


Approved:   
TIMOTHY T. HOWARD  
Assistant United States Attorney

Before: HONORABLE JAMES C. FRANCIS IV  
United States Magistrate Judge  
Southern District of New York

- - - - - x  
UNITED STATES OF AMERICA : COMPLAINT  
:   
- v. - : Violation of  
: 18 U.S.C. § 1029(a)(3),  
MIR ISLAM, : 1029(a)(5), 1029(b)(1)  
a/k/a "JoshTheGod," : and 2  
a/k/a "Ijew," :   
a/k/a "Josh Matthews," : COUNTY OF OFFENSE:  
a/k/a "Robert Whitetaker," : New York  
a/k/a "josh@obbahhost.com," :   
Defendant. :   
:   
- - - - - x

SOUTHERN DISTRICT OF NEW YORK, ss.:

DENNIS J. KAMPH, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

**COUNT ONE**  
**(Attempted Access Device Fraud)**

1. From at least on or about June 13, 2012, through at least on or about June 25, 2012, in in the Southern District of New York and elsewhere, MIR ISLAM, a/k/a "JoshTheGod," a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," the defendant, knowingly and with intent to defraud, and affecting interstate and foreign commerce, attempted to possess fifteen and more devices which were unauthorized access devices, to wit, ISLAM took possession of what he believed to be fifteen counterfeit cards containing stolen American Express credit card numbers.

(Title 18, United States Code, Section 1029(a)(3), 1029(b)(1) and 2.)

COUNT TWO  
(Access Device Fraud)

2. From at least on or about June 13, 2012, through at least on or about June 25, 2012, in in the Southern District of New York and elsewhere, MIR ISLAM, a/k/a "JoshTheGod," a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," the defendant, knowingly and with intent to defraud, and affecting interstate and foreign commerce, effected and attempted to effect transactions, with one and more access devices issued to another person or persons, to receive payment and any other thing of value during any 1-year period the aggregate value of which is equal to and greater than \$1,000, to wit, ISLAM took possession of what he believed to be fifteen counterfeit cards containing stolen American Express credit card numbers, with the purpose of obtaining at least \$1,000 of goods and services.

(Title 18, United States Code, Section 1029(a)(5), 1029(b)(1) and 2.)

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

3. I have been personally involved in the investigation of this matter. This affidavit is based upon my investigation, my conversations with other law enforcement agents, and my examination of reports and records. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

4. I have been a Special Agent with the FBI for approximately one and a half years. Since approximately February 2012, I have been assigned to the computer intrusion squad in the FBI's New York Field Office. I have received training regarding computer technology, computer fraud, and white collar crimes.

Background on the UC Site

5. Based on my training and experience, I have learned the following:

a. Carding: "Carding" refers to various criminal activities associated with stealing personal identification information and financial information belonging to other individuals - including the account information associated with credit cards, bank cards, debit cards, or other access devices - and using that information to obtain money, goods, or services without the victims' authorization or consent. For example, a criminal might gain unauthorized access to (or "hack") a database maintained on a computer server and steal credit card numbers and other personal information stored in that database. The criminal can then use the stolen information to, among other things: (1) buy goods or services online; (2) manufacture counterfeit credit cards by encoding them with the stolen account information; (3) manufacture false identification documents (which can be used in turn to facilitate fraudulent purchases); or (4) sell the stolen information to others who intend to use it for criminal purposes. "Carding" refers to the foregoing criminal activity generally and encompasses a variety of federal offenses, including, but not limited to, identification document fraud, aggravated identity theft, access device fraud, computer hacking, wire fraud, and bank fraud.

