by the UC. USPS confirmed that the tracking number associated with the parcel was generated with the Fakeplastic Click-N-Ship Account.

34. On or about October 2, 2013, the UC ordered additional counterfeit payment cards from the Website. On or about October 9, 2013, the UC again received, by mail, a package from an address in Melbourne, Florida, containing the contraband ordered by the UC.

C. The Budlighthouse Gmail Account and the Platplus Tormail Account

The Budlighthouse Gmail Account

35. On or about May 22, 2013, law enforcement obtained a search warrant in the District of New Jersey to search the Budlighthouse Gmail Account. As further detailed below, ROBERSON was identified as the user of the Budlighthouse Gmail Account.

36. Review of the Budlighthouse Gmail Account confirmed that it was in fact associated with the Fakeplastic Website. Review of the account also confirmed that the Fakeplastic Website was designed to automatically send emails to the Budlighthouse Gmail Account, including the details of orders made through the Website.

37. For example, law enforcement's initial review of the Budlighthouse Gmail Account revealed that the account contained approximately 499 emails, from December 2012 through May 2013, which were automatically generated by the Website and sent to the Budlighthouse Gmail Account using the email address "info@fakeplastic.biz" (the "Website Order Emails"). Each of these emails had a subject line beginning with the words "Website Order," followed by an order number and date and time. The body of the emails contained the details of orders placed on the Fakeplastic Website and followed the same basic structure, as outlined below:

- a. As an example, the subject line for one of the Website Order Emails, sent to the Budlighthouse Gmail Account on May 22, 2013, was "Website Order 2113 - 5/23/2013 03:01:42." The body of the email contained the following information: (a) a shipping method for the order; (b) the username of the Fakeplastic Website user placing the order; (c) an address and "Drop Name" to send the order to; and (d) the actual order, which in this case was described as a "29 pcs - Embossing Order," followed by a list of 29 payment card numbers, along with expiration date, a name, and card verification value codes. Law enforcement confirmed with the issuing banks that a number of these accounts have been associated with fraudulent transactions.

38. Review of the "Drop Name" and address information included in the Website Order Emails showed that the names and addresses in those orders generally correlated with mailing labels made with the Fakeplastic Click-N-Ship Account.

The Platplus Tormail Account

39. Review of the Budlighthouse Gmail Account revealed that all of the Website Order Emails identified in that account were sent to two email addresses, the Budlighthouse Gmail Account and platplus@tormail.net (the "Platplus Tormail Account").

40. The Tor network was designed specifically to facilitate anonymous communication over the Internet. Tormail was a free, anonymous e-mail service provider that operated over the Tor network. The Platplus Tormail Account is a Tormail email account. The Tormail email server is not currently operating. While Tormail was operational, it was frequently used by individuals engaged in criminal activity to avoid detection by law enforcement because it allowed users to conceal their true identities and geographic locations.

41. Between July 22, 2013 and August 2, 2013, in connection with an unrelated criminal investigation, the FBI obtained a copy of a computer server located in France via a Mutual Legal Assistance Treaty request to France, which contained data and information from the Tormail email server, including the content of Tormail e-mail accounts.

42. On or about September 24, 2013, law enforcement obtained a search warrant to search the contents of the Platplus Tormail Account, which resided on the seized Tormail server.

43. Search of the Platplus Tormail Account revealed approximately 1,140 Website Order Emails, dated from on or about September 9, 2012 through August 1, 2013, which were sent to both the Platplus Tormail Account and the Budlighthouse Gmail Account. Based on my training and experience, as well as law enforcement's review of the Platplus Tormail Account, there is probable cause to believe that SEAN ROBERSON, who, as explained below, is the administrator of the Fakeplastic Website, used the Platplus Tormail Account as a repository for Website Order Emails generated by the Website. The Platplus Tormail Account contained every Website Order Email found in the Budlighthouse Gmail Account, and more, and appeared to contain every Website Order Email generated by the Website since in or around September 2012 through in or around August 2013.

D. SEAN ROBERSON

44. As described below SEAN ROBERSON was the user of the Budlighthouse Gmail Account and ran the Fakeplastic Website.

ROBERSON was the User of the Budlighthouse Gmail Account

45. SEAN ROBERSON was convicted in 2006 for fraud and related activity in connection with means of identification, in violation of Title 18, United States Code, Section 1028. ROBERSON was convicted for selling counterfeit identification documents on an online criminal forum known as www.shadowcrew.com (the "Shadowcrew Forum"). The Shadowcrew Forum was used, among other things, as an electronic bulletin board for members to advertise and promote the sale of stolen payment card data, bank account information, other personally identifying information, and counterfeit identification documents.

46. Chats and forum postings from the Shadowcrew Forum obtained by law enforcement showed that ROBERSON used the online nickname "GoldCard" on the Shadowcrew Forum, and, in connection with his criminal activity on that forum, referred to his use of the following monikers: "slacker," "slackerxxx," and "slackerX."

47. The user of the Budlighthouse Gmail Account also used the "slacker" moniker. In multiple e-mails from the Budlighthouse Gmail Account, the user of the account was referred to, and referred to himself, as "slacker." The user of the Budlighthouse Gmail Account also appeared to have had a Liberty Reserve² account in the name "Slacker Technologies." Also, a September 30, 2012 e-mail from the account "noreply@doublevpn.com" to the Budlighthouse Gmail Account indicated that the user of the Budlighthouse Gmail Account opened an account with doublevpn.com³ with the login name "slackerplastics."

48. Review of the Budlighthouse Gmail Account also revealed that ROBERSON and his co-conspirators used customized spreadsheets designed to automate the process of printing

² As indicated above Liberty Reserve, its founders, and certain of its officers were recently indicted in the Southern District of New York, 13-cr-368 for, among other things, money laundering.

³ Doublevpn.com provides a proxy service that allows users to hide their true IP address while accessing the Internet.

images and numbers onto counterfeit credit cards. These spreadsheets were called "Embossing Orders.xlsm" (the "Embossing Order Spreadsheets") and over 214 different Embossing Order Spreadsheets were sent from the Budlighthouse Gmail Account.

49. Review of the metadata⁴ for the Embossing Order Spreadsheets revealed that the user who installed the version of Microsoft Excel used to create these spreadsheets entered the name "Sean," without a surname, as his or her name when installing the software. The metadata also showed that the spreadsheets were saved by an individual logged in to a computer under the username "Slacker."

50. The investigation revealed that the user of the Budlighthouse Gmail Account used proxy services, such as doublevpn.com, to hide the user's true IP address. However, law enforcement identified a number of emails in the Budlighthouse Gmail Account indicating the user's true IP address. Law enforcement then compared this IP address to IP addresses used by ROBERSON to conduct online transactions under his real name. On several occasions, the same IP address used by ROBERSON was also used by the user of the Budlighthouse Gmail Account.

51. For example, the Budlighthouse Gmail Account contained a number of emails from Mt. Gox, a widely used Bitcoin exchanger. On or about August 27, 2012, the Budlighthouse Gmail Account received two withdrawal confirmation emails from Mt. Gox indicating that certain withdrawals were made from the IP address 97.104.141.223 (the "Budlighthouse IP Address"). Law enforcement determined that the Budlighthouse IP Address is owned by the internet service provider Bright House Networks Information Services ("BHNIS"), and not a proxy service. On or about July 17, 2013, in response to a federal grand jury subpoena, BHNIS informed law enforcement that it provided internet service to ROBERSON's home.

52. BHNIS indicated that its records only went back to September 14, 2012, and did not go back far enough to determine which of its subscribers was assigned the Budlighthouse IP Address on August 27, 2012, the date of the Mt. Gox withdrawals from the Budlighthouse IP Address.

53. However, through additional investigation, law enforcement discovered an account with the online retailer, Amazon.com, held by SEAN ROBERSON (the "Roberson Amazon Account"). Law enforcement subpoenaed Amazon for, *inter alia*, IP addresses used by ROBERSON to purchase goods online from Amazon. On or about September 23, 2013, in response to a federal grand jury subpoena, Amazon confirmed that the Roberson Amazon Account was accessed approximately 6 times between June 4, 2012 and July 24, 2012, from the Budlighthouse IP Address to make purchases.

54. In sum, the same IP address used by ROBERSON on or about July 24, 2012 to purchase items from Amazon was used by the user of the Budlighthouse Gmail Account on or about August 27, 2012 to make withdrawals from Mt. Gox.

⁴ Metadata is data stored within a file indicating certain attributes regarding the file, such as the date created, the time last accessed, the username of the last individual to access a file, etc.

Purchases Made Through the Roberson Amazon Account

55. Additionally, many of the purchases made through the Roberson Amazon Account were for items commonly used to make fake identification cards and counterfeit payment cards. Moreover, as detailed below, some of the items purchased through the Roberson Amazon Account are referenced in the Budlighthouse Gmail Account.

56. For instance, on or about August 3, 2011, ROBERSON ordered a total of 2,000 white PVC cards with magnetic stripes through the Roberson Amazon Account. Based on my training and experience, these are the types of cards used to create counterfeit payment cards.

57. Additionally, on or about August 25, 2011, ROBERSON ordered 4 rolls of “Fargo 84061 YMCFK Full-Color Ribbon for HDP5000 ID Card Printer” through the Roberson Amazon Account. Based on my training and experience, the HDP5000 ID Card Printer is a high-end printer capable of printing fake identification cards and counterfeit payment cards.

58. Review of the Budlighthouse Gmail Account revealed two emails, dated June 7, 2012 and November 29, 2012, indicating that the user of that account used “YMCFK” film. Additionally, in an April 12, 2012 email sent from the Budlighthouse Gmail Account to a company that provides software used to print and encode cards, ROBERSON indicated that, “[c]urrently we are using 2 HDP5000 printers.”

ROBERSON’s Trip to Dollywood

59. The investigation revealed that the Fakeplastic Website was down from December 22, 2012 through January 6, 2013. This was indicated in the “Current News” section of the Website upon logging in.

60. Review of the Budlighthouse Gmail Account revealed that an email auto response was sent out from the account from December 22, 2012 through January 4, 2013. The body of the response stated: “Will respond to your message when I return from vacation. Sorry for the inconvenience but I need an escape also :)” Although no auto response emails were generated after January 4, 2013, no emails were sent from the Budlighthouse Gmail Account until January 8, 2013.

61. In or around August 2013, pursuant to a federal grand jury subpoena, law enforcement obtained credit card statements from Discover for ROBERSON’s wife. The credit card statements included charges from December 19, 2012 through January 7, 2013. Those charges indicated that ROBERSON’s wife travelled by car to, and stayed at, a hotel in Lake Buena Florida on December 22, 2012, then drove through Georgia to Tennessee, and ultimately stayed at Dollywood, a resort and amusement park in Tennessee, during the time period that the Fakeplastic Website was down and during the time that the Budlighthouse Gmail Account was sending out auto responses. The Discover charges also indicated that by January 6, 2013, ROBERSON’s wife was back in Palm Bay, Florida. Law enforcement also identified a photograph of SEAN ROBERSON with his wife and others in Dollywood, posted on the

Facebook page of SEAN ROBERSON's mother. Therefore, there is probable cause to believe that ROBERSON was with his wife during this trip, during the time that the Fakeplastic Website and the Budlighthouse Gmail Account were unattended.

E. Vinicio Gonzalez

62. The investigation also revealed that mailings associated with the Fakeplastic Website were mailed out from a post office in Melbourne, Florida, by Vinicio Gonzalez.

63. On or about June 12, 2013, the USPS obtained a search warrant in the Middle District of Florida, to use a GPS device ("Tracking Device #1") on Gonzalez's vehicle to track his movements. On or about November 18, 2013, the USPS obtained additional search warrant in the Middle District of Florida, to use a GPS device ("Tracking Device #2") on Gonzalez's vehicle to continue to track his movements.

64. On or about June 13, 2013, law enforcement conducted surveillance of Gonzalez. Gonzalez was observed exiting a Babcock Storage unit located in Palm Bay, Florida (the "Babcock Storage Unit") with several express mail envelopes under his arm. Law enforcement then observed Gonzalez go to a post office in Melbourne, Florida, and had USPS personnel at that location provide photocopies of the mailings deposited by Gonzalez. USPS records confirmed that the mailing labels used on these mailings were created from the Fakeplastic Click-N-Ship Account.

65. Data obtained from Tracking Device #1 showed that Gonzalez frequently visited ROBERSON's home. For instance, GPS data from the device showed that Gonzalez visited ROBERSON's home on or about the following dates: June 14, 2013; June 19, 2013; June 21, 2013; June 24, 2013; June 25, 2013; June 26, 2013; July 2, 2013; July 5, 2013; July 10, 2013; and July 16, 2013. The Fakeplastic Click-N-Ship Account was used to create tracking numbers for approximately 109 parcels for Fakeplastic Website orders that were shipped during this time period, from June 14, 2013 through July 16, 2013.

66. On or about November 19, 2013, law enforcement conducted additional surveillance of Gonzalez and observed Gonzalez drive from his residence that morning to Inksplat. After spending approximately thirty minutes at that location, Gonzalez was then observed leaving Inksplat at approximately 10:55 a.m. and driving directly to an "Ample Storage" storage facility where he entered a storage unit (the "Ample Storage Unit") located in Melbourne, Florida. After spending over an hour at a unit in the Ample Storage Unit, Gonzalez was observed leaving the facility at approximately 1:55 p.m. carrying several express mail envelopes. Gonzalez was then observed entering a post office in Melbourne, Florida. USPS personnel at that location provided law enforcement with photocopies of the mailings deposited by Gonzalez. USPS records confirmed that the mailing labels used on these mailings were created from the Fakeplastic Click-N-Ship Account.

67. On or about November 20, 2013, law enforcement continued its surveillance of Gonzalez and observed him exit his home. Data obtained from Tracking Device #2 confirmed that Gonzalez drove to the Ample Storage Unit. Gonzalez arrived at the Ample Storage Unit at

approximately 11:29 a.m. Gonzalez then departed from the Ample Storage Unit at approximately 1:14 p.m. Data from Tracking Device #2 indicated that Gonzalez drove to the post office in Melbourne at approximately 3:18 p.m. that day. Later that day, law enforcement received a call from USPS personnel at the post office in Melbourne, confirming that three additional mailings, with tracking numbers generated by the Fakeplastic Click-N-Ship Account, were received at the post office. Data from Tracking Device #2 also indicated that after leaving the post office, Gonzalez drove to ROBERSON's home and stayed at that location from approximately 3:35 p.m. to 5:58 p.m.

F. Hugo Rebaza

68. As further described below, Rebaza was responsible for picking up packages of contraband and criminal proceeds delivered to the Co-Conspirators at one or more CMRAs.

69. Review of the Budlighthouse Gmail Account revealed that the Co-Conspirators used a number of CMRAs to receive payment for contraband ordered through the Website, and to receive orders of holographic overlays from individuals overseas, to resell to their customers.

- a. For example, in a May 2, 2013 email from the Budlighthouse Gmail Account to another email address associated with a Co-Conspirator in China ("CC-1"), ROBERSON requested a total of "20,000 hologram overlays" for the following ten states: Delaware; Florida; Ohio; Connecticut; Illinois; Kentucky; Maryland; Mississippi; New Jersey; and South Carolina. In response, CC-1 quoted a price of "6100USD." Based on my training and experience, as well as the context of the communication, there is probable cause to believe that ROBERSON was referring to the purchase of holographic overlays to be used in connection with the creation of fake identifications.
- b. Subsequently, in a May 8, 2013 email from the Budlighthouse Gmail Account to CC-1, ROBERSON indicated that payment for the holographic overlays would be sent in three separate wires to locations overseas, and asked that the holographic overlays be sent to a name, "Jose Lima," at an address for a CMRA in West Melbourne, Florida.

70. Review of the Budlighthouse Gmail Account also revealed that the Co-Conspirators used CMRAs to receive payment for orders of contraband ordered through the Website.

- a. For example, in a January 2013 email exchange between ROBERSON, using the Budlighthouse Gmail Account, and another Co-Conspirator ("CC-2"), CC-2 referred to various orders CC-2 placed with ROBERSON for counterfeit payment cards. At the end of the exchange, in an email dated January 29, 2013, ROBERSON indicated that he would be filling some of CC-2's orders for counterfeit payment cards, and added "[a]lso worker got ID today so hopefully tonight will get the box open." In a follow up e-mail sent later that

same day, ROBERSON provided the name "Jose Lima" and an address for a CMRA in Indialantic, Florida (the "Indialantic CMRA").

71. Law enforcement confirmed that the address provided for the Indialantic CMRA is indeed the address for a mailbox at a CMRA called "Atlantic Pack & Parcel." In response to a USPS inquiry, Atlantic Pack & Parcel confirmed that the Indialantic CMRA mailbox address referenced in the email above was opened by an individual under the name "Jose Lima" and provided copies of the account-opening documents, including copies of the identification provided by the individual who opened the account.

72. The records relating to the Indialantic CMRA mailbox account revealed that the account was opened on or about January 29, 2013, as indicated in ROBERSON's email described above.

73. Law enforcement's review of the identification card used to open the Indialantic CMRA mailbox account revealed that it was a fake New Jersey driver's license in the name of "Jose Lima." Comparison of the image on the fake driver's license, surveillance video from Atlantic Pack & Parcel showing the individual picking up parcels from the Indialantic CMRA mailbox, and DMV records, revealed that the individual pictured in the fake identification and seen on the surveillance video accessing the Indialantic CMRA mailbox is Rebaza.

74. Additionally, on or about July 26, 2013, the owner of the Atlantic Pack & Parcel advised law enforcement that the individual who rented the Indialantic CMRA mailbox came in to the Atlantic Pack & Parcel and picked up a Federal Express parcel that was mailed to the Indialantic CMRA mailbox. The owner advised that the individual was driving a Tan Dodge Durango and provided the license plate number for the vehicle. Florida DMV records revealed that the vehicle was registered to Rebaza.

G. Searches of ROBERSON's Home and the Ample Storage Facility

75. On or about December 4, 2013, and pursuant to search warrants obtained in the Middle District of Florida, law enforcement searched, *inter alia*, ROBERSON's home and the Ample Storage Facility.

76. In connection with its search, law enforcement observed Gonzalez entering the Ample Storage Facility and arrested him while he was in the process of opening the rolling, garage-style door to the storage unit. The search revealed that the storage facility had been used as a counterfeit payment card plant to manufacture the counterfeit payment cards, and to prepare delivery of holographic stickers and holographic overlays, sold through the Website. Among other items, law enforcement found and seized counterfeit cards (see Exhibits I & J), computers configured to print counterfeit cards (see Exhibit K), storage closets of supplies used to create the counterfeit cards (see Exhibit L), and printers used to print and emboss counterfeit cards (see Exhibits M, N & O).

77. Law enforcement also searched ROBERSON's home and arrested him that same day. Law enforcement found and seized a number of computers, blank plastic cards used to

make counterfeit payment cards, and at least one fake identification card from ROBERSON's home. Search of ROBERSON's computers revealed an encrypted file containing ROBERSON's login credentials for the Fakeplastic Website, the Budlighthouse Gmail Account, as well as other accounts. Indeed, the encrypted file also contained a spreadsheet with a detailed accounting of ROBERSON's gross receipts, as well as his expenses, related to the Website and his criminal activity from April 2011 through December 2013.

H. Law Enforcement's Assumption of Control of the Website

78. Since on or about December 5, 2013, the FBI and USPIS assumed control of the Fakeplastic Website as well as the Budlighthouse Gmail Account and has been taking orders from the Website's members.

79. Since on or about December 5, 2013, the Website received over 50 orders requesting the purchase of, in the aggregate, over 1,500 counterfeit payment cards, over 550 state identification overlays, and 1,030 holographic stickers.

80. Upon receiving these orders, the USPIS, in coordination with federal, state, and local prosecutors' offices around the country, conducted over 30 controlled deliveries, leading to 11 additional arrests and the seizure of approximately 3 counterfeit payment card plants. In connection with these controlled deliveries and related searches, law enforcement has seized over 700 counterfeit payment cards, 10 pieces of fake identification, multiple illegally-possessioned firearms, and controlled substances.

EXHIBIT A

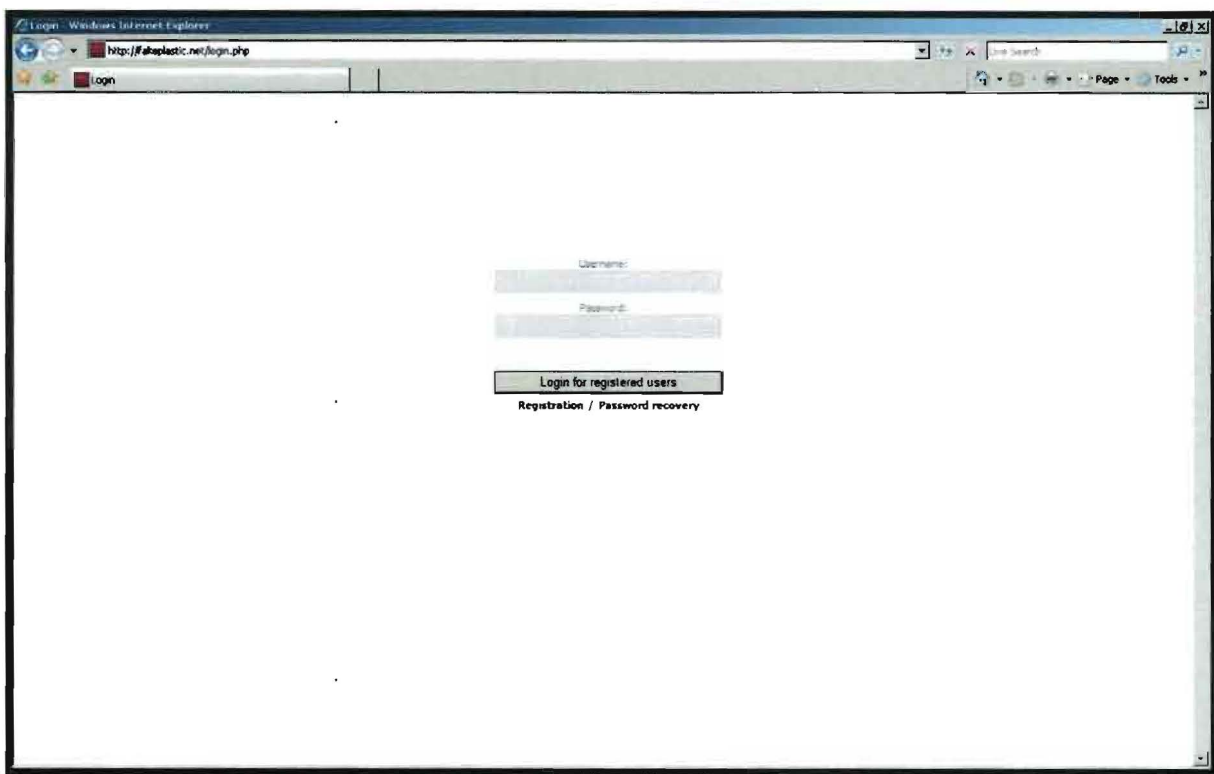


EXHIBIT B



FAKEPLASTIC.NET
carders supply shop

Items: 0 Price: \$0.00

Hello, [log out](#)

[HOME](#)

[ORDER HISTORY](#)

[PROFILE](#)

[SUPPORT](#)

[CHECKOUT](#)

Product categories

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

Now Accepting ...



HOME

Welcome to Fakeplastics.biz We have the best quality plastics and holograms available to the public.

We strive to get your orders in your hands as quick as possible. In most cases, we will ship your order within 24-48 hours of your payment.

We do have bulk pricing on all our products. Pricing will automatically update in the shopping cart when your quantities are updated.

This is a private site and we ask that you keep it that way. If you trust someone then let them know. But what we do not need, is too many people knowing this site exists and making many attempts to shut it down.

CURRENT INVENTORY:

Blanks: 3113
Holograms: 57087
Overlays: 14336

CURRENT COUPONS:

CURRENT NEWS:

7/24/13

VISA holas back in stock. Everything stocked at this point. Enjoy!

07.16.13

We are officially out of stock for VISA STICKERS. We cannot ship out any orders for visa blanks or embossed. We expect them in a few days. More than likely early next week. We apologize for the outage. If you need stuff asap then get Mastercard, Amex, or Discover and we can ship as normal.

05.28.13

We attempted to setup a PerfectMoney account for you guys to use but after 1 payment it was locked. It is unfortunate, but we will only be able to accept Bitcoin going forward. Use any popular exchanger to convert your money to bitcoin. You can have it send to us directly if you rather not hold bitcoins. Simply place your order, after payment you will be given a page with information of how much bitcoin to send and the address to send it to. After your money is sent, our site will automatically update your status to PAID.

05.22.13

So for anyone that has not heard. Liberty Reserve was shutdown indefinitely for Money Laundering. What does this mean for fakeplastic??? It means we are going to accept Bitcoin as our primary payment system. What about PerfectMoney or Webmoney??? These sites are well known for shutting off accounts and freezing funds. It is only a matter of time before the US shuts down PerfectMoney for the same reasons they did LR.

I strongly urge everyone who is working in our line of work to start using Bitcoin. Bitcoin cannot be shutdown by any person or government, it cannot track your ass down, it is anonymous and safe! It is why SilfRoad (largest drug buying marketplace) has always used Bitcoin as a payment processor.

EXHIBIT C

Product categories

- All
- Blank plastic
- Canada
- Philippines
- UK
- Embossed Plastic
- Hologram
- ID Overlays
- Misc

SAMPLES - ID Overlays

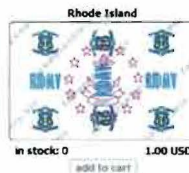
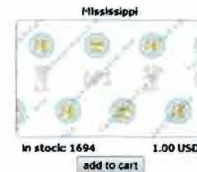
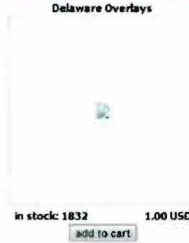


EXHIBIT D



EXHIBIT E



FAKEPLASTIC.NET
carders supply shop

Items: 0 Price: \$0.00

Hello,

[log out](#)

[HOME](#)

[ORDER HISTORY](#)

[PROFILE](#)

[SUPPORT](#)

[CHECKOUT](#)

Product categories

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

Now Accepting ...



SAMPLES - Blank plastic

Amex Citi Aadvantage



in stock: 35 12.00 USD

[add to cart](#)

Amex Green



in stock: 18 12.00 USD

[add to cart](#)

Amex Optima



in stock: 41 12.00 USD

[add to cart](#)

Barclays Black



in stock: 15 12.00 USD

[add to cart](#)

Barclay Card



in stock: 95 12.00 USD

[add to cart](#)

BOA Alaska Airlines



in stock: 12 12.00 USD

[add to cart](#)

EXHIBIT F



FAKEPLASTIC.NET
carders supply shop

Items: 0 Price: \$0.00

Hello,

[log out](#)

[HOME](#)

[ORDER HISTORY](#)

[PROFILE](#)

[SUPPORT](#)

[CHECKOUT](#)

Product categories

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

Now Accepting ...



SAMPLES - Holograms

Visa Stickers - Small Silver



in stock: 4970 1.00 USD

[add to cart](#)

Visa Stickers - Large Silver



in stock: 99 1.00 USD

[add to cart](#)

Visa Stickers - Large Gold



in stock: 2108 1.00 USD

[add to cart](#)

Visa Stickers - Small Gold



in stock: 10956 1.00 USD

[add to cart](#)

Master Card Stickers - Silver



in stock: 5232 1.00 USD

[add to cart](#)

Master Card Stickers - Gold



in stock: 7824 1.00 USD

[add to cart](#)

Discover Stickers - Silver



in stock: 25898 1.00 USD

[add to cart](#)

EXHIBIT G



FAKEPLASTIC.NET
carders supply shop

Items: 0 Price: \$0.00

Hello,

[log out](#)

[HOME](#)

[ORDER HISTORY](#)

[PROFILE](#)

[SUPPORT](#)

[CHECKOUT](#)

Product categories

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

Now Accepting ...



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.

5340404069849851,1605,James Davis,739
5525415613790653,1407,James Davis,926
5568322421255903,1408,James Davis,327
5214273506980782,1501,James Davis,617
527381008381540,1412,James Davis,214
5245900476363624,1507,James Davis,863
5145057671975832,1511,James Davis,463

[Check Embossing Info](#)

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

EXHIBIT H

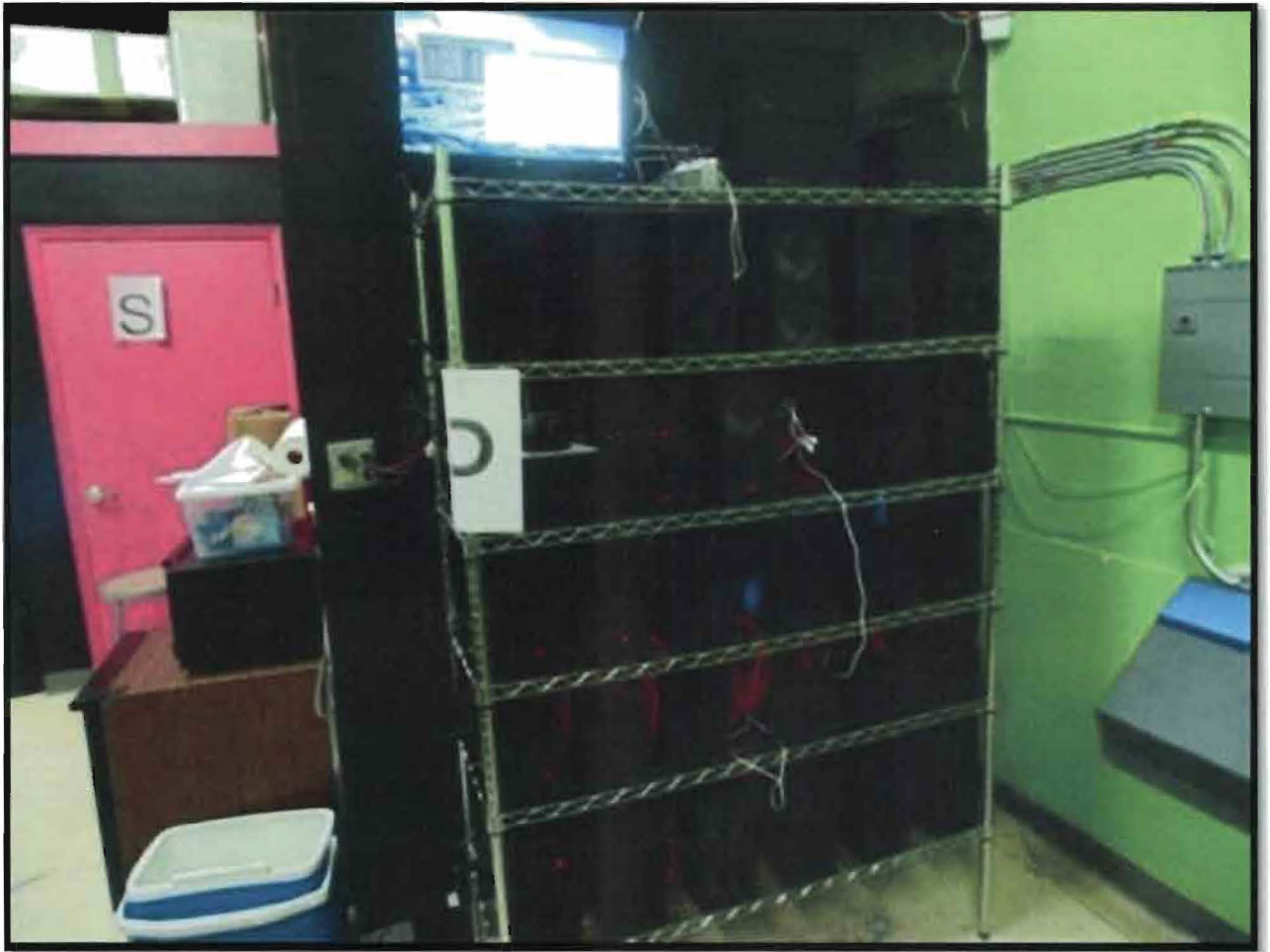


EXHIBIT I

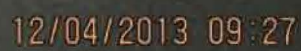


EXHIBIT J



EXHIBIT K



EXHIBIT L



EXHIBIT M



EXHIBIT N



EXHIBIT O

