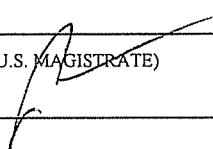


WARRANT FOR ARREST

United States District Court		DISTRICT SOUTHERN DISTRICT OF NEW YORK	
UNITED STATES OF AMERICA v. CHRISTIAN CANGEOPOL, a/k/a "404myth"		DOCKET NO. 12 MAG 01667	MAGISTRATE'S CASE NO. 01667
WARRANT ISSUED ON THE BASIS OF: <input type="checkbox"/> Order of Court <input type="checkbox"/> Indictment <input type="checkbox"/> Information <input checked="" type="checkbox"/> Complaint		NAME AND ADDRESS OF INDIVIDUAL TO BE ARRESTED CHRISTIAN CANGEOPOL, a/k/a "404myth" 2345 Evergreen Lane, Lawrenceville, GA 30043	
TO: UNITED STATES MARSHAL OR ANY OTHER AUTHORIZED OFFICER		DISTRICT OF ARREST	
		CITY	
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.			
DESCRIPTION OF CHARGES			
Access Device Fraud Conspiracy			
IN VIOLATION OF	UNITED STATES CODE TITLE 18	SECTION 1029(b)(2)	
BAIL	OTHER CONDITIONS OF RELEASE		
ORDERED BY ANDREW J. PECK UNITED STATES MAGISTRATE JUDGE SOUTHERN DISTRICT OF NEW YORK	SIGNATURE (FEDERAL JUDGE/U.S. MAGISTRATE) 		DATE ORDERED JUN 21 2012
CLERK OF COURT	(BY) DEPUTY CLERK		DATE ISSUED
RETURN			
This warrant was received and executed with the arrest of the above-named person.			
DATE RECEIVED	NAME AND TITLE OF ARRESTING OFFICER	SIGNATURE OF ARRESTING OFFICER	
DATE EXECUTED			

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 01667

-----	x	:	
		:	
UNITED STATES OF AMERICA		:	<u>SEALED COMPLAINT</u>
		:	
- v. -		:	Violation of
		:	18 U.S.C. § 1029(b) (2)
CHRISTIAN CANGEOPOL,		:	
a/k/a "404myth,"		:	COUNTY OF OFFENSE:
		:	New York
Defendant.		:	
		:	
-----	x	:	

SOUTHERN DISTRICT OF NEW YORK, ss.:

Patrick D. Hoffman, 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
(Access Device Fraud Conspiracy)

1. From in or about November 2011, up to and including in or about April 2012, in the Southern District of New York and elsewhere, CHRISTIAN CANGEOPOL; a/k/a "404myth," the defendant, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit access device fraud in violation of Section 1029(a) (5).

2. It was a part and an object of the conspiracy that CHRISTIAN CANGEOPOL, a/k/a "404myth," the defendant, and others known and unknown, would and did knowingly and with intent to defraud effect transactions, affecting interstate and foreign commerce, with one and more access devices issued to another person and persons, to receive payment and any other things of

value during a one-year period, the aggregate value of which was equal to or greater than \$1,000.

(Title 18, United States Code, Section 1029(b)(2).)

Overt Acts

3. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about November 5, 2011, CHRISTIAN CANGEOPOL, a/k/a "404myth," the defendant, sent a message to a co-conspirator through the Internet on a server maintained in the Southern District of New York, in which he offered to arrange in-store pick-ups from Walmart of electronic devices purchased with stolen credit card information.

b. On or about November 7, 2011, CHRISTIAN CANGEOPOL, a/k/a "404myth," the defendant, picked up an Apple iPad from a Walmart store in Lawrenceville, Georgia, that had been purchased by a co-conspirator using stolen credit card information.

(Title 18, United States Code, Section 1029(b)(2).)

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

4. 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.

5. I have been a Special Agent with the FBI for over 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

6. 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").

7. 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 ("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

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.

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.

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.

Conspiracy to Commit Access Device Fraud by "404myth"

8. As set forth below, CHRISTIAN CANGEOPOL, a/k/a "404myth," the defendant, was a user of the UC Site who retrieved electronic devices from Walmart stores that had been purchased by a co-conspirator using stolen credit card information. CANGEOPOL further agreed to resell the devices to others and split the profits with the co-conspirator.³

9. On or about April 14, 2011, an individual registered on the UC Site with the username "404myth." The individual provided his e-mail address as "404myth@gmail.com" for the purpose of receiving registration instructions.

