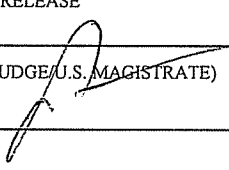


WARRANT FOR ARREST

12 MAG 01640

<p><i>United States District Court</i></p>		DISTRICT SOUTHERN DISTRICT OF NEW YORK	
UNITED STATES OF AMERICA v. MARK CAPARELLI, a/k/a "Cubby"		DOCKET NO. 12 MAG 01640	MAGISTRATE'S CASE NO. 01640
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 MARK CAPARELLI, a/k/a "Cubby," 6857 Fisk Ave, San Diego, CA	
		DISTRICT OF ARREST	
TO: UNITED STATES MARSHAL OR ANY OTHER AUTHORIZED OFFICER		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			
Wire Fraud, Access Device Fraud			
IN VIOLATION OF	UNITED STATES CODE TITLE 18	SECTION 1343 & 1029(a)(2)	
BAIL	OTHER CONDITIONS OF RELEASE		
ORDERED BY	SIGNATURE (FEDERAL JUDGE/U.S. MAGISTRATE) 		DATE ORDERED
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
SERRIN TURNER
Assistant United States Attorney

12 MAG 01040

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

-----	x	:	
UNITED STATES OF AMERICA	:	:	<u>SEALED COMPLAINT</u>
	:	:	
- v. -	:	:	Violations of
	:	:	18 U.S.C. §§ 1343 &
MARK CAPARELLI,	:	:	1029(a) (2)
a/k/a "Cubby,"	:	:	
	:	:	COUNTY OF OFFENSE:
Defendant.	:	:	New York
-----	x	:	

SOUTHERN DISTRICT OF NEW YORK, ss.:

John Leo, Jr., 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
(Wire Fraud)

1. From on or about December 15, 2010, up to and including on or about May 17, 2011, in the Southern District of New York and elsewhere, MARK CAPARELLI, a/k/a "Cubby," the defendant, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, knowingly transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, to wit, as part of a scheme to defraud Apple, Inc., CAPARELLI posted messages on a website in which he offered to fraudulently obtain Apple iPhones in return for compensation.

(Title 18, United States Code, Section 1343.)

COUNT TWO
(Access Device Fraud)

2. From on or about December 15, 2010, up to and including on or about May 17, 2011, in the Southern District of New York and elsewhere, MARK CAPARELLI, a/k/a "Cubby," the defendant, knowingly and with intent to defraud trafficked in and used one and more unauthorized access devices during a one-year period, in and affecting commerce, and by such conduct obtained things of value aggregating \$1,000 and more during that period, to wit, CAPARELLI used stolen credit card numbers to obtain Apple iPhones.

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

The bases for my knowledge and for the foregoing charges 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 6 years. For the past 5 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

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.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 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,

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.

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 Fraudulent "Apple Call-In" Scheme

7. Based on my training and experience, and my review of publicly available information from Apple, Inc., I know that, during the time period relevant to this Complaint, Apple provided customers an "Express Replacement Service" option for the replacement of certain defective products, including defective iPhones. Under the terms and conditions of this service:

a. The customer could call Apple to report a defect in an Apple product eligible for the Express Replacement Service and request a replacement for the product.

b. In the event that Apple determined that the reported defect warranted a replacement, Apple would ship a replacement product to the customer immediately upon the customer's request. The customer was not required to return the defective product to Apple in advance of the replacement product being shipped out.

c. The customer was instead required to return the defective product upon receiving the replacement product, using packaging provided with the replacement product.

d. As security for this service, Apple required the customer to provide a valid credit card number before any replacement product could be shipped. In the event that the customer failed to return the defective product to Apple after receiving the replacement product, Apple would charge the credit card number for the value of the replacement product.

8. Based on my training and experience, I know that, during the time period relevant to this Complaint, a fraudulent scheme commonly referred to as "Apple call-ins" was discussed in carding circles on the Internet. In its basic outline, the scheme worked as follows:

a. A carder would obtain a serial number for an Apple product.

b. The carder would call Apple claiming that the product with this serial number was defective, and would request an immediate replacement for the product pursuant to Apple's Express Replacement Service.

c. Upon being asked for a credit card number as security for the return of the purportedly defective product, the carder would provide a stolen credit card number.

d. Apple would ship out the replacement product as requested.

e. No defective product would be returned to Apple. Any resulting charge for the replacement product would be placed on the stolen credit card supplied by the carder. Since the replacement product would already have been received by the carder at this point, the carder would bear no risk of the credit card charge not going through.³

Fraudulent "Apple Call-In" Service Provided by "Cubby"

9. As set forth below, MARK CAPARELLI, a/k/a "Cubby," the defendant, was a user of the UC Site who obtained Apple iPhones for other users in exchange for compensation, by conducting fraudulent "call-ins" to Apple as described above.

10. On or about September 2, 2010, an individual registered on the UC Site with the username "Cubby." "Cubby" provided the e-mail address "Markeec00@yahoo.com" for the purpose of receiving registration instructions.

11. On the day that he registered with the UC Site, "Cubby" posted a message in which he introduced himself to other UC Site users.⁴ "Cubby" stated, "Hey guys, it's Cubby. Some of you might know me from [an online computer-hacking forum], I post there a lot." "Cubby" further stated that he wanted "to card" and to "make money" from it.

³ The FBI has alerted Apple to the existence of this scheme.

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.

12. Later that day, "Cubby" received a private message from another UC Site user, asking "Cubby" whether he had an account at MSN Messenger, a popular instant-messaging, or "chat," service on the Internet. "Cubby" responded, "I don't go on MSN anymore, since there's a crap load of people wanting me to SE for them." Based on my training and experience, I know that the abbreviation "SE" is commonly used by carders to refer to the practice of obtaining goods or services through "social engineering" - that is, through manipulating or deceiving people, such as customer service representatives, in phone conversations or other one-on-one communications. Thus, I believe that, in stating that he had many people "wanting me to SE for them," "Cubby" meant that he was already known in hacking or carding circles as someone who was effective at obtaining goods and services through social engineering.

13. On or about December 15, 2010, at approximately 1:10 a.m.,⁵ "Cubby" started a discussion thread on the UC Site entitled "Cubby's iPhone Service" (hereafter, the "Call-In Thread"). From reviewing the Call-In Thread, I know the following:

a. In his opening post, "Cubby" advertised that he was "selling Apple iPhone call-ins."

b. "Cubby" further stated in his opening post that he had "iPhone 4 32 gB" devices "[i]n [s]tock" and was selling them for "\$250." "Cubby" clarified in a subsequent post that by "in stock" he did not mean that he had actual iPhone 4 devices in stock; rather, he meant that he had "serials [i.e., serial numbers] for that device in stock."

c. "Cubby's" post further instructed interested users that they would be responsible for providing an address (or "drop") where their desired iPhone would be shipped, stating: "Once I have completed your call and send tracking, it is all on you to make it to your drop and sign for your phone." "Cubby" explained that he did not have "drops" of his own where the iPhones he was ordering could be sent. If he did, "Cubby" elaborated, he would use them to obtain iPhones for himself so that he could sell them "on Craigslist" for "\$500+," as opposed to the lower price he was charging for his call-in service.

d. "Cubby" further explained that users interested in buying a "call-in" from him would be required to pay for the

⁵ All times referenced herein are in Eastern Standard Time.

service up front, and that anyone who was unwilling to do so should use the UC Site's escrow service.⁶

e. Finally, "Cubby" explained that users who were interested in his service could contact him via private message or ICQ - a popular Internet chat service. "Cubby" provided the ICQ number at which he could be reached.

14. Later on or about December 15, 2010, at approximately 1:26 p.m., another UC Site user ("User-1") posted a message on the Call-In Thread. In his message, User-1 stated, "i want to order an iphone through escrow asap."

15. At approximately 1:33 p.m. on or about December 15, 2010, "Cubby" posted a response to User-1's message, advising User-1 to contact a site administrator of the UC Site to set up the escrow transaction.

16. At approximately 1:56 p.m. on or about December 15, 2010, User-1 contacted me via ICQ, in my undercover capacity as a site administrator of the UC Site. User-1 sought to arrange an escrow payment of \$75, plus escrow fees, for an "iphone call in from cubby." I instructed User-1 to make the payment into an undercover account at Liberty Reserve, an Internet-based payment processing system, used for the UC Site's escrow service (the "UC Escrow Account"). I subsequently verified that the funds were deposited into the UC Escrow Account.

17. At approximately 2:05 p.m. on or about December 15, 2010, User-1 posted a message to the Call-In Thread, telling "Cubby" that he had "just sent money to escrow for iphone 4 16 gb" and that "Cubby" could verify the transaction with me.

18. At approximately 2:13 p.m. on or about December 15, 2010, "Cubby" sent a private message to me, again, in my undercover capacity as a site administrator. In the message:

a. "Cubby" told me that he was "selling Apple call-ins" and wanted to "becom[e] an authenticated seller." "Cubby" added, "Let me know what needs to be done."⁷

⁶ As is common with carding forums, the UC Site offered an escrow service for users who wished to purchase goods or services from each other. Specifically, the escrow service permitted buyers to post their payment to an escrow account, rather than pay the seller directly in advance of delivery of the goods or services being purchased. Once delivery was completed, the payment would be released from the escrow account to the seller.

b. "Cubby" also asked me about the escrow transaction initiated by User-1, stating: "I have been told that [User-1] has just used you for escrow, he was going to be purchasing an Apple iPhone 4 16GB. If you could confirm that he has indeed sent you \$75 for the service and the fees for escrow I could go ahead and do the call, thanks."

19. At approximately 2:36 p.m. on or about December 15, 2010, I replied to "Cubby" via private message. In my message:

a. I told "Cubby" that authentication of his services would require him to do a "test" call-in for an iPhone and to have the item shipped to an address that I would specify. "Once the item is received," I explained, "we can then authenticate you."

b. I also told "Cubby" in this message that I had received the escrow payment for his transaction with User-1.

20. At approximately 2:41 p.m. on or about December 15, 2010, "Cubby" replied to me via private message. In his message:

a. "Cubby" asked for the shipping address where I wanted the iPhone to be shipped for the "test" call-in.

b. "Cubby" also stated that he would "get [User-1's] call done" soon and would be back in touch with tracking information to confirm that User-1's iPhone had been shipped out, so that I could release User-1's escrow payment to "Cubby."

21. At approximately 3:01 p.m. on or about December 15, 2010, I replied to "Cubby" via private message with the shipping address where the iPhone for the "test" call-in could be sent, which was located in New York, New York (the "UC Shipping Address").

⁷ The UC Site allowed users wishing to sell goods or services on the site to become "authenticated sellers" 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 an "authenticated seller" of the goods or services on the UC Site. Among other things, this process enabled the FBI to obtain evidence of the user's criminal activity and to analyze carding hardware, software, and methods submitted for authentication.

22. At approximately 5:12 p.m. on or about December 15, 2010, "Cubby" sent me a private message, stating, "I had time to do your call," and informing me that an iPhone was being sent out to the UC Shipping Address. "Cubby" included in his message a link to an e-mail from Apple's technical support department, which included a "Repair ID" number for the transaction.

23. On or about December 21, 2010, I received a private message from "Cubby" offering proof that he had completed a call-in for User-1. Specifically, "Cubby" forwarded a private message from User-1 containing the address where User-1 wanted his iPhone to be shipped ("User-1's Shipping Address"), along with an e-mail from Apple stating that a "replacement IPHONE 4" had been shipped to User-1's Shipping Address. The forwarded e-mail from Apple included a Federal Express tracking number for the shipment, as well as the serial numbers of the "replacement" iPhone being shipped and the original iPhone it was a replacement for (the "Replacement Serial Number" and "Original Serial Number," respectively).

24. I replied to "Cubby" via private message later that day, telling him that, once I received confirmation from User-1 that his iPhone had arrived, I would release User-1's escrow payment.

25. I have reviewed records from Federal Express concerning the tracking number included in the e-mail from Apple forwarded to me by "Cubby" concerning User-1's iPhone, as described in paragraph 23. The records reflect that a package corresponding to the tracking number was sent by Apple Customer Service and delivered to User-1's Shipping Address on December 21, 2010.

26. I have also reviewed records from Apple concerning the Original Serial Number and Replacement Serial Number referenced in the e-mail described in paragraph 23. The records show the following:

a. On or about December 16, 2010, a customer identifying himself as "Peter Kluge" called to report a problem with dead pixels on his iPhone (bearing the Original Serial Number).

b. On or about December 20, 2010, the customer called to report that the problem was still not resolved.

c. On or about December 20, 2010, at the customer's request, Apple shipped an "advance replacement" for the iPhone,

bearing the Replacement Serial Number, to User-1's Shipping Address.

27. On or about December 21, 2010, User-1 posted a message to the Call-In Thread, stating: "well i got my iphone from cubby today, kept me updated on everything. . . . thanks cubby pleasure doing business with you, i might get an ipad off you soon." The message also included a link to an image file stored on an image-sharing website. I have clicked on the link and reviewed the image file. The file is a photograph of what appears to be a new iPhone, next to a scrap of paper with User-1's UC Site username written on it.

28. On or about December 22, 2010, a Federal Express package was delivered to the UC Shipping Address from Apple. I subsequently examined the package, which contained a new iPhone 4. The package also contained documentation indicating that the iPhone had been shipped as a replacement for a defective product, along with packaging to be used in shipping the defective product back to Apple. A packing slip on the outside of the package contained a shipper reference number matching the "Repair ID" included in the Apple e-mail forwarded to me by "Cubby" concerning the "test" iPhone, as described above in paragraph 22.

29. I have reviewed records from Apple concerning the iPhone sent to the UC Shipping Address. The records show that the phone was shipped at the request of a customer identifying himself as "John Lelnard," as a replacement for another iPhone.

30. On or about December 26, 2010, User-1 posted a message to the Call-In Thread, telling Cubby that he "might need more phones." "Cubby" posted a reply later that day, stating, "Sweet, look forward to another deal with you."

31. On or about January 2, 2011, User-1 posted a message to the Call-In Thread indicating that he wanted to talk with Cubby via ICQ, an instant-messaging service on the Internet.

32. On or about January 3, 2011, User-1 transferred \$100 to the UC Escrow Account.

33. Later that day, a cooperating witness acting as a site administrator of the UC Site ("CW-1") contacted "Cubby" via ICQ.⁸

⁸ 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

From reviewing the ICQ chat, which was electronically preserved, I know the following:

a. During the chat, CW-1 informed "Cubby" that User-1 had "paid into the escrow account" for an "iphone deal."

b. CW-1 also asked "Cubby" how his call-in service was going. In responding, "Cubby" stated that call-ins "are easy money," adding that a person can "make 500+ cash each time" from re-selling an iPhone obtained from a call-in.

c. "Cubby" also noted during the chat that he had "raided an apple store a month or so back" and had "like 30 serials [i.e., serial numbers]" for iPhone devices. Based on my training and experience, I believe that, by this remark, "Cubby" meant that he had physically visited an Apple store and obtained serial numbers from devices on display in the store, for use in call-in transactions. CW-1 asked "Cubby," "[S]o after the 30 serials, no more call ins?" "Cubby" responded, "no Ill get more."

34. On or about January 10, 2011, "Cubby" posted a message to the Call-In Thread announcing that he was starting an "iPhone raffle" for "10\$ a ticket." The post instructed those who were interested to "[p]lick a number from 1 to 10" and provide it to "Cubby" when they sent him payment for a ticket.

35. On or about January 11, 2011, "Cubby" posted a message to the Call-In Thread stating, "Winner has been picked for first raffle!" The message contained a link to a YouTube video, posted by the YouTube user "CPCubby." I have reviewed the video, which shows actions on a computer screen while the user of the computer visits a website used to generate random numbers. The website is shown generating the number 6. After providing the link to the video, "Cubby's" message stated, "[C]ongratulations to #6!"

36. Later that day, another UC Site user ("User-2") sent "Cubby" a private message, stating, "Here's the drop." The message contained a shipping address in Florida.

37. Several days later, User-2 posted a message on "Cubby's" thread, stating: "Got my phone today the one i won in

has pleaded guilty to various charges pursuant to a cooperation agreement with the Government and is awaiting sentencing. CW-1's involvement in chats and private messages relating to the UC Site was at the direction of, and monitored by, the FBI.

the raffle, well my drop got it. You are seriously legit, I try doing US [United States] call ins and I always fucking fail, you are too GOOD!"

38. On or about January 12, 2011, a UC Site user started a discussion thread asking for advice on a "method" for obtaining a type of video-game headset from the manufacturer of the product. On or about January 13, 2011, "Cubby" posted a reply to the thread, stating, "All it is [sic] social engineering, there is no method. Have you tried contacting them or anything? If you know the basic functionality of the headphones/mixamp, I'm sure if you think of some defect or whatever, be creative, they would be willing to help out with a replacement. That's just a guess, as I do not know, but experiment with it, don't be lazy." Based on my training and experience, I believe that, in providing this advice, "Cubby" was drawing on his own experience reporting false defects to Apple as part of his "call-in" service.

39. "Cubby" continued offering his "Apple call-in" service on the UC Site until on or about May 17, 2011, when he posted a message on the Call-In Thread stating, "This service is on hold until further notice." "Cubby's" last login to the UC Site was on May 25, 2011.

Use of Stolen Credit Card Data as Part of "Cubby's" Apple Call-In Service

40. Various postings and private messages from "Cubby" reflect that he used stolen credit card data in connection with his call-in transactions with Apple. For example:

a. On or about January 16, 2011, another UC Site user ("User-3") sent "Cubby" a private message stating that he was having trouble doing Apple "call-ins" himself. He asked "Cubby" whether there were any particular types of credit cards that he would suggest using for the transactions. "Cubby" replied, "try amex platinums" and "amex centurion." User-3 asked "Cubby," "is there anyone u recommend getting them from." "Cubby" identified another UC Site user ("User-4"), who he said "has been good so far, and [has] best prices around. Tell him I sent you."

b. On or about January 23, 2011, "Cubby" sent a private message to User-4. The message contained a record of a transfer of funds made through Liberty Reserve earlier that day. The message further stated: "Just sent you some money for a card. . . . I need a Amex, . . . from San Diego, CA. 99122

would be the best zip. Need it for tomorrow, so if you could send it anytime today/tonight that would be great."

c. On or about February 17, 2011, "Cubby" sent another private message to User-4, stating, "I need cards asap Need them for callins tomorrow, thanks." "Cubby" instructed User-4 to get in contact with him via a chat service.

41. Based on my training and experience, and my familiarity with the "Apple call-in" scheme described above in paragraphs 7 and 8, I believe that "Cubby" was using stolen credit cards in his call-in transactions with Apple for the purpose of meeting the security requirement entailed in Apple's Express Replacement Service policy, so as to induce Apple to ship out replacement iPhones without first requiring the receipt of the defective iPhones he was reporting in his calls.

Identification of "Cubby"

42. As noted above, when "Cubby" registered with the UC Site, he provided his e-mail address as "Markeec00@yahoo.com."

43. Based on a search of the Facebook website, I discovered a Facebook user with the username "Markeec00@yahoo.com." The contents of this user's Facebook page are accessible in part to public view. On his Facebook page, the user lists his name as "Mark Caparelli" and his place of employment as "GameStop."

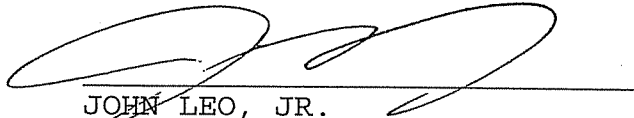
44. On or about January 27, 2011, "Cubby" posted a message to the Call-In Thread in which he mentioned that he "[w]ork[s] at gamestop."

45. Based on a search of law enforcement databases, I have identified a "Mark Caparelli" with a particular address on Fisk Avenue in San Diego, California (the "Fisk Avenue Address").

46. On or about February 21, 2011, another UC Site user ("User-5") with whom "Cubby" had transacted business on the UC Site sent "Cubby" a private message, titled, "address." In the message, User-5 stated, "You want your money or what, message me your fucking address." Later that day, "Cubby" replied via private message, sending User-5 the Fisk Avenue Address as his address.

47. Accordingly, I believe that the individual described above as "Cubby," is MARK CAPARELLI, a/k/a "Cubby," the defendant.

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



JOHN LEO, JR.
Special Agent
Federal Bureau of Investigation

Sworn to before me this
19th day of June 2018



UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK