

AO106 (Rev 5/85) Affidavit for Search Warrant

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

FILED**OCT 25 2007**

In the Matter of the Search of
 (Name, address or brief description of person, property, or premises to be searched)

**UNDER SEENIS. District and
 Bankruptcy Courts**

Yahoo!, Inc.
 701 First Avenue
 Sunnyvale, California 94089

**APPLICATION AND AFFIDAVIT
 FOR SEARCH WARRANT**

CASE NUMBER: **07-518-M-01**

(Further described below)

I Joseph Yuhasz being duly sworn depose and say:

I am a(n) Special Agent with the Federal Bureau of Investigation and have reason to believe
 (Official Title)

that ☐ on the person of or ☒ on the property or premises known as (name, description and or location)

Yahoo!, Inc., headquartered at 701 First Avenue, Sunnyvale, California, within the network operated by Yahoo!, Inc., including any file, mail and web servers located on these premises or operated by Yahoo!, Inc., at a co-located facility under their management.

in Sunnyvale, California, there is now concealed a certain person or property, namely (describe the person or property to be searched)

SEE EMAIL ACCOUNTS AND WEB SITES IN ATTACHMENT A

(further described in Attachment A)

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

evidence and instrumentalities

concerning a violation of Title 18 United States Code, Section(s) §§ 1343, 1028A, and 371. The facts to support a finding of Probable Cause are as follows:

SEE ATTACHED AFFIDAVIT INCORPORATED BY REFERENCE AS IF FULLY RESTATED HEREIN

Continued on the attached sheet and made a part hereof. ☒ YES ☐ NO

Gavin A. Corn
 U.S. Department of Justice
 (202) 353-9076

Joseph Yuhasz
 Signature of Affiant
 Joseph Yuhasz, Special Agent
 Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence

Date **DEBORAH A. ROBINSON**
U.S. MAGISTRATE JUDGE

Name and Title of Judicial Officer

at Washington, D.C.
Deborah A. Robinson
 Signature of Judicial Officer

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF)
Internet Service Provider YAHOO!, INC.,)
)

07-518-M-01
MAGISTRATE NO.
FILED UNDER SEAL

AFFIDAVIT

I, Joseph Yuhasz, being duly sworn depose, say, and provide the following information:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") assigned to work cyber crime matters. I have been employed by the FBI for approximately eight years. I have over 12 years of experience working with computers, to include working as a network engineer. As a Special Agent of the FBI, I am authorized to investigate crimes involving computer intrusions, Internet fraud, and identity theft. I am familiar with the information contained in this affidavit from information provided to me by other agents of the FBI, including FBI agents currently working in the Joint U.S.-Romanian Task Force located in Bucharest, Romania, my personal experience in investigating on-line fraud and other crimes, discussions with computer experts, and public source information available on the Internet. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter.

2. This affidavit is offered in support of an application for a warrant pursuant to 18 U.S.C. §§ 2703(a) and 2703(b)(1)(A) to compel Yahoo! Incorporated, headquartered at 701 First Avenue, Sunnyvale, CA 94089, which is a provider of electronic communication and remote computing services, to provide subscriber

information, records, and the contents of wire and electronic communications pertaining to the electronic mail ("e-mail") accounts identified below, and the contents of all files, code, and stored data associated with the web sites identified below. The accounts and web sites to be searched, which are further described in Attachment A, are as follows:

E-Mail Accounts:

rdnmp_2007@yahoo.com
 bibiana_vivi@yahoo.com
 gigi_shaw123@yahoo.com
 fc5vxbvxc@yahoo.com
 ac5bvxcbv@yahoo.com
 karjalakarjala123@yahoo.com
 cucurigu_boierimari@yahoo.com
 hau_gigi_be@yahoo.com
 cepwelameaam@yahoo.com
 gigifraierikasunt@yahoo.com
 haules_mucia@yahoo.com
 fan_tt_audi@yahoo.com
 ksajksadksad@yahoo.com
 kahnpath@yahoo.com
 margareta_xx1@yahoo.com

Web Sites¹:

www.brdro.net
 www.brd-ro.net
 www.conturi-brd.net
 www.cont-brdro.net
 www.nou-brdro.net
 www.rocont-brd.net
 www.cont-brd.net
 www.ro-brd.net
 www.confirmare-brd.net
 www.accessconturi-brd.net
 www.accesscont-brd.net
 www.internet-brd.net
 www.brd-bnkcadou.com

3. Based upon my training and experience, and after reviewing the evidence set forth in more detail below, I believe that these accounts were used by individuals in

¹ As described in more detail below, these web sites are "phishing" pages targeting a Romanian bank named Banca Română pentru Dezvoltare, Groupe Société Générale, commonly referred to as "BRD"

Romania² and the United States to commit Internet fraud and other crimes, including but not limited to engaging in a "phishing" scheme designed to obtain, through the use of fraud, victims' bank account and other personal information. Specifically, in a process known as "phishing," the subjects created and maintained fraudulent web pages that they designed to look like the legitimate web pages of a Romanian bank. They then used these phony bank web pages to lure bank customers and other victims into providing their personal information to the subjects, including the victims' bank account information." The evidence also indicates that these individuals facilitated their fraud schemes by using personal identity information stolen from US victims.

4. The phony web pages that the subjects used in their "phishing" scheme are associated with the Yahoo! e-mail accounts and web pages identified above. Thus, as set forth herein, there is probable cause to believe that, on the computer systems of Yahoo!, there exists evidence, fruits, and instrumentalities of the violations of Title 18, United States Code, Sections 1343 (wire fraud), 1028A (aggravated identity theft), and 371 (conspiracy to commit wire fraud and aggravated identity theft) (hereinafter the "Subject Offenses"). Based upon my training and experience, I believe that the email accounts associated with the phishing web sites may contain communications from victims and/or coconspirators in the Subject Offenses. I likewise believe that the web pages themselves are likely to contain computer files and code that will contain evidence of the offenses under investigation, including information related to where and how the web pages were

² Based upon information shared by the United States with Romanian law enforcement authorities, the Romanian National Police ("RNP") has identified three Romanian nationals who the RNP believes to be involved in the phishing attacks against BRD. These individuals are Dragos Tudor Beldea, DOB 3/21/1987, Victor Emanuel Bulacu, DOB 7/9/1987, and Sergiu Tudoricescu, DOB 5/16/1987. At this stage of the investigation, however, I am not of the fully aware of what involvement these individuals may have had in the events described in this affidavit.

created, and information related to how the stolen identity information was transmitted back to the perpetrators of the offenses.

5. In my training and experience, I have learned that Yahoo! is a company that provides free web-based Internet e-mail access to the general public and that stored electronic communications, including opened and unopened e-mail for Yahoo! subscribers, may be located on the computers of Yahoo! Further, I am aware that computers at Yahoo! contain information and other stored electronic communications belonging to third parties. Accordingly, this affidavit and application for search warrant seek authorization solely to search the computer accounts and/or files and following the procedures described herein and in Attachment A.

Background Regarding Phishing Schemes

6. I have had both training and experience in the investigation of computer-related crimes, including "phishing" schemes. Based on my training, experience, and knowledge, I know the following:

a) A "phishing" scheme is designed to lure victims, often customers of banks and other financial institutions, into providing criminals with the victims' personal information, including their bank account and credit card numbers, passwords, dates of birth, social security numbers, and other valuable personal data. This information is often in turn either used by the "phisher" to access victims' accounts or sold to other criminals on a black market Internet website. In many cases, the criminal will create a fraudulent "phishing" web page that closely resembles, or "spoofs," a legitimate web page, usually a bank or other financial institution's web page. This "phishing" page in turn prompts the victim to input his or her personal information, and it will typically have the ability to collect the victim's personal information and transmit it to the criminal.

b) In order to lure victims to visit the "phishing" web page and in turn input their personal information, the criminal will often send, or cause others to send, mass quantities of e-mail ("spam"). The spam e-mail purports to be sent from a representative of the relevant bank or financial institution, and the message

attempts to dupe the recipient into visiting the spoofed "phishing" web page. For example, the message will falsely warn that there is a problem with the victim's account and directs the victim to rectify the problem by clicking on a link that then takes the victim to the "phishing" web page. Operating under the mistaken belief that the victim is dealing with the real bank, the victim will then visit the "phishing" page and be tricked into entering his or her personal information.

c) Much like a legitimate web page, a "phishing" web page is compiled of one or more computer files. As described above, some of these files function to collect victims' personal information such as their names, addresses, and account information. By collecting these files, a list of victims and compromised accounts can be obtained. Sometimes the computer language that makes up the "phishing" web page also contains an e-mail address to which the collected victims' personal information can then be forwarded.

d) Criminals often do not use their own name or their own credit card when purchasing web hosting or other services to operate their "phishing" web pages. Rather, the fees associated with hosting a "phishing" web page are usually paid for using the names and credit card numbers of previous victims of identity theft.

e) To create a phishing site, criminals usually purchase a domain name (such as **www.brdro.net** or one of the other site-names identified above) and then buy space on the server of a web-hosting company such as Yahoo!. They then upload code to the web-hosting server to create a web page that looks like a legitimate site of a financial institution connected with the web site's name (such as BRD). "Phishers" often embed within this code scripts that either cause information entered into the phishing pages by victims to be transmitted directly to a database file that is then accessed by the criminals, or cause the information to be forwarded to an email address controlled by the criminals.

f) When creating web-sites on servers such as those provided by Yahoo!, individuals must provide email accounts. Usually these email accounts are associated with the Yahoo! user i.d. that must be created to obtain web-hosting services from Yahoo!. Occasionally, however, a second email account is provided by individuals as a contact point when creating a web site.

g) The e-mail address(es) provided when a "phishing" web page is posted on a web server sometimes contain communications pertinent to the "phishing" scheme. Many times it contains correspondence between co-conspirators. The e-mail address is rarely used for any legitimate purpose other than to facilitate the scheme.

Probable Cause

7. On or about March 29, 2007, the Romanian National Police ("RNP") became aware of what appeared to be a "phishing" web page that spoofed the web page of a Romanian bank named Banca Română pentru Dezvoltare, Groupe Société Générale, (hereinafter "BRD" or "BRD Bank"). The legitimate BRD web page is located at the following uniform resource locator ("url"): <http://www.brd.ro>, and is hosted by a BRD server in Romania. The "phishing" web page's address that spoofed the BRD web page was located at the following similarly-worded url: <http://www.brdro.net>. This "phishing" web page, which had no legitimate affiliation with BRD Bank, was hosted by Yahoo! Incorporated (hereinafter "Yahoo!"), which is headquartered at 701 First Avenue, Sunnyvale, CA 94089. Representatives of the RNP informed me that their investigation indicates that this web page is not affiliated with the BRD Bank web page and that it appears to be a "phishing" web page that is spoofing the BRD Bank web page.

8. Soon after this "phishing" web page was identified by the RNP, other similar "phishing" web pages also appeared on the Internet. All of these phishing web pages, which were hosted by Yahoo!, spoofed BRD Bank through the use of web names similar to the real BRD Bank's web page - a practice that is common among illegal phishing schemes. All of the web pages also used the web file with the same file name - "idehom.html" - indicating that they are somehow associated. The following is a complete list of urls of "phishing" web pages identified by the RNP and the dates they were first identified by the RNP:

www.brdro.net
www.brd-ro.net
www.conturi-brd.net

March 29, 2007
March 30, 2007
April 4, 2007

www.cont-brdro.net	May 4, 2007
www.nou-brdro.net	May 4, 2007
www.rocont-brd.net	May 4, 2007
www.cont-brd.net	April 9, 2007
www.ro-brd.net	April 16, 2007
www.confirmare-brd.net	April 16, 2007
www.accessconturi-brd.net	April 16, 2007
www.accesscont-brd.net	April 16, 2007
www.internet-brd.net	April 17, 2007
www.brd-bnkcadou.com	April 21, 2007 (Approximate)

9. The RNP provided this information to the joint U.S.-Romanian Task Force located in Bucharest, Romania. The RNP indicated that all of the above web addresses are fraudulent and have no legitimate purpose. The RNP also indicated that mass amounts of "spam" e-mail, or unsolicited e-mail, were sent across the Internet notifying recipients that something was wrong with their BRD Bank account and that they needed to click on a link to correct the problem. According to the RNP, the sender of the spam fraudulently represented himself/herself as a representative of BRD Bank. When the recipient of one of these spam emails would click on a link provided in the email, they would be directed to one of the above urls. This is typical for an illegal phishing scheme.

10. Within a few days of the phishing web pages' being posted on the Internet, the RNP and the FBI contacted Yahoo! and notified Yahoo! representatives of their existence. In response, Yahoo! shut the web sites down. The FBI Legal Attache in Romania requested that Yahoo! preserve existing records on these sites and the related email accounts pursuant to Title 18, United States Code, Section 2703(f).

11. All but one of the registration records for the above urls were obtained from Yahoo! Yahoo! records indicated that some of the above-referenced web domain accounts were created by a user or users who logged in from Romanian internet service providers. Others were created by a user or users who logged in from an America Online

("AOL") IP Address. Based upon my training and experience, I know that Romanian on-line scammers frequently use AOL's network to proxy into other accounts that they use to commit frauds. This provides an added level of security to obscure the identity of the criminals.

12. Several of the above listed web domain accounts were created by a user or user who logged into Yahoo!'s system from a computer that is controlled by a company in Bennington, Vermont. An agent of the FBI has communicated with an individual in that company who advised that they had no knowledge of the Yahoo! hosted sites and offered to allow the FBI to examine the company's computer server to determine if it were infected by some sort of computer malware. Based on my training and experience, I believe it is likely that the server in Vermont was accessed without the authority of its owner as a proxy to create the Yahoo! based phishing site. This practice is common among phishers and spammers.

13. According to Yahoo! records, the following individuals purchased the domain names and paid for the hosting of the "phishing" web pages using credit cards. Set forth below is a summary of records obtained from Yahoo! indicating the name of the url and the name of the person identified as purchasing the web hosting services from Yahoo!:

www.brdro.net	Daca Mer 820 N. Main Street Wakeeney, KS 67672
www.brd-ro.net	Marcia A. Hill 1314 79 th Avenue, Apt. B, Oakland, CA 94621
www.conturi-brd.net	Carrie M. Dobsch 3629 Humphrey

	St. Louis, MO 63116
www.cont-brdro.net	(Unknown)
www.nou-brdro.net	William Ellis 636 Prestwick Saint Clair, MI 48079
www.rocont-brd.net	Annette Karjala 17 Bodock Emporia, KS 66801
www.cont-brd.net	Bruce Toelle 557 Catherine Court Santa Rosa, CA 95409
www.ro-brd.net	Matthew Robin Wolfe 8232 Stewarts Ferry Parkway Nashville, TN 37214
www.confirmare-brd.net	Gordan B. Mann 1751 Las Brisas Santa Ana, CA 92866
www.accessconturi-brd.net	Kelly Beth Adams 1003 N. Main Street Carthage, TN 37030
www.accesscont-brd.net	Joseph Hommertzheim 115 N. Cherry Medicine Lodge, KS 67104
www.internet-brd.net	Janice Goodrich 810 No. Stevenson Court Liberty Lake, WA 99019
www.brd-bnkcadou.com	Stan Stan Str Lalelei CTA, 8700

14. When creating a web name through Yahoo!, an individual must first create an account name or login name with Yahoo! This account name corresponds with a Yahoo! e-mail address. Basically, each person who creates a web account through

Yahoo! will choose an account name or login name with a corresponding Yahoo! e-mail address. Yahoo! would normally communicate billing issues, technical issues, and other administrative issues with the individual through this associated Yahoo! e-mail address. When creating an account with Yahoo!, an individual sometimes lists an alternative e-mail address in addition to the corresponding Yahoo! address. Information provided by Yahoo! indicates the following:

15. On March 28, 2007, the web site **www.brdro.net** was created and hosted at Yahoo! The corresponding Yahoo! e-mail address was **rdnmp_2007@yahoo.com**. The individual who created this account listed an alternative e-mail address of **daca@brdro.net**.

16. On April 7, 2007, the web site **www.brd-ro.net** was created and hosted at Yahoo! The corresponding Yahoo! e-mail address was **bibiana_vivi@yahoo.com**.

17. On April 4, 2007, the web site **www.conturi-brd.net** was created and hosted at Yahoo! The corresponding Yahoo! e-mail address was **gigi_shaw123@yahoo.com**.

18. On April 5, 2007, the web site **www.cont-brdro.net** was created and hosted at Yahoo! The corresponding Yahoo! e-mail address was **fc5vxbvxc@yahoo.com**.

19. On April 5, 2007, the web site **www.nou-brdro.net** was created and hosted at Yahoo! The corresponding Yahoo! e-mail address was **ac5bvxcbv@yahoo.com**.

20. On April 5, 2007, the web site **www.nou-brdro.net** was created and hosted at Yahoo! The corresponding Yahoo! e-mail address was

ac5bvxcbv@yahoo.com. The individual who created this account listed an alternative e-mail address of **william@nou-brdro.net**.

21. On April 5, 2007, the web site **www.rocont-brd.net** was created and hosted at Yahoo! The corresponding Yahoo! e-mail address was **karjalakarjala123@yahoo.com**. The individual who created this account listed an alternative e-mail address of **annette@ www.rocont-brd.net** .

22. On April 9, 2007, the web site **www.cont-brd.net** was created and hosted at Yahoo! The corresponding Yahoo! e-mail address was **cucurigu_boierimari@yahoo.com**.

23. On April 16, 2007, the web page **www.ro-brd.net** was created and hosted at Yahoo! The corresponding Yahoo! e-mail address was **hau_gigi_be@yahoo.com**.

24. On April 16, 2007, the web page **www.confirmare-brd.net** was created and hosted at Yahoo! The corresponding Yahoo! e-mail address was **cepwelameaam@yahoo.com**.

25. On April 16, 2007, the web page **www.accessconturi-brd.net** was created and hosted at Yahoo! The corresponding Yahoo! e-mail address was **gigifraierikasunt@yahoo.com**. The individual who created this account listed an alternative e-mail address of **k@accessconturi-brd.net**.

26. On April 16, 2007, the web page **www.accesscont-brd.net** was created and hosted at Yahoo! The corresponding Yahoo! e-mail address was **haules_mucia@yahoo.com**. The individual who created this account listed an alternative e-mail address of **himi@accesscont-brd.net**.

27. On April 16, 2007, the web page **www.internet-brd.net** was created and hosted at Yahoo! The corresponding Yahoo! e-mail address was **fan_tt_audi@yahoo.com**.

28. On April 21, 2007, the web page **www.brd-bnkcadou.com** was created and hosted at Yahoo! The corresponding Yahoo! e-mail address was **ksajksadksad@yahoo.com**. The individual who created this account listed an alternative e-mail address of **stan@brd-bnkcadou.com**.

29. From contacting some of the individuals identified above whose names were identified as having purchased the "phishing" web sites, I have confirmed that at least some of these accounts appear to have been created with stolen credit card and identity information.

30. On September 13, 2007, I spoke with Marcia A. Hill. Hill stated that she never used the e-mail address **bibiana_vivi@yahoo.com** and she never purchased the web name **www.brd-ro.net**. Hill further confirmed that unauthorized charges appeared on her credit card from Yahoo! for a web account she never opened.

31. On September 10, 2007, I spoke with Carrie M. Dobsch. Dobsch stated that she never used the e-mail address **gigi_shaw123@yahoo.com** and she never purchased the web name **www.conturi-brd.net**. Dobsch further stated that unauthorized charges had appeared on her credit card a few months earlier. The unauthorized charges were for services at a web page called **whitepages.com**.

32. On September 10, 2007, I spoke with William Ellis. Ellis stated that he never used the e-mail address **ac5bvxcbv@yahoo.com** and he never purchased the web

name **www.nou-brdro.net**. Ellis further stated that unauthorized charges appeared on his credit card a few months earlier.

33. On September 11, 2007, I spoke with Bruce and Maryann Toelle. Both stated that they never used the e-mail address **cucurigu_bolerlmari@yahoo.com** and never purchased the web name **www.cont-brd.net**.

34. On September 10, 2007, I spoke with Gordan B. Mann. Mann stated that he never used the e-mail address **cepwelameaam@yahoo.com** and he never purchased the web name **www.confirmare-brd.net**. Mann further stated that unauthorized charges had appeared on his credit card a few months earlier.

Victims Targeted in the United States

35. As stated above, from assistance provided by the United States, the RNP and Romanian Prosecutor General's Office have identified individuals in Romanian who participated in the phishing scam against BRD Bank. The Romanian authorities subsequently obtained legal authority to intercept various communications of the targets of their investigation.

36. In October 2007, Romanian authorities investigating the BRD phishing scam advised the FBI Legal Attaché in Romania that the individuals under investigation in Romanian had recently directed a telephone-based scam against customers of Flagstar Bank in the Detroit, Michigan, area. According to information provided by the Romanians, from U.S. news coverage, and by an official from Flagstar Bank, customers of Flagstar Bank received recorded telephone calls claiming to be from the bank and requesting that the customers provide their account numbers and PINs. The perpetrators of this scam used "voice broadcasting" services through the Internet to send out these

messages. These services allow a user to upload a calling list of numbers and then a recorded voice message. The service then places the pre-recorded calls to the individuals on the list. According to the Romanian authorities, they detected the Flagstar Bank scam through intercepted communications of the BRD phishing scam suspects.

37. The Romanian authorities also advised that they intercepted communications of individuals in the United States who were picking up money transfers for the individuals conducting the fraud schemes in Romania. On October 7, 2007, the Romanian authorities intercepted a Yahoo! "InstantMessage" chat session between Yahoo! users **kahnpaht**, who claims to be in Arizona, and **margareta_xxl**, which is a user i.d. of one of the subjects of the Romanian investigation. Relevant portions of this chat session are detailed below:

10/07/2007 05:21:39 margareta_xxl hi
 10/07/2007 05:21:50 kahnpaht hi u got my message?
 10/07/2007 05:21:53 margareta_xxl no
 10/07/2007 05:21:55 kahnpaht can we work it out?
 10/07/2007 05:22:29 kahnpaht i said my runners kinda ran out on me so im stuck with some debt so i need alot of work to pay u and ur boys out of my %
 10/07/2007 05:23:28 margareta_xxl so you cant send the 3k
 10/07/2007 05:23:29 margareta_xxl ?
 10/07/2007 05:23:35 kahnpaht i can send \$
 10/07/2007 05:23:50 kahnpaht is np but is kinda ugly for me
 10/07/2007 05:23:57 kahnpaht but dont worry if u cant work
 10/07/2007 05:24:03 kahnpaht fisrt thing monday morning
 10/07/2007 05:24:22 kahnpaht u will have 3.5k for the trouble
 10/07/2007 05:24:33 margareta_xxl dude
 10/07/2007 05:24:40 margareta_xxl we need you to be fast with the money if you want us to work
 10/07/2007 05:24:48 kahnpaht man
 10/07/2007 05:24:50 kahnpaht from now on
 10/07/2007 05:24:54 kahnpaht i will do them on my own
 10/07/2007 05:25:06 kahnpaht i mooved to arizona so i can pos on vucom
 10/07/2007 05:25:20 kahnpaht and that is the fastest way in the game
 10/07/2007 05:25:28 margareta_xxl whats vucom?
 10/07/2007 05:25:34 kahnpaht a atm
 10/07/2007 05:25:39 kahnpaht i use to send wu's to my name

10/07/2007 05:25:42 kahnpaht from cards
10/07/2007 05:25:44 margareta_xxl aaaa

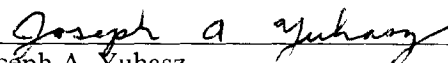
10/07/2007 05:25:49 kahnpaht i can pos so very fast
10/07/2007 05:25:56 kahnpaht no checks involved or anything
10/07/2007 05:25:59 kahnpaht just pure cash
10/07/2007 05:26:14 margareta_xxl ok
10/07/2007 05:26:19 margareta_xxl so we'll work monday
10/07/2007 05:26:28 kahnpaht then monday night
10/07/2007 05:26:30 kahnpaht ur time
10/07/2007 05:26:36 kahnpaht u will have a fat mten from me
10/07/2007 05:27:02 kahnpaht and i engage in paying bulacu the 4.5k
10/07/2007 05:27:07 kahnpaht we wasted on wu
10/07/2007 05:27:12 margareta_xxl ok:)
10/07/2007 05:27:17 margareta_xxl have you spoken lately to john
10/07/2007 05:27:17 margareta_xxl ?
10/07/2007 05:27:25 kahnpaht no
10/07/2007 05:27:30 kahnpaht he ripped alot of people off
10/07/2007 05:27:31 kahnpaht here
10/07/2007 05:27:39 kahnpaht not his supplier but people he knows
10/07/2007 05:27:53 margareta_xxl is there any chance I get my 2k?
10/07/2007 05:27:55 kahnpaht his friends
10/07/2007 05:28:00 kahnpaht get me work
10/07/2007 05:28:03 kahnpaht and ill pay u
10/07/2007 05:28:14 margareta_xxl ok
10/07/2007 05:28:21 margareta_xxl monday we start working
10/07/2007 05:28:26 kahnpaht ok
10/07/2007 05:28:29 kahnpaht have fun
10/07/2007 05:28:31 kahnpaht cya then
10/07/2007 05:28:32 margareta_xxl but be fast
10/07/2007 05:28:38 kahnpaht light speed
10/07/2007 05:28:39 margareta_xxl dont waste a lot of time
10/07/2007 05:28:53 kahnpaht my only 2 words are light speed
10/07/2007 05:28:57 margareta_xxl ok
10/07/2007 05:29:02 kahnpaht cya mday
10/07/2007 05:29:04 margareta_xxl cya

Conclusion

38. Based upon the foregoing and my training and experience as a Special Agent of the FBI, I submit that probable cause exists to believe the e-mail accounts and web-site files on the computer systems owned, maintained, and/or operated by Yahoo!,

Inc., headquartered at 701 First Avenue, Sunnyvale, California 94089, identified herein and in Attachment A, will contain evidence, fruits and instrumentalities of the Subject Offenses. These include, but are not limited to, personal information of victims such as their name and account numbers, information regarding stolen identity and credit card data from U.S. victims, correspondence in the form of e-mail messages relevant to the "phishing" schemes, and code and scripts related to the transmission of data from victims of the phishing scams to members of the criminal organization. By this affidavit and application, I request that the Court issue search warrants directed at Yahoo! compelling the production of the e-mail, web domain files, and other information stored on the Yahoo! servers for the Subject Accounts and associated files listed herein and in Attachment A, following the search procedure described in Attachment A.

I swear the above statements are true and correct.


Joseph A. Yuhasz
Special Agent