10. On or about May 27, 2011, "404myth" posted to a discussion thread concerning Apple laptops.⁴ In the posting, "404myth" commented that he had recently "instored" four Apple Macbook Pro laptop computers, adding, "I . . . love the re-sell

³ The FBI has taken steps to alert Walmart and the relevant credit card companies concerning these fraudulent transactions.

⁴ 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.

value on these babies." Based on my training and experience, I know that "instore" is a term used by carders to refer to using stolen credit card accounts to make in-store, as opposed to online, purchases of items.

11. On or about November 5, 2011, another UC Site user ("CC-1") sent "404myth" a private message, soliciting "404myth" to do "instore pickup" transactions at Walmart. CC-1 explained: "I can order iPads, iPods etc and you send a guy who picks them up with a fake id." Based on my training and experience, I understand CC-1's proposal to have been as follows: (a) he would use stolen credit card data to order electronic devices on Walmart's website; (b) in selecting a delivery option, CC-1 would opt to have the item delivered to a Walmart store for customer pick-up and would identify an individual authorized to retrieve the item; (c) "404myth" would then take care of picking up the item from the designated store location, using a fake identification containing the name of the individual authorized to do the pick-up; and (d) CC-1 and "404myth" would then re-sell the carded devices and split the proceeds.

12. Later that day, "404myth" replied to CC-1 by private message to tell him that he was interested in CC-1's proposal. "404myth" stated: "I have people who can pick up everyday if you can order iPads. I also have buyers for them. So if you want to work a % deal and we can make some money from pick-ups, there is about 10 different locations in my area alone." Based on my training and experience, in stating that there were about "10 different locations in my area alone," I understand "404myth" to have meant that there were about 10 different stores in his area where he could pick up items ordered by CC-1, so that he would not have to do all the transactions at one store, which would pose a greater risk of getting caught.

13. Later that day, CC-1 responded, "if I can get good CCs [credit cards] its np [no problem]. If we can work out some deal like 1 stuff shipped to me it would be nice. I can get iPads tomorrow or new ipods, Xboxes, ps3s." Based on my training and experience, I believe that, in proposing "some deal like 1 stuff shipped to me," CC-1 was proposing that "404myth" could send him one of whatever items he would be picking up, as compensation for carding the items.

14. Later that day, "404myth" responded, "I have a buyer for any small electronics, so no have to ship to you every single time. I can ship a few times if you want for personal use and then i can send % through WU or LR. Get on MSn so we can talk details." Based on my training and experience, I

believe that "404myth" was proposing that, instead of compensating CC-1 in kind, he could resell the carded items to other buyers and send CC-1 a percentage of the profits through Western Union or Liberty Reserve (an electronic form of currency). Further, based on my training and experience, in telling CC-1 to "get on MSn," "404myth" was inviting CC-1 to talk further over MSN Messenger, a popular instant-messaging, or "chat," service on the Internet.

15. Pursuant to a search warrant, I have obtained and reviewed the contents of the "404myth@gmail.com" e-mail account used by "404myth" to register with the UC Site. The account includes an e-mail sent on November 7, 2011, at 3:42 p.m., from Walmart.com to "404myth@gmail.com," as well as another e-mail address. The e-mail concerned an order placed under a particular customer name ("Customer-1") for an Apple iPad2; it stated that the item is "now ready for pickup" at a Walmart location in Lawrenceville, Georgia. In addition to Customer-1, the e-mail listed "Johnathan Wincor" as a person authorized to pick up the item.

16. Approximately one hour later, at 4:56 p.m. on or about November 7, 2011, CC-1 sent "404myth" a private message on the UC Site, stating "its ready... pick it up fast!!!!!!" Based on my training and experience, I believe that CC-1 was the second addressee on the e-mail described in the previous paragraph, and that, in this private message, CC-1 was alerting "404myth" that an iPad CC-1 had carded was ready for pick-up.

17. Based on documents subpoenaed from Walmart, I have confirmed that, on November 7, 2011, someone using a Visa credit card issued in the name of Customer-1 ordered an Apple iPad for \$528.94 through the Walmart.com website, for pick-up at a Walmart store in Lawrenceville, Georgia. The documents further indicate that the item was in fact picked up.

18. Also included in the "404myth@gmail.com" account is an e-mail dated November 9, 2011, 12:47 p.m., sent from another e-mail address, forwarding an e-mail from Walmart.com. The forwarded e-mail concerned an order placed under a second customer name ("Customer-2") for another Apple iPad2; it stated that the item is "now ready for pickup" at a Walmart location in Lawrenceville, Georgia. In addition to Customer-2, the e-mail listed "Johnathan Wincor" as a person authorized to pick up the item.

19. Based on documents subpoenaed from Walmart, I have confirmed that, on November 9, 2011, someone using a Visa credit

card issued in the name of Customer-2 ordered an Apple iPad for \$528.94 through the Walmart.com website, for pick-up at a Walmart store in Lawrenceville, Georgia. The documents further indicate that the item was in fact picked up.

20. According to additional documents obtained from Walmart:

a. During the period from November 1 to November 15, 2011, five other orders for Apple devices were placed through Walmart's website, requesting pick-up of the items at various store locations in the area of Lawrenceville, Georgia, and listing "Johnathan Wincor" as a person authorized for the pick-up.

b. The orders were placed using five different credit cards, each held in a different name.

21. From in or about November 2011 through in or about March 2012, CC-1 sent "404myth" numerous other private messages concerning goods that CC-1 asked "404myth" to retrieve for him through various means, including Apple Macbook Pro laptop computers, Apple iPads, and computer hard drives.

Identification of "404myth" and
Further Confirmation of His Carding Activity

22. I have reviewed the IP addresses used by "404myth" to access the UC Site. Using publicly available search tools, I have traced many of these IP addresses to AT&T Internet Services, an Internet service provider.

23. I have reviewed records subpoenaed from AT&T Internet Services concerning a sample of the IP addresses used by "404myth" that trace back to AT&T Internet Services (the "Sample IP Addresses"). According to these records, at the times when the Sample IP Addresses were used by "404myth" to access the UC Site, the IP addresses were assigned to a female subscriber of AT&T Internet Services with the last name "Cangeopol," at a particular address on Evergreen Lane in Lawrenceville, Georgia (the "Evergreen Lane Address"). Based on a search of law enforcement and publicly available databases, I have learned that this subscriber is a relative, believed to be the mother, of an individual named "Christian Cangeopol," who also resides at the Evergreen Lane Address.

24. I have reviewed a police report filed by an officer of the Milton, Georgia Police Department on or about April 11,

2012, concerning an arrest of a "Christian Cangeopol," who is listed in the report as residing at the Evergreen Lane Address. In the report, Officer-1 states:

a. On or about April 11, 2012, Officer-1 was dispatched to a Fry's Electronics store in the Milton, Georgia area, in response to a reported fraud at the store.

b. Upon arriving at the store, Officer-1 spoke to a loss prevention associate ("LPA") at the store. The LPA reported that he had detained a customer who had attempted to purchase an Apple Macbook laptop computer with a credit card the LPA suspected to be counterfeit.

c. According to the LPA, when the customer gave the cashier his credit card to pay for the laptop, the transaction was approved, but the store's credit card terminal displayed a card number different from the number actually printed on the card.

d. The LPA provided the credit card receipt that had been printed during the transaction, which the customer had signed in the name "Claude Turok."

e. After speaking with the LPA, Officer-1 spoke to the detained customer. The customer identified himself to Officer-1 as "Claude Turok."

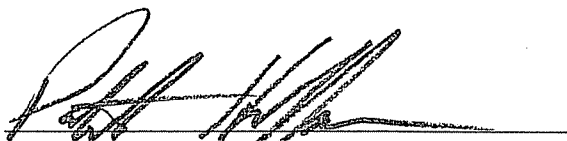
f. Officer-1 ran this name through a law enforcement database without obtaining a match. Officer-1 then informed the customer that, if the customer failed to truthfully identify himself he could be charged with providing a false identity. The customer then identified himself as "Christian Cangeopol."

g. Upon further questioning, Cangeopol admitted that he had encoded the card used in the transaction with stolen credit card information.

h. Officer-1 placed Cangeopol under arrest for credit card fraud.

25. On or about April 24, 2012, "404myth" posted a public message on the UC Site, stating: "If anyone was wondering where I've roamed off to in the past month or so, it's a long story but instoring is not as safe of an art anymore as it was in the past, unfortunate for me to say, but I think my time in physical/IRL ["in real life"] fraud is coming to an end, I will have to find better methods for online/virtual fraud."

WHEREFORE, I respectfully request that an arrest warrant be issued for CHRISTIAN CANGEOPOL, a/k/a "404myth," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.



PATRICK D. HOFFMAN
Special Agent
Federal Bureau of Investigation

Sworn to before me this
21st day of June 2012



UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK