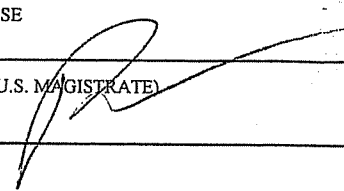
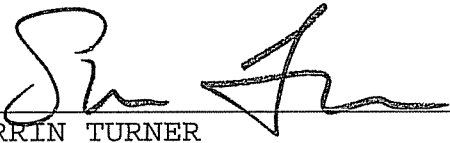


WARRANT FOR ARREST

<p><i>United States District Court</i></p>		<p>DISTRICT</p> <p>SOUTHERN DISTRICT OF NEW YORK</p>	
<p>UNITED STATES OF AMERICA</p> <p>v.</p> <p>STEVEN HANSEN, a/k/a "theboner1"</p>		<p>DOCKET NO. 12 MAG 01641 MAGISTRATE'S CASE NO.</p>	
<p>WARRANT ISSUED ON THE BASIS OF: <input type="checkbox"/> Order of Court</p> <p><input type="checkbox"/> Indictment <input type="checkbox"/> Information <input checked="" type="checkbox"/> Complaint</p>		<p>NAME AND ADDRESS OF INDIVIDUAL TO BE ARRESTED</p> <p style="text-align: center;">STEVEN HANSEN, a/k/a "theboner1" 300 Wilton Circle, Paducah, KY, 42003</p>	
<p>TO: UNITED STATES MARSHAL OR ANY OTHER AUTHORIZED OFFICER</p>		<p>DISTRICT OF ARREST</p>	
<p>YOU ARE HEREBY COMMANDED to arrest the above-named person and bring that person before the United States District Court to answer to the charge(s) listed below.</p>		<p>CITY</p>	
<p>DESCRIPTION OF CHARGES</p>			
<p>Fraud in Connection with Identification Information</p>			
<p>IN VIOLATION OF</p>	<p>UNITED STATES CODE TITLE</p> <p>18</p>	<p>SECTION</p> <p>1028(a)(7)</p>	
<p>BAIL</p>	<p>OTHER CONDITIONS OF RELEASE</p>		
<p>ORDERED BY</p>	<p>SIGNATURE (FEDERAL JUDGE/U.S. MAGISTRATE)</p> 		<p>DATE ORDERED</p>
<p>CLERK OF COURT</p>	<p>(BY) DEPUTY CLERK</p>		<p>DATE ISSUED</p>
<p>RETURN</p>			
<p>This warrant was received and executed with the arrest of the above-named person.</p>			
<p>DATE RECEIVED</p>	<p>NAME AND TITLE OF ARRESTING OFFICER</p>	<p>SIGNATURE OF ARRESTING OFFICER</p>	
<p>DATE EXECUTED</p>			

Note: The arresting officer is directed to serve the attached copy of the charge on the defendant at the time this warrant is executed.

Approved: 
SERRIN TURNER
Assistant United States Attorney

Before: HONORABLE ANDREW J. PECK
United States Magistrate Judge
Southern District of New York

12 MAG 01641

----- x
: UNITED STATES OF AMERICA : SEALED COMPLAINT
: :
: - v. - : Violation of
: : 18 U.S.C. § 1028(a)(7)
: STEVEN HANSEN, :
: a/k/a "theboner1," : COUNTY OF OFFENSE:
: : New York
: Defendant. :
: :
----- x

SOUTHERN DISTRICT OF NEW YORK, ss.:

Miguel A. Castellanos, 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
(Fraud in Connection with Identification Information)

1. From on or about June 22, 2010, up to and including on or about July 11, 2010, in the Southern District of New York and elsewhere, STEVEN HANSEN, a/k/a "theboner1," the defendant, knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person with the intent to commit, and to aid and abet, and in connection with, unlawful activity that constitutes a violation of Federal law, and that constitutes a felony under applicable State and local law, to wit, HANSEN possessed stolen account information for at least 30 credit cards, and distributed the information to others with the intent to help them conduct fraudulent transactions.

(Title 18, United States Code, Section 1028(a)(7).)

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

2. 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.

3. I have been a Special Agent with the FBI for approximately one year. I am currently 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

4. 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").

5. 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.¹ 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

¹ 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.

("IP") addresses of users' computers when they accessed the site.²

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 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.

² 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.