b. Carding Forums: "Carding forums" are websites used by criminals engaged in carding ("carders") to facilitate their criminal activity. Carders use carding forums to, among other things: (1) exchange information related to carding, such as information concerning hacking methods or computer-security vulnerabilities that could be used to obtain personal identification information; and (2) buy and sell goods and services related to carding, for example, stolen credit card or debit card account numbers, hardware for creating counterfeit credit cards or debit cards, or goods bought with compromised credit card and debit card accounts. Carding forums often permit users to post public messages (postings that can be viewed by all users of the site), sometimes referred to as "threads." For example, a user who has stolen credit card numbers may post a public "thread" offering to sell the numbers. Carding forums also often permit users to communicate one-to-one through so-called "private messages." Because carding forums are, in essence, marketplaces for illegal activities, access is typically restricted to avoid law enforcement surveillance. Typically, a prospective user seeking to join a carding forum can only do so if other, already established users "vouch" for the prospective user, or if the prospective user pays a sum of money to the operators of the carding forum. User accounts are typically identified by a username and access is restricted by

password. Users of carding forums typically identify themselves on such forums using aliases or online nicknames ("nics").

6. Based on my participation in the investigation of this matter, I know the following:

a. In or about June 2010, the FBI established an undercover carding forum (the "UC Site"), enabling users to discuss various topics related to carding and to communicate offers to buy, sell, and exchange goods and services related to carding, among other things.

b. The FBI established the UC Site as an online meeting place where the FBI could locate cybercriminals, investigate and identify them, and disrupt their activities.<sup>1</sup> The UC Site was configured to allow the FBI to monitor and to record the discussion threads posted to the site, as well as private messages sent through the site between registered users. The UC Site also allowed the FBI to record the Internet protocol ("IP") addresses of users' computers when they accessed the site.<sup>2</sup>

c. Access to the UC Site was limited to registered members and required a username and password to gain entry. Various membership requirements were imposed from time to time to restrict site membership to individuals with established knowledge of carding techniques or interest in criminal activity. For example, at times new users were prevented from joining the site unless they were recommended by two existing users who had registered with the site, or unless they paid a registration fee.

d. New users registering with the UC Site were required to provide a valid e-mail address as part of the registration process. An e-mail message was sent to that email address containing registration instructions. In order to complete the registration process, the new user was required to open the e-mail, click on a link in it, and then enter an activation code specified in the e-mail message. The e-mail

---

<sup>1</sup> The registration process for the UC Site required users to agree to terms and conditions, including that their activities on the UC Site were subject to monitoring for any purpose.

<sup>2</sup> Every computer on the Internet is identified by a unique number called an Internet protocol ("IP") address, which is used to route information properly between computers.

addresses entered by registered members of the site were collected by the FBI.

e. In the course of the undercover operation, the FBI contacted multiple affected institutions and/or individuals to advise them of discovered breaches in order to enable them to take appropriate responsive and protective measures. Based on information obtained through the site, the FBI estimates that it helped financial institutions prevent many millions of dollars in losses from credit card fraud and other criminal activity, and has alerted specific individuals regarding breaches of their personal email or other accounts.

f. At all times relevant to this Complaint, the server for the UC Site, through which all public and private messages on the UC Site were transmitted, was located in New York, New York.

#### Background on "Ijew"

7. On or about September 10, 2010, an individual registered with the UC Site under the nickname "Ijew." "Ijew" provided his e-mail address as "Sabbir1234567890@gmail.com" ("E-Mail Account-1") for the purpose of receiving registration instructions. As detailed below, this individual has been identified as MIR ISLAM, a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," a/k/a "JoshTheGod," the defendant. The investigation has further revealed that ISLAM is involved with, among other things, receiving, possessing, using and distributing stolen credit card numbers.

8. On or about September 10, 2010, "Ijew" posted a message on the UC Site, stating, "Tell me what you want to card and il tell you the site to use ;) and first 3 ppl to ask il give free us cards."<sup>3</sup> Based on my training and experience investigating carding crimes, and my familiarity with this investigation, I believe that in this message, "Ijew" offered to give advice to other members of the UC Site as to which Internet websites were best to card various types of commercial products, and offered to provide information for stolen United States-based credit cards ("free us cards") to the first three people who responded to his posting.

---

<sup>3</sup> Quotations from emails and online postings are reproduced substantially as they appear in the original text; that is, errors in spelling and punctuation have not been corrected.

9. On or about September 10, 2010, another member of the UC Site ("Member-1") responded to the post discussed above in paragraph 8, with a posting stating "What is a website that you can card Ipods." "Ijew" responded with a posting, which stated, "Ipds just card it directly from apple.com card it within \$350 and they wont ask for verification :D and pm me for card bro and rep me if you lovez me." Based on my training and experience investigating carding crimes, and my familiarity with this investigation, I believe that in this message, MEMBER-1 asked "Ijew" for advice on the best website to card Apple iPod portable music players. Further, I believe "Ijew" informed MEMBER-1 that the best website was Apple.com, so long as he kept his order under \$350 in United States currency, because Apple.com would not ask for verification of any stolen credit cards used to card items under that threshold. Finally, I believe that "Ijew" instructed MEMBER-1 to send him a private message ("pm me") to get a free stolen credit card number, and asked that MEMBER-1 make a public posting on the UC Site to promote "Ijew"'s reputation ("rep me"). Later that day, MEMBER-1 sent a message to "Ijew" using the UC's private message system, requesting a "free cw," and "Ijew" responded by providing a credit card number, with the associated customer name and address.

10. On or about September 11, 2010, another member of the UC Site ("MEMBER-2") sent a private message to "Ijew," which stated "u have any I can have bro?" "Ijew" responded, "don't have any free ones atm bro sorry." MEMBER-2 responded, "for sale?" and "Ijew" later responded, "I sell at \$4 per cc." Based on my training and experience investigating carding crimes, and my familiarity with this investigation, I believe that in this series of private messages, MEMBER-2 asked "Ijew" for free stolen credit card information, and "Ijew" informed MEMBER-2 that he did not have any to distribute for free, at the moment ("atm"). Further, I believe that "Ijew" told MEMBER-2 that he was willing to sell stolen credit information for \$4 per stolen card ("\$4 per cc").

11. On or about February 24, 2012, the Honorable Frank Maas, United States Magistrate Judge, authorized a search of E-Mail Account-1. I have reviewed the contents of E-Mail Account-1, and have discovered an e-mail dated on or about March 21, 2011, from another e-mail account to E-Mail Account-1, which included information for over 50,000 credit cards belonging to different individuals, including associated customer information, including, among other things, the customer's name, credit card number, and address. I have reviewed records

provided by Discover, and I have confirmed that at least approximately 20 of these credit card numbers corresponded to genuine Discover accounts belonging to someone other than MIR ISLAM, a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," a/k/a "JoshTheGod," the defendant. Further, based on my training and experience investigating carding crimes, and my familiarity with this investigation, I believe that these were stolen credit card numbers based on the volume, format and manner in which they were sent to E-Mail Account-1.<sup>4</sup>

Identification of MIR ISLAM, a/k/a "JoshTheGod,"  
a/k/a "Ijew," a/k/a "Josh Matthews,"  
a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com"

12. On or about November 23, 2011, "Ijew" sent a message to another member of the UC Site ("MEMBER-3"), providing, among other things, an address of a specific apartment in Bronx, New York ("Apartment-1"), along with a receipt for an online Internet payment.

13. On or about December 10, 2011, "Ijew" accessed the UC Site from a specific Internet Protocol address<sup>5</sup> ending in "195." ("IP Address-1"). I have reviewed records maintained by Optimum Online, an Internet Service provider. According to those records, on or about December 10, 2011, at the time that "Ijew" accessed the UC site as described in this paragraph, an IP Address-1 was assigned to a computer located at Apartment-1.

