UNITED STATES DISTRICT COURT

for the

District of Delaware

UNITED STATES OF AMERICA :

v. :

AUSTIN ALCALA, :
a/k/a "AAmonkey," :
a/k/a "AAmonkey1," :

Defendant. :

CRIMINAL NO. 13- 206M

REDACTED

FILED
CLERK U.S. DISTRICT COURT
DISTRICT OF DELAWARE
2013 NOV 14 PM 1:45

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true and correct to the best of my knowledge and belief.

From, on or about January 2011 to on or about October 2013, in the county of New Castle in the District of Delaware and elsewhere, the defendant violated 18 U.S.C. §§ 371, 1028(a)(7) and 1030(a)2)(C), (a)(6), and (c)(2)(B)(i) and (iii), offenses described as follows:

Conspiracy; Identity Theft; and Unlawful Access to a Protected Computer Network

This complaint is based on these facts:

SEE ATTACHED AFFIDAVIT

Continued on the attached sheet: YES

[redacted]

Sworn to before me and subscribed in my presence.

Date: November 14, 2013

Judge's signature

City and state: Wilmington, Delaware

Hon. Mary Pat Thynge, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

UNITED STATES OF AMERICA	:	
	:	
v.	:	
	:	**CRIMINAL NO. 13-** 206M
AUSTIN ALCALA,	:	
a/k/a "AAmonkey,"	:	
a/k/a "AAmonkey1,"	:	
	:	
Defendant.	:	

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, [redacted] ("Your affiant"), a Special Agent with the Federal Bureau of Investigation (FBI), Baltimore Division, Wilmington, Delaware, being duly sworn, depose and state as follows:

1. I have been a Special Agent with the FBI since [redacted] As part of my duties, I investigate violations of federal law, including cyber cases such as computer intrusions, copyright infringement, identity theft, internet fraud, and the online exploitation of children. I have gained expertise in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. This Affidavit is submitted in support of a criminal complaint charging AUSTIN ALCALA, age 18, of McCordsville, Indiana, with violating Title 18, United States Code, Section 1028(a)(7) (Identity Theft) and Section 1030(a)(2)(C), (a)(6), and (c)(2)(B)(i) and (iii) (Unlawful Access to a Protected Computer Network), and Section 371 (Conspiracy).

4. For the reasons set forth below, I respectfully submit that this Affidavit contains ample probable cause to believe that AUSTIN ALCALA trafficked in, possessed and utilized stolen means of indentification, including authentic computer network login credentials relating to other persons to engage in unauthorized access to protected computer networks for the purposes of commercial gain.

5. The information contained in this affidavit is either personally known to your affiant or has been relayed to your affiant by other law enforcement agents. Since this affidavit is being submitted for the limited purpose of securing a complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that AUSTIN ALCALA has committed the crimes of Conspiracy, Identity Theft, and Unauthorized Access to a Protected Computer Network, in violation of Title 18, United States Code, Sections 371, 1028 and 1030.

APPLICABLE STATUTES

6. Title 18, U.S.C., Section 1028 states, in part:

(a) Whoever, in a circumstance described in subsection (c) of this section—

* * * * *

(7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, on in connection with, any unlawful activity that constitutes a violation of Federal law .

. . .

Shall be punished as provided in subsection (b) of this section.

* * * * *

(c) The circumstance referred to in subsection (a) of this section is that—

* * * * *

(3) either—

(A) the production, transfer, possession, or use prohibited by this section is in or affects interstate or foreign commerce, including the transfer of a document by electronic means . . . .

7. Title 18, U.S.C., Section 1030 states, in part:

(a) Whoever—

* * * * *

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

* * * * *

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

8. Title 18, United States Code, Section 371, entitled "Conspiracy to commit offense or to defraud United States," provides, in pertinent part:

If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.

If, however, the offense, the commission of which is the object of the conspiracy, is a misdemeanor only, the punishment for such conspiracy shall not exceed the maximum punishment provided for such misdemeanor.

Background

9. Microsoft Corporation ("Microsoft") is a provider of computer software, hardware, video games, game engine technology, online gaming platforms, and related products and services. Microsoft is headquartered in Redmond, Washington. Microsoft is the developer, manufacturer and intellectual property rights holder of the Xbox gaming console (hereinafter "Xbox"). The latest version of the Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One," is scheduled to be released for sale to consumers on or about November 22, 2013. Xbox One is a computer system and multimedia entertainment and telecommunications hub that allows users not only to play computer games, but also to watch television and movies and to access the Internet. Microsoft has spent millions of dollars developing the Xbox gaming consoles, including Xbox One. Microsoft's Xbox-related revenues for 2011 and 2012 exceeded $8 billion per year.

10. Microsoft operates a "Game Development Network Portal" ("GDNP"), which is a private computer network allowing prospective developers of games for Microsoft's Xbox and other gaming platforms to access, through an authentication system, the pre-release Xbox "Durango" operating system development tools and software. Microsoft controls access to the GDNP by, among other methods, imposing licensing requirements, non-disclosure agreements and other restrictions and requiring authorized users to be registered with Microsoft. Microsoft also administers separate access enclaves for more-restricted data on GDNP.

11. Zombie Studios ("Zombie") is a developer of computer games and helicopter simulation applications and is headquartered in Seattle, Washington. Among Zombie's

simulation customers are electronic gaming companies and the United States Department of the Army.

12. Between January 2011 and present, Microsoft and Zombie have been the target of repeated instances of unauthorized access to their computer networks by a group of hackers that includes Defendant Austin ALCALA, of McCordsville, Indiana; Nathan LEROUX, of Bowie, Maryland; Sanadodeh NESHIEWAT, of Washington, New Jersey; David POKORA, of Ontario, Canada; and [redacted] of Perth, Western Australia. They will be collectively referred to herein as the "XU Group."

Overview of the Hacking Methods

13. Members of the XU Group leased, controlled, and used Internet-connected computers in New Jersey, California, Canada, Utah, Texas, the Netherlands, Hong Kong, Australia, the United Kingdom, and elsewhere (collectively, "the Hacking Platforms") to: (1) store malware; (2) stage attacks on protected computer networks; and (3) receive, store and share stolen Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution.

14. Members of the XU Group provided each other and others with unauthorized access to the protected computer networks and would locate, store, and transmit Network Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution from the Victims' networks.

15. Members of the XU Group hacked into the Victims' networks using various techniques, including, among others, SQL Injection Attacks, to steal, among other things,

Network Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution from the Victims' networks.

16. Once they hacked into the computer networks, members of the XU Group conducted network reconnaissance to find and to steal Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution from the Victims' networks.

17. Members of the XU Group communicated via the computer program Skype, which allowed them to use their Internet connections to talk to and advise each other in real time regarding how to navigate the Victims' networks and to locate Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution from the Victims' networks. By doing so, their electronic communications traveled between computers connected to the Internet from, among other places, Ontario, Canada, Delaware, Indiana, New Jersey, Maryland, and Australia.

18. Members of the XU Group used the computer program TeamViewer to remotely view other computer desktops in real time, and to allow them to communicate about their unauthorized access of the Victims' networks and the location of Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution from the Victims' networks. By doing so, their electronic communications traveled between

computers connected to the Internet from, among other places, Ontario, Canada, Delaware, Indiana, New Jersey, Maryland, and Australia.

19. Members of the XU Group communicated via the computer program AOL Instant Messenger ("AIM"), which allowed them to use their Internet connections to exchange messages with each other in real time; to share files; to provide access to websites they controlled; and to direct each other on how to navigate the Victims' networks and locate Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution from the Victims' networks. By doing so, their electronic communications traveled between computers connected to the Internet from, among other places, Ontario, Canada, Delaware, Indiana, New Jersey, Maryland, and Australia.

20. Members of the XU Group used computer servers located in various states and countries, including Utah, Texas, the United Kingdom, and Canada to store, receive and disseminate Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution stolen from the Victims' networks.

21. Members of the XU Group concealed their hacking into the Victims' networks by, among other things, conducting their hacking via Virtual Private Networks, including but not limited to computer programs that used encryption to protect communications transmitted via the Internet.

22. Members of the XU Group concealed their hacking into the Victims' networks by, among other things, disguising their true Internet Protocol addresses through the use of "proxies," or intermediary computers.

23. Members of the XU Group concealed their theft of Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution from the Victims' networks by encrypting the contents of their own computers and digital media with TrueCrypt and other encryption software.

24. Members of the XU Group concealed their activities within the Victims' computer networks by utilizing Log-In Credentials, Personal Identifiers, and Authentication Keys of other individuals to steal data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution from the Victims' computer networks.

Criminal Actions of AUSTIN ALCALA (a.k.a AAmonkey and AAmonkey1)

25. Beginning in or about January 2011 and continuing to the present, members of the XU Group utilized stolen Log-In Credentials to gain unauthorized access to Microsoft's computer networks, including the GDNP protected computer network, resulting in the theft of Log-In Credentials, Trade Secrets, and Intellectual Property relating to its Xbox gaming system. In particular, these individuals accessed GDNP with valid, but stolen, accounts associated with legitimate Microsoft software-development partners. The group then spent hundreds of hours searching through these networks for unprotected files.

26. Beginning in or before March 2012, members of the XU Group utilized stolen Log-In Credentials to gain unauthorized access to Zombie's computer networks, resulting in the theft of Log-In Credentials, Trade Secrets, and Intellectual Property related to Zombie software products.

27. During an online electronic communication session conducted by the co-conspirators via Skype on or about July 13, 2012 from computers connected to the Internet from Australia, Canada, Delaware, Maryland, and Indiana, David POKORA, Austin ALCALA, and other individuals discussed using compromised GDNP accounts to steal intellectual property from Microsoft, which they then could sell. They specifically discussed how they might divide the proceeds from such sales. During this session, one co-conspirator stated, "I know where you live Austin ALCALA."

28. During the July 13, 2012 online Skype session, the conspirators strategized about using a single account to obtain the intellectual property and avoid detection. ALCALA, who other co-conspirators referred to as "Austin" throughout the recorded session, stated that he "had an account" they could use to conduct the hack into the GDNP network. ALCALA also said he "had experience" gaining unauthorized access to GDN login credentials. The group discussed their expectation of being able to resell the intellectual property they planned to steal from Microsoft for up to $30,000. During the recorded session, the co-conspirators also stated, among other things:

Pokora: If you do multiple accounts it might raise a flag at GDN overall . . .

And then they might want to implement new security . . .

We don't want that . . .

We still want access to GDN, but we don't want to raise a flag at GDN ...

We just want to make them think that one developer was hacked ...

It'd be too weird if an entire like developer database...cause we want this access for the next generation of consoles as well

. . . .

ALCALA: What do we do if one of us gets caught?

. . . .

POKORA: If you're stealing 12 kits. That's worth a decent amount of money. Microsoft might come after you.

ALCALA: Dave, one of my accounts has access to order one more Durango.

29. On or about July 29, 2012, via computers connected to the Internet from, among other places, Delaware, Indiana, Maryland, Australia and Canada, Austin ALCALA, [redacted], Nathan LEROUX and others, including Person A, utilized TeamViewer software and stolen Log-In Credentials to access the computer network of Zombie Studios.

30. During this intrusion, [redacted] accessed pre-release software and software builds for gaming software being developed by Zombie Studios, as well as personally identifying information of Zombie Studios' employees. [redacted] transmitted the means of identification, including the name, social security number, home address, and tax documents, of "C.L.," a Zombie Studios employee, to Person A in Delaware; to Austin ALCALA, in Indiana; and to Nathan LEROUX, in Maryland. After gaining access to C.L.'s personally identifiable information, [redacted] subsequently submitted credit card applications in the names of C.L. and M.L, for limits of $15,000 and $10,000. [redacted] additionally attempted to open a "Lendingclub.com" account in the name of C.L for approximately $20,000. [redacted] accessed these accounts online and provided a Delaware mailing address associated with Person A to defeat financial institution anti-fraud countermeasures.

31. Person A subsequently received credit account activation notices in the names of C.L. and M.L. via United States Mail, at a Delaware address.

32. On or about February 20, 2013, Austin ALCALA, while accessing the Internet from a computer in Indiana, transmitted a database file named "db.html" to Person A, who was accessing the Internet from a computer in Delaware. The file contained approximately 11,621

stolen Log-In Credentials (*i.e.*, network username and password and email address) for victim computer networks that had been assembled by members of the XU Group.

33. On or about August 13, 2013, via computers connected to the Internet from, among other places, Delaware, Indiana, Canada, the United Kingdom, and Washington, Austin ALCALA, David POKORA, Person A and others utilized TeamViewer and Skype software to conduct computer intrusions into various private computer networks, including Microsoft's GDNP. The co-conspirators gained access to these protected computer networks by utilizing previously stolen means of identification of legitimate users of the computer networks.

34. At one point during the August 13, 2013 hacking session, David POKORA and Austin ALCALA referred to each other by their full names. One also said, "hello, Delaware," where Person A was located during the hacking session. POKORA then expressed concern about using their actual, full names during the session, stating "we always call each other by our aliases." At other points throughout the recorded hacking session, POKORA and ALCALA referred to each other as "Dave" and "Austin."

35. During this August 13, 2013 hacking session, Austin ALCALA, using a TeamViewer application under the alias "aamonkey," engaged in the following actions, among others:

a. Displayed a command window on his computer desktop that contained a home directory listed as "Austin Alcala."

b. Logged into an application called "Social Club," using the email address austin.alcala@yahoo.com.

c. Transmitted to co-conspirators and Person A, in Delaware, a series of victim credentials from "phpbb_db_backup_found.txt," identified as a

database dump taken from Autodesk, Inc.'s Scaleform web forum. The file contained email addresses (*i.e.*, user names) and unencrypted text (*i.e.*, user passwords). Multiple entries listed email addresses corresponding to email domain "scaleform.com." The file contained at least 11,266 entries.

d. Transmitted a file named "holyolo.txt" to co-conspirators and Person A, in Delaware. The file contained usernames, passwords, email addresses, and a possible date of birth for Ubisoft.com employee C.J. Also listed in the "holyolo.txt" file were Log-In Credentials for Popcap Games, Inc.'s ("Popcap") Virtual Private Network (VPN) and an individual webmail account for "hclark@popcap.com."

e. Copied credentials from the Scaleform file and attempted to login into Popcap's VPN, located at "corp.sea.popcap.com."

f. Performed an unauthorized login into the Gmail web account of [redacted]@popcap.com, that was transmitted to co-conspirators and Person A, in Delaware. During this login, ALCALA copied phone number "206-XXX-XXX" listed for "[redacted]" into "holyolo.txt." ALCALA also reviewed the saved web history for Gmail user "[redacted]"

g. Transmitted to co-conspirators and Person A, in Delaware, a spreadsheet named "kuju steam.xls." As ALCALA was opening the file in Microsoft Excel, the file properties were displayed, showing the "Authors" of the file as "Austin Alcala." This spreadsheet contained email addresses and passwords, along with the names of projects associated with each user, for Kuju Entertainment Ltd. ("Kuju.com"), a United Kingdom-based gaming

development company. ALCALA also logged into the Microsoft Hotmail.com account for "[redacted]XXXXhotmail.co.uk."

h. Transmitted to co-conspirators and Person A, in Delaware, the Log-In Credentials for "Sr. Software Engineer" at Electronic Arts (EA) Canada, from a file entitled "eacanada.txt."

i. Displayed to co-conspirators and Person A, in Delaware, his computer's Google Chrome cache, which had past download references to Microsoft's GDNP developer website (*i.e.*, developer.xboxlive.com). Visible were multiple Microsoft files that ALCALA had downloaded using the Google Chrome browser on or about August 12, 2013, including files labeled:

1. AllADKSamples 08 2013.zip
2. All XDKSamples 08 2013.zip
3. XboxOneADKdocsetup 08 2013.zip
4. XboxOne XDKdocsetup 08 2013.zip
5. SmartGlassSDK 08 2013.zip
6. XboxOneSymbols 08 2013.zip
7. XboxOneXDK 08 2013.zip
8. XboxOne Update 08 2013.zip

j. Displayed to co-conspirators and Person A, in Delaware, files on his local TrueCrypt disk that matched the XU Group's prior attempts to steal intellectual property relating to Microsoft's Xbox One. These included "GDN.txt," "Durango instructions.png," and "P4 Epic.txt." ALCALA

also displayed a folder named "Durango\Latest," which contained a file named "Xbox One Roadmap."

36. Also during the August 13, 2013 hacking session, Austin ALCALA conducted an online instant message chat with Skype user "[redacted]," who asked ALCALA how much he would charge "for the xna," which your affiant believes is a reference to a development kit for a prior version of the Xbox. ALCALA responded: "3100 total is fine." "[redacted]" responded by providing ALCALA with a "shipping address" in Austria and wrote, "off to paypal site" and, minutes later, "check your paypal." ALCALA then logged into the PayPal account under the name "[redacted]." With the "[redacted]" PayPal account still open and visible on his desktop," ALCALA wrote back to "[redacted]" in the Skype instant message chat: "which one," followed by "oh . . . got it." On ALCALA's desktop, two separate tabs were opened to "My Account – PayPal."

37. During an independent investigation into unauthorized access to Microsoft's Xbox Live gaming network, law enforcement agents in Washington obtained records for the PayPal account associated with the username "[redacted]." Business records produced by PayPal indicated that the account was created on or about August 24, 2010 and listed the account administrators as "Austin Alcala" and "[redacted]." PayPal records also listed the phone number (317) [redacted] as the contact number for the PayPal account. "317" is the area code that covers an area in central Indiana, including McCordsville, where ALCALA resides.

38. On or about September 26 and 27, 2013, two individuals (A[redacted] S. [redacted] and [redacted] E. A[redacted] used a stolen building security card to gain entry into secure buildings on the campus of Microsoft Corporation, in Redmond, Washington. S[redacted] and A[redacted] then stole three Xbox One development consoles, which are non-public versions of the Xbox One and which

contain confidential and proprietary intellectual property of Microsoft, including the source code for the Xbox One operating system. According to Microsoft, which captured the unlawful entry and theft on security video, the stolen equipment alone is valued at approximately $30,000.

39. On or about October 14, 2013, a Microsoft representative interviewed S[redacted], who admitted to entering the Microsoft building with a valid building security code stolen from a Microsoft employee. S[redacted] also admitted to stealing two Xbox One consoles. S[redacted] further admitted to giving one of these consoles to "Austin Alcala," by shipping it to an address in Colorado. S[redacted] claimed that he provided the Xbox One console to ALCALA in exchange for login credentials to the GDNP network that ALCALA possessed.

40. During a separate interview with a law enforcement agent on or about October 28, 2013, S[redacted] reported that he kept one of the stolen Xbox One consoles for himself. S[redacted] further stated that his friend shipped another of the stolen consoles to Austin ALCALA and the third stolen console to a person he knows as "Dave."

41. S[redacted] further stated that he received GDNP login credentials from ALCALA in return for the stolen Xbox One console, and that ALCALA had access to additional GDNP account credentials. S[redacted] also stated that he communicated with ALCALA online via Skype, AOL Instant Messenger and TeamViewer. In particular, S[redacted] said he engaged in TeamViewer sessions with Austin ALCALA and "Dave," during which they navigated around the Xbox Development Kit environment. S[redacted] stated that he has known Austin ALCALA for about six years, and "Dave" for about two years. S[redacted] stated that he initially met both men online, and has met them in person about three times in Seattle.

42. Microsoft's tentative commercial release date for the consumer version of Xbox One (which will not contain software source code intended to be accessible to consumers) has been publicly listed as November 22, 2013.

43. Pursuant to a search warrant executed upon the residence of co-conspirator Nathan LEROUX, a Motorola cell phone was seized. A forensic analysis of the cell phone revealed phone calls to and from the phone number (317) [redacted], which is listed in the PayPal records for the "[redacted]" account – one of the PayPal accounts that Austin ALCALA accessed during the August 13, 2013 hacking session.

44. The forensic analysis of LEROUX's cell phone revealed incoming phone calls to LEROUX's phone from the phone number (317) [redacted] (saved under the name "Captain D[redacted] L[redacted]") on July 31, 2013 and August 3, 2013. The phone's memory also contained entries for two outgoing phone calls to (317) [redacted] at approximately 12:34 a.m. (GMT) on August 13, 2013. In addition, the phone contained text messages referencing "aamonkey," one of ALCALA's online aliases.

45. On or about February 28, 2013, your affiant received information from Western Australia's Tech Crime Police (WAPOL) pursuant to search executed on [redacted]'s residence in Australia. WAPOL provided a cellular device log containing Skype records. Call log data stored on [redacted]'s phone referenced "aamonkey" with Skype user "Austin.alcala11."

46. During the course of the investigation, Paypal account "[redacted]@]hotmail.com" also was connected to members of the XU Group including Sanadodeh NESHEIWAT. In response to a subpoena, Paypal identified the following individual as having transferred funds to "[redacted][@]hotmail.com," on December 8, 2010 at 22:36:48 (GMT-05:00):

Name: Frank Alcala
email address: webmaster[@]undergroundforest.com
Shipping Address: Frank Alcala, [redacted] McCordsville, IN [redacted], United States
IP address [redacted].

47. A check of Indiana Department of Motor Vehicle records revealed a record for AUSTIN REED ALCALA that contained the following information:

Name - ALCALA, AUSTIN REED
[redacted]
Address - [redacted]
MC CORDSVILLE, INDIANA [redacted]
SEX/MALE HGT/603 WGT/220
HAI/BRO EYE/BLU

48. Based on the investigation, your affiant has learned that Austin ALCALA maintains a Facebook profile under the name "Austin Alcala." On or about November 6, 2013, your affiant reviewed this Facebook profile, which includes a profile picture depicting two white males. One of the depicted white males appears to be the same individual depicted in the DMV photograph and record for Austin ALCALA. Also, the month and day of birth listed in the Facebook profile of "Austin Alcala" matches the day and month of birth listed for Austin ALCALA in his DMV record.

49. Based on the above information, there is probable cause to believe that AUSTIN ALCALA has engaged in Identity Theft, Unauthorized Access to a Protected Computer Network, and Conspiracy, in violation of Title 18, United States Code, Sections 1028(a)(7) and 1030(a)(2)(C), (a)(6), and (c)(2)(B)(i) and (iii), and 371.

[redacted]

Sworn and subscribed before me
this 14 day of November 2013

Honorable Mary Pat Thynge
United States Magistrate Judge