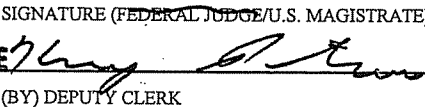


WARRANT FOR ARREST

<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>ERIC BOGLE, a/k/a "Swat Runs Train"</p>		<p>DOCKET NO.</p>	<p>MAGISTRATE'S CASE NO.</p> <p>12 MAG 1602</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>Eric Bogle, 67 Lawrence Crescent, Red Deer, Alberta, Canada</p>	
<p>TO: UNITED STATES MARSHAL OR ANY OTHER AUTHORIZED OFFICER</p>		<p>DISTRICT OF ARREST</p>	
<p>TO: UNITED STATES MARSHAL OR ANY OTHER AUTHORIZED OFFICER</p>		<p>CITY</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>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>HENRY PITMAN UNITED STATES MAGISTRATE JUDGE SOUTHERN DISTRICT OF NEW YORK</p>	<p>SIGNATURE (FEDERAL JUDGE/U.S. MAGISTRATE)</p> 		<p>DATE ORDERED</p> <p>6-15-12</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 12 MAG 1602
SERRIN TURNER
Assistant United States Attorney

Before: HONORABLE HENRY PITMAN
United States Magistrate Judge
Southern District of New York

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

SOUTHERN DISTRICT OF NEW YORK, ss.:

Ilhwan Yum, 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 in or about June 2010, up to and including in or about November 2010, in the Southern District of New York and elsewhere, ERIC BOGLE, a/k/a "Swat Runs Train," 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, BOGLE possessed stolen account information for at least 32 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 over four years. For the past three years, 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

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 "Swat Runs Train"

6. As set forth below, ERIC BOGLE, a/k/a "Swat Runs Train," the defendant, was a user of the UC Site, who possessed stolen account information for at least 32 credit cards and distributed the information to other users on the UC Site, with the intent to help them effect fraudulent transactions.

7. On or about June 16, 2010, an individual registered on the UC Site with the username "Swat Runs Train." The user provided his e-mail address as "grimraper@gmail.com" for the purpose of receiving registration instructions.

8. On or about June 23, 2010, "Swat Runs Train" started a discussion thread titled "Looking for Cash/Carders."³ From reviewing the thread I know the following:

a. In his initial posting to the thread, "Swat Runs Train" stated: "I have tons of CVVs or CVV2s etc. I need people to get the cash off them for me. fees/percentage is negotiable, I also do not care how you get the cash nor how long it takes etc, as long as I see the money adventually. To start you will get one info, when i get the money from that one we shall continue, adventually once we have built some trust you can have a few at a time."

b. Based on my training and experience, I know that the terms "CVV" and "CVV2" are used by carders to refer to types of debit or credit card data that include, among other information, the name, number, expiration date, and security code that appear on the card. Such information is typically used by carders to make fraudulent purchases on the Internet or over the telephone.

c. Thus, in stating that he needed "people to get the cash off [CVVs] for me," I believe that "Swat Runs Train" meant that he was looking for co-conspirators to whom he could supply stolen debit or credit card information, so that they could in turn use the information to obtain cash by making

³ Unless otherwise noted, all discussion threads 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.

fraudulent purchases with the card information and selling the carded goods.

9. Over the following week, "Swat Runs Train" exchanged private messages with several other UC Site users who expressed interest in response to his June 23, 2010 posting. In these exchanges, the other users provided their usernames on MSN Messenger - a popular instant messaging, or "chat," service on the Internet - indicating, based on my training and experience, that they intended to continue their discussions with "Swat Runs Train" off the UC Site.

10. On or about August 25, 2010, "Swat Runs Train" started a discussion thread on the UC Site titled "enjoy these CVV!" In this posting, "Swat Runs Train" provided "CVV" data for 23 unique credit cards, including the customer names, account numbers, expiration dates, and security codes for each card. "Swat Runs Train" prefaced the list of card data by stating: "enjoy these CVV! They're kind of scrambled etc but if you can decipher a few go for it."⁴ Based on my training and experience, in telling other users to "enjoy" the CVVs and to "go for it," "Swat Runs Train" was encouraging users to use the credit card data to effect fraudulent transactions.

11. Based on consultations with the relevant credit card companies, I have confirmed that 22 of the 23 credit card numbers provided by "Swat Runs Train" in his August 25, 2010 posting correspond to genuine credit card accounts.⁵

12. Later on August 25, 2010, "Swat Runs Train" sent a private message to another UC Site user ("User-1"), titled "here :)." In the message, "Swat Runs Train" passed User-1 "CVV" data for seven additional credit cards. Based on consultations with the relevant credit card companies, I have confirmed that these seven credit card numbers correspond to genuine credit card accounts.

13. On or about October 11, 2010, "Swat Runs Train" started a discussion thread titled in part "Used/dead fulls." From reviewing the thread I know the following:

⁴ The account information for each card was provided in the form of long strings of text that had to be parsed in order to be deciphered.