14. As noted above in paragraph 7, "Ijew" used E-Mail Account-1 to register for the UC Site. During my review of the contents of E-Mail Account-1, I discovered an outgoing e-mail dated on or about February 26, 2011, sent from E-Mail Account-1 entitled "id card" which contained the name "Josh Matthews," address, weight, gender, date of birth ("IJEW DOB"), and attached an image ("IJEW PHOTO"). In addition, the e-mail stated, "id numb - any." Based on my training and experience investigating carding crimes, and my familiarity with this investigation, I believe that in this message, "Ijew" was

---

<sup>4</sup> Upon discovery of this e-mail, the FBI promptly provided notification to American Express, Visa, MasterCard and Discover that these credit card accounts may have been compromised.

<sup>5</sup> An Internet Protocol address, also referred to as an "IP address," refers to a unique number used by a computer to access the Internet.

sending his photo, along with other personal information, in order to obtain a fraudulent identification card in the name "Josh Matthews." From my training and experience, I know that carders frequently seek fraudulent identification documents under aliases, so that they can use stolen credit information that has been encoded on cards embossed with their alias at physical stores where they can make point-of-sale purchases. Further, as set forth below in paragraph 16, further investigation has revealed that "Ijew" has claimed to have fraudulent identification documents in other names. Accordingly, I believe that the IJEW PHOTO depicts "Ijew".

#### American Express Credit Card Fraud Scheme

15. On or about June 13, 2012, an undercover FBI agent ("UC-1"), pretending to be a worker in a retail store with access to customer information) had an online conversation on Microsoft MSN Messenger, an online messaging service, with an individual using the account "josh@obbahhost.com." As discussed below, the investigation has shown that "josh@obbahhost.com" is another online alias used by MIR ISLAM, a/k/a "JoshTheGod," a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," the defendant. During that conversation, in sum and in part, ISLAM informed UC-1 that he "found a new method when we get dumps . . . to make millions . . . \$10k a day." Based on my training and experience investigating carding crimes, I know that "dumps" is a term used by carders to reference stolen credit card information. Accordingly, I believe that in this message, ISLAM informed UC-1 that he had discovered a new way to obtain stolen credit card information ("dumps") that could be used to make approximately \$10,000 in United States currency per day. Later in the conversation, ISLAM informed UC-1 that there is only a "certin [sic] type of card that only works . . . amexs" and asked that UC-1 "get as many as u can." I believe that in these messages, ISLAM informed UC-1 that the carding scheme required American Express credit cards ("amexs"). In other online chats, which I reviewed, ISLAM requested that UC-1 ("Amex dumps") for the purpose of the scheme ("AMEX FRAUD SCHEME").

16. On or about June 16, 2012, UC-1 had another online conversation with MIR ISLAM, a/k/a "JoshTheGod," a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," the defendant, on MSN Messenger, during which, in sum and in part, ISLAM told UC-1: "so um put the track data in the cards emboss them." Later in the conversation, ISLAM stated, that he knew a store in Virginia that "doesn't



have any high verification for amex . . . we gonna be getting visa gift cards." Later, ISLAM stated "emboss the card . . .the name on it has to match id name." Based on my training and experience investigating carding crimes, and my familiarity with this investigation, I believe that in this discussion, ISLAM discussed the AMEX FRAUD SCHEME and informed UC-1 that he knew a store located in Virginia where they could use American Express cards to purchase Visa gift cards, and he instructed UC-1 to encode cards with stolen American Express account numbers. Further, ISLAM instructed UC-1 to emboss the cards with names matching fake identifications ("emboss the card . . .the name on it has to match id name"). Later in the conversation, ISLAM informed UC-1, in sum and substance that he had a "fake id" in the name "Robert Whitetaker." Based on my training and experience, I know that individuals involved in carding frequently encode cards with stolen data that are embossed with names matching fake identification cards, so that if used in a point-of-sale purchase, the carder can show the fake identification to verify his or her fraudulent identity.

17. On or about June 18, 2012, UC-1 had another online conversation with MIR ISLAM, a/k/a "JoshTheGod," a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," the defendant, on MSN Messenger, during which, in sum and in part, ISLAM provided two credit card numbers, belonging to two different individuals, along with associated CVV numbers, addresses and phone numbers. Based on my training and experience in carding crimes, and my familiarity with this investigation, I believe that in this message, ISLAM provided UC-1 with one stolen American Express credit card number and one stolen Mastercard number. From speaking with a representative of American Express, I have confirmed that the American Express credit card number corresponded to a genuine American Express account belonging to someone other than ISLAM. ISLAM indicated that he had obtained these numbers from "pawnshop.cc," which I know, based on my training and experience, to be another carding website, similar to the UC Site. Further, during this conversation, ISLAM indicated, in sum and substance, that he wanted to travel to Virginia with UC-1 on or about June 25, 2012 or June 26, 2012, and that "money isnt an issue . . . nah money wont ever e an issue." Based on my familiarity with this investigation, I believe that ISLAM was proposing a trip to Virginia with the UC for the purpose of executing the AMEX FRAUD SCHEME.

18. On or about June 19, 2012, I accompanied several Detectives with the New York City Police Department ("NYPD"), as

they knocked on the door of Apartment-1 and identified themselves as police, and mentioned, in a ruse, that they were investigating an unrelated crime. I observed MIR ISLAM, a/k/a "JoshTheGod," a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," the defendant, answer the door, and identify himself as "Mir Islam." ISLAM's appearance matched the IJEW PHOTO.

19. On or about June 20, 2012, at the direction MIR ISLAM, a/k/a "JoshTheGod," a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," the defendant, UC-1 had another online conversation with ISLAM on another online messaging service, pursuant to ISLAM's direction to use the other service. According to UC-1, during that conversation, ISLAM informed UC-1, in sum and in part, that the police had come to his door the previous day and had asked him about an unrelated crime.

20. On or about June 23, 2012, UC-1 had another online conversation with MIR ISLAM, a/k/a "JoshTheGod," a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," the defendant, on MSN Messenger, during which, in sum and in part, ISLAM asked UC-1, "how many cards did u skim." UC-1 responded, "15". ISLAM then asked UC-1, "how many pins u got." UC-1 responded, "9." Later in the conversation, ISLAM and UC-1 discussed traveling to Virginia on or about June 25, 2012 or June 26, 2012, and stated, in part, "take ur embosser n shit we might need it there." UC-1 responded, "Ok.. sweet but I dont got no more trak data." ISLAM responded, "that's not a problem il buy the track data." Based on my training and experience with carding crimes, and my familiarity with this investigation, I believe that ISLAM wanted to know how many stolen American Express cards UC-1 was able to obtain ("how many cards did u skim"), and how many personal identification numbers ("PINS") UC-1 was able to steal. I know, from my training and experience, that an individual with a stolen credit card number and associated PIN number can use that information at an Automated Teller Machine ("ATM") to make unauthorized cash withdrawals. Finally, during this conversation, I believe that ISLAM discussed the AMEX FRAUD SCHEME and asked UC-1 to bring an embosser, a device that can be used to make counterfeit credit cards, because they might need it in Virginia to commit further fraud. UC-1 responded that he could bring the embosser, but that he did not have any access to any more stolen credit card information ("I don't got no more trak data"), and ISLAM responded that he would be able to buy additional stolen credit card numbers ("il buy the track data").

21. On or about June 24, 2012, UC-1 had another online conversation with MIR ISLAM, a/k/a "JoshTheGod," a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," the defendant, on MSN Messenger, during which, in sum and in part, UC-1 asked ISLAM "wat should I bring wit me to va." ISLAM responded, in sum and in part, "bring the msr n embosser." Based on my training and experience with carding crimes, and my familiarity with this investigation, I believe that during this conversation, ISLAM confirmed that UC-1 should bring an embosser for the upcoming trip to Virginia, and also requested that UC-1 bring a magnetic strip reader ("MSR") as well. I know, from my training and experience, that individuals involved in carding crimes use magnetic strip readers to encode blank cards with stolen credit card information, in order to make counterfeit credit cards.

22. On or about June 25, 2012, at approximately 5:30 p.m., UC-1 had a conversation with MIR ISLAM, a/k/a "JoshTheGod," a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," the defendant, on an online messaging service. During that conversation, ISLAM indicated, in sum and in part, that he was going to run an errand later that day at a store in the vicinity of 34<sup>th</sup> Street between 7<sup>th</sup> and 8<sup>th</sup> Avenues in New York, New York. ISLAM and UC-1 agreed to meet at that location, and ISLAM instructed UC-1 to send ISLAM a text message to a cellular telephone with a number ending in 1346 (the "1346 PHONE") once UC-1 had arrived.

23. At approximately 7:05 p.m., other FBI agents established surveillance of the vicinity of 34<sup>th</sup> Street between 8<sup>th</sup> and 9<sup>th</sup> Avenue, in New York, New York. At approximately the same time, UC-1 sent a text message to MIR ISLAM, a/k/a "JoshTheGod," a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," the defendant, on the 1346 PHONE, indicating, in sum and in part, that he had arrived. By approximately 7:25 p.m., ISLAM approached UC-1. This meeting was surveilled by FBI agents and also audio recorded. ISLAM displayed a Florida Driver's License to UC-1, in the name "Robert Whitetaker." As discussed above in paragraph 16, ISLAM had instructed UC-1 to emboss counterfeit American Express cards in the name "Robert Whitetaker," so that he could use the stolen information in order to engage in carding at retail stores as part of the AMEX FRAUD SCHEME. ISLAM then entered a liquor store, and purchased two bottles of alcohol.

24. At approximately 7:55 p.m., UC-1 and MIR ISLAM, a/k/a "JoshTheGod," a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," the defendant, entered a Dunkin' Donuts in the vicinity of 37<sup>th</sup> Street and 8<sup>th</sup> Avenue in New York, New York. During the meeting, which was surveilled by other FBI agents and audio recorded. During this meeting, the following, among other things, took place:

a. ISLAM displayed a Dunkin' Donuts gift card ("Gift Card-1") with a magnetic strip to UC-1, and informed him, in sum and in part, that he had added funds to Gift Card-1 from stolen credit card numbers belonging to other individuals. UC-1 then observed ISLAM make a purchase using Gift Card-1.

b. Following the purchase, ISLAM and UC-1 sat at a table, and the following occurred:

i. ISLAM and UC-1 sat at a table, and ISLAM informed UC-1, in sum and substance, that on or about June 24, 2012, he had filed a police report with the NYPD, stating that his identity had been stolen, and was being used by an individual associated with the online nickname "JoshTheGod." As set forth below in paragraph 25(b), during a post-arrest statement, ISLAM admitted that he used the online nickname "JoshTheGod," which is the online nickname associated with his activities with the "UGNazi" hacker group ("UGNAZI HACKER GROUP"). ISLAM informed UC-1 that he made the police report so that if he was arrested by law enforcement in connection with his online activities as "JoshTheGod," he could claim that he was being framed by another individual who had stolen his identity.

ii. UC-1 provided 15 American Express cards, five of which were embossed with the name "Robert Whitetaker," and ten of which were embossed with other fake names not associated with real individuals. As set forth above in paragraph 16, ISLAM had previously asked UC-1 to emboss American Express cards encoded with stolen information with the name "Robert Whitetaker," for the purposes of executing the AMEX FRAUD SCHEME. In addition, UC-1 provided a piece of paper including a list of PIN numbers associated with nine of the cards that UC-1 provided to ISLAM.

iii. ISLAM inspected the 15 cards that UC-1 provided to him, and informed UC-1, in sum and in part, that they looked good. Further, ISLAM indicated that he could only use the five cards embossed with the name "Robert Whitetaker" to

card, but that he could use the other cards for which PIN numbers were provided to make unauthorized withdrawals from ATM machines. Further, ISLAM indicated that he expected to withdraw approximately \$500 to \$1,500 from each of the cards with PIN numbers, and that he expected to make purchases of at least \$1,000 from each card embossed with the name "Robert Whitetaker." ISLAM indicated that they would continue to card after they traveled to Virginia, and that they would split the proceeds of the scheme equally. ISLAM retained five cards, including four of the five cards embossed with the name "Robert Whitetaker," and one card embossed with a fake name ("Card-1"), and returned the other cards to UC-1.

iv. ISLAM instructed UC-1, in sum and in part, to obtain additional stolen credit card information. Further, he indicated that he was also interested in stolen Visa and MasterCard credit card numbers, so long as UC-1 could also obtain PIN numbers associated with the stolen credit card numbers.

v. UC-1 then asked ISLAM if they should test out one of the cards with an associated PIN number. ISLAM agreed, and UC-1 followed ISLAM to an ATM located in the vicinity of 8<sup>th</sup> Avenue between 38<sup>th</sup> Street and 39<sup>th</sup> Street in New York, New York ("ATM-1"). ISLAM then made two attempts to withdraw cash from ATM-1 using Card-1, which were both denied. ISLAM departed the vicinity of ATM-1, and was arrested.

25. Following the arrest of MIR ISLAM, a/k/a "JoshTheGod," a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," the defendant, ISLAM was advised of his Miranda rights. ISLAM waived his Miranda rights and agreed to speak with other FBI agents. I have spoken with another FBI Agent ("Agent-1") who was present during the interview. According to Agent-1, during that interview, ISLAM stated, in sum and substance, and among other things:

a. ISLAM stated that he used the online nickname "Ijew" on the UC Site. Further, ISLAM admitted that he advertised "doxing" services on the UC Site. Based on my training and experience, I know that "doxing" is a term commonly used by hackers and carders to refer to the public release of personal identification information for individuals, including but not limited to information such as the individual's name, address, phone, number, date of birth, Social Security number, e-mail address in order to embarrass, harass, or retaliate against such individual. Further, ISLAM admitted that he had

released personal financial and identification information on the UC Site regarding at least ten individuals, including their credit card number, along with associated names and addresses.

b. ISLAM mentioned he uses the online nickname "JoshTheGod," in connection with the UGNAZI HACKER GROUP. Further, he admitted that, among other things, he has participated in "doxing" individuals on behalf of the UGNAZI HACKER GROUP.

c. ISLAM stated that he is the operator and an administrator for another carding website, called "fraud.su." which I know, based on my familiarity with this investigation, was formerly called "carders.org" ("Carding Site-2"). I have reviewed Carding Site-2, and have confirmed that Carding Site-2 is a carding forum, similar to the UC Site, which facilitated carding activity, including but not limited to the sale and exchange stolen credit card and other personal identification information.


d. ISLAM admitted that he has made online purchases using stolen credit card information.

e. ISLAM stated that he uses E-Mail Account-1.

f. ISLAM stated that he has purchased fake identification documents.

26. Following the arrest of MIR ISLAM, a/k/a "JoshTheGod," a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," the defendant, I executed a search of the ISLAM's residence in the Bronx, New York ("Residence-1"), pursuant to a search warrant authorized by the Honorable James C. Francis IV, United States Magistrate Judge. During that search, I recovered, from a bedroom, among other things: (a) two laptop computers; (b) various handwritten documents, signed by "Robert Whitetaker," instructing packages to be left for him at Residence-1; (c) handwritten documents containing what appear to be various credit card numbers; and (d) various correspondence addressed to "Mir Islam."

WHEREFORE, I respectfully request that an arrest warrant be issued for MIR ISLAM, a/k/a "JoshTheGod," a/k/a "Ijew," a/k/a "Josh Matthews," a/k/a "Robert Whitetaker," a/k/a "josh@obbahhost.com," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.



DENNIS J. KAMPH  
Special Agent  
Federal Bureau of Investigation

Sworn to before me this  
26<sup>th</sup> day of June 2012

---

JAMES C. FRANCIS IV  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF NEW YORK