Possession and Distribution of
Stolen Credit Card Information by "theboner1"

6. As set forth below, STEVEN HANSEN, a/k/a "theboner1," the defendant, was a user of the UC Site who possessed stolen account information for at least 30 credit cards, and who distributed the information to other users on the UC Site with the intent to help them effect fraudulent transactions.

7. On or about June 15, 2010, an individual registered on the UC Site with the username "theboner1." The individual provided his e-mail address as "theprophet1985@live.com" for the purpose of receiving registration instructions.

8. On or about June 27, 2010, "theboner1" started a discussion thread, titled "Should have done this when I joined," in which he introduced himself on the UC Site.³

a. In the message, "theboner1" stated that he was a "long time carder," with "around 2.5 years" of experience.

b. "theboner1" stated that he was interested in selling "CVVs" on the site. Based on my training and experience, I know that the term "CVV" is used by carders to refer to a type of debit or credit card data that includes, among other information, the card number, expiration date, and security code, as well as the name and address of the card holder. Such information is typically used by carders to make fraudulent purchases over the Internet or telephone.

9. On or about June 17, 2010, "theboner1" contacted a site administrator of the UC Site through ICQ, a popular instant-messaging, or "chat," service on the Internet. In actuality, the site administrator was a cooperating witness in the investigation ("CW-1").⁴ During the chat, "theboner1" asked

³ Unless otherwise noted, all postings and private messages referred to herein were posted or sent on the UC Site and were retained as part of the operation of the UC Site. Quotations from such messages and any other electronic communications are reproduced substantially as they appear in the original text; errors in spelling and punctuation have not been corrected.

⁴ Based on my involvement in this investigation, I know that CW-1 was arrested by law enforcement and agreed to cooperate with the Government in the hope of receiving a reduced sentence. CW-1 has pleaded guilty to various charges pursuant to a cooperation agreement with the Government and is awaiting sentencing. CW-

CW-1 about how he could become "verified" as a vendor of CVVs on the UC Site. CW-1 told "theboner1" that he would need to send samples of the credit cards he had available for sale.⁵ "theboner1" replied that he would be back in contact with the necessary samples in the coming days.

10. On or about June 22, 2010, "theboner1" started a discussion thread titled in part "Selling CVVs Almost any country." From reviewing the thread, I know the following:

a. In his initial posting, "theboner1" advertised that he was "selling CVVs (credit cards)."

b. "theboner1" quoted a price of \$2.50 per card for Visa cards, \$3.00 for MasterCard and Discover cards, and \$4.00 for American Express cards.

c. "theboner1" added: "If you would like a particular State it is Another [\$].50 and if you want city it is a total of 1 dollar (state+city)." Based on my training and experience, in offering credit cards from "almost any country" and from particular states and cities, I understand "theboner1" to have meant that he could sell stolen credit card data based on the location of the address on the credit card account. With this service, a carder wanting to purchase goods from a particular location, or ship goods to a particular location, could buy a stolen credit card account based in that same location, and thereby avoid fraud alerts that otherwise might be triggered by the use of a credit card to purchase or ship goods outside its normal area of usage.

d. "theboner1" stated that those interested in his CVVs could contact him either via ICQ or via private message on the UC Site.

1's involvement in chats and private messages relating to the UC Site was at the direction of, and monitored by, the FBI.

⁵ The UC Site allowed users wishing to sell goods or services on the site to become "verified vendors" by submitting their goods or services for review by a site administrator (who, in actuality, would be either an undercover agent or a confidential source in the investigation). If the site administrator determined that the goods or services offered by the user were as advertised, the user could represent himself as a "verified vendor" on the UC Site. This process enabled the FBI to obtain evidence of the user's criminal activity and to investigate carding hardware, software, and methods.

e. On or about June 23, 2010, "theboner1" posted a subsequent message to the thread in response to a question from another user concerning whether the CVVs he had for sale could be used for in-store purchases. "theboner1" answered, "Basically Cvv's are used for ONLINE purchases."

f. Later that same day, "theboner1" posted a message to the thread responding to a question from another user concerning whether there were substantial balances on the credit cards for which he was selling CVVs. "theboner1" answered: "Yes that is the point of purchasing a cvv. It is a stolen/fraudulent credit card. Even though I can't guarantee the amount of funds that will be available to use on the card as they all vary."

11. On or about June 24, 2010, "theboner1" exchanged a series of private messages with another UC Site user ("User-1"). From reviewing the exchange, I know the following:

a. User-1 contacted "theboner1" to inquire about purchasing "CC's . . . from London."

b. "theboner1" responded that he had "plenty for sale," and told User-1 to send payment for any cards he wanted to a particular account at Liberty Reserve (the "Subject Liberty Reserve Account"), an on-line payment processor.

c. User-1 responded, "I'll take 3 London Visa ones."

d. User-1 subsequently forwarded a message from Liberty Reserve reflecting a payment of \$14.75 into the Subject Liberty Reserve Account.

e. "theboner1" replied with CVV data for three Visa credit cards, each including a cardholder address in London, England. I have confirmed with representatives of Visa that the three credit card numbers provided correspond to genuine Visa accounts.⁶

12. From on or about June 27, 2010, through on or about July 11, 2011, "theboner1" conducted similar transactions via private message exchanges with three other UC Site users ("User-2," "User-3," and "User-4"). Specifically, "theboner1" sold two Visa CVVs to User-2, one Visa CVV to User-3, and one Visa CVV

⁶ As to all credit card accounts referenced in this Complaint, the FBI has alerted the relevant credit card companies to the compromise of the accounts.

and one American Express CVV to User-4, after each user indicated that they had made payments into the Subject Liberty Reserve Account. I have confirmed with representatives of Visa and American Express that all of the credit card numbers "theboner1" provided to these users correspond to genuine credit card accounts.

13. On or about July 5, 2010, "theboner1" contacted CW-1 via ICQ to inquire again about becoming a "verified vendor" of CVVs. From reviewing their ICQ chat, which was electronically preserved, I know the following:

a. During the chat, "theboner1" asked CW-1: "Are you ready to review me. I got like 20 [CVVs] right now."

b. CW-1 indicated that this sample would be sufficient for a review and asked "theboner1" to send him the CVV data over ICQ.

c. "theboner1" replied by sending CVV data for twelve American Express credit cards and ten Visa credit cards. I have confirmed with representatives of American Express and Visa that all of these credit card numbers correspond to genuine American Express and Visa accounts, respectively.

Identification of "theboner1"

14. As noted above in paragraph 7, when "theboner1" registered with the UC Site, he provided the e-mail address "theprophet1985@live.com" for the purpose of receiving registration instructions. According to records obtained from Microsoft, the provider for the account, the account is subscribed to "Steve Hansen," who listed Illinois as his state of residence and his zip code as 61065.

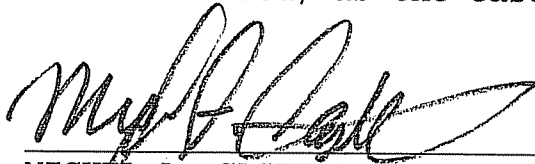
15. I have reviewed records from Media Communications Corporation, an Internet service provider, concerning the IP address used by "theboner1" at the time that he registered with the UC Site on June 15, 2010 (the "Registration IP Address"). According to these records, at the time in question, the Registration IP Address was assigned to a Media Communications customer with the last name "Hansen," with an address in Poplar Grove, Illinois, including the same zip code as listed in the subscriber information for the "theprophet1985@live.com" e-mail address described in the preceding paragraph.

16. I have obtained criminal history records from the State of Illinois concerning a "Steven Hansen" with the same

Poplar Grove, Illinois address as listed on the Media Communications account to which I traced the Registration IP Address. According to these records, on or about July 14, 2010, Steven Hansen pled guilty to identity theft in violation of Chapter 720, Section 250/8 of the Illinois Compiled Statutes. Specifically, the indictment to which Hansen pled guilty charged that he obtained approximately \$592 in goods from a hardware store using a stolen credit card number.⁷

17. Accordingly, I believe that the individual described above as "theboner1" is STEVEN HANSEN, a/k/a "theboner1," the defendant.

WHEREFORE, I respectfully request that an arrest warrant be issued for STEVEN HANSEN, a/k/a "theboner1," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.



MIGUEL A. CASTELLANOS
Special Agent
Federal Bureau of Investigation

Sworn to before me this
19th day of June 2012



UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

⁷ According to investigative documents that I obtained from the local authorities involved in this Illinois prosecution, the credit card number used in this \$592 transaction was not one of the 30 credit card numbers known to have been distributed by "theboner1" on the UC Site, as described above.