⁵ 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.

a. In his initial posting to the thread, "Swat Runs Train" announced that he had "used/dead fulls" for sale. Based on my training and experience, I know that the term "fulls" is used by carders to refer to full account information for a credit card holder, including such information as the account holder's social security number, date of birth, and mother's maiden name. Further, based on my training and experience, in describing his "fulls" as "used/dead," I believe that "Swat Runs Train" meant that the account information he had available was for expired accounts.

b. "Swat Runs Train" stated that his prices were "[n]egotiable" but that he was willing to sell the accounts for \$2 each, with "discounts for buyers buying in bulk."

c. "Swat Runs Train" provided information from a particular MasterCard account as a sample of the account information he had available. The information included, among other data, the card holder's name, address, social security number, birth date, mother's maiden name, and bank account information. I have spoken directly with the affected card holder and confirmed that the account information is genuine.

d. In a subsequent posting to the thread later that same day, "Swat Runs Train" stated that the "fulls" he was selling were good for "Bill Me Later" and "many other uses." Based on my training and experience, I understand "Swat Runs Train" to have meant that the account data he was selling could be used to open fraudulent accounts at billmelater.com, an online credit service, among other purposes.

e. Later that same day, another UC Site user ("User-2") posted to the thread, adding that the "fulls" that "Swat Runs Train" was selling "contain usefull info." User-2 elaborated, "You can sign up for loads of things with this info, like bank accounts, credit cards, and other shit. This contains all infos that you would need to know on someone, which is really useful." Based on my training and experience, I understand User-2 to have meant that, even though the account information being offered by "Swat Runs Train" was for expired credit card accounts, the information was still valuable, because the account holders' identity information could be used to open fraudulent bank and credit card accounts.

14. On or about October 11, 2010, another UC Site user ("User-3") contacted "Swat Runs Train" by private message, expressing interest in "talk[ing] about the dead fulls." The

two agreed to talk further over ICQ, a popular Internet chat service.

15. On or about November 1, 2010, "Swat Runs Train" sent another UC Site user ("User-4") full account data for a particular American Express credit card account, similar to the sample MasterCard account provided in his October 11, 2010 posting. I have confirmed with American Express that the account information provided in the message corresponds to a genuine, expired American Express account that belonged to the account holder listed. Later that day, User-4 sent a private message to "Swat Runs Train" replying, "Thanks :)."

Identification of "Swat Runs Train"

16. On or about June 16, 2010, the same day that he registered with the UC Site, "Swat Runs Train" sent a private message to a site administrator of the UC Site. In the message, "Swat Runs Train" noted in passing that he "reside[s] in Canada" and that he was "21" years old. "Swat Runs Train" signed the message, "Eric Bogle."

17. On or about November 19, 2010, "Swat Runs Train" exchanged several messages with another UC Site user ("User-5"), concerning funds that User-5 wanted to send to "Swat Runs Train" through MoneyGram, a wire transfer service. In this exchange, "Swat Runs Train" instructed User-5 to send the money to "eric bogle" in Red Deer, Alberta, Canada.

18. In several other private messages with other UC Site users, "Swat Runs Train" provided a particular address in Red Deer, Alberta, Canada where users could ship certain items to him.

19. I have reviewed the IP addresses used by "Swat Runs Train" to access the UC Site, and I have looked up these addresses in a publicly available database used to trace IP addresses to their geographical location of origin. Based on the results of this search, I know that "Swat Runs Train" frequently accessed the UC Site from IP addresses based in Red Deer, Alberta, Canada.

20. As noted in paragraph 7, when "Swat Runs Train" registered with the UC Site, he provided the e-mail address "grimraper@gmail.com" for the purpose of receiving registration instructions. According to records obtained from Google, this e-mail account is subscribed to in the name "Eric Bogle." Further, I have reviewed the contents of this e-mail account

pursuant to a search warrant. The contents include multiple e-mails addressed to "Eric Bogle."

21. I have obtained criminal history records from the Royal Canadian Mounted Police concerning an "Eric Bogle," from which I have learned the following:

a. The records list an address for the subject "Eric Bogle" in Red Deer, Alberta, Canada. The address is the same as the shipping address provided by "Swat Runs Train" in the private messages described above in paragraph 18.

b. The records state that the subject "Eric Bogle" was born in April 1989. As noted above in paragraph 16, in a private message that "Swat Runs Train" sent to a site administrator on or about June 16, 2010, "Swat Runs Train" stated that he was "21" years old.

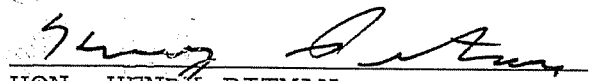
22. Accordingly, I believe that the individual described above as "Swat Runs Train" is ERIC BOGLE, a/k/a "Swat Runs Train," the defendant.

WHEREFORE, I respectfully request that an arrest warrant be issued for ERIC BOGLE, a/k/a "Swat Runs Train," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.



ILHWAN YUM
Special Agent
Federal Bureau of Investigation

Sworn to before me this
15th day of June 2012



HON. HENRY PITMAN
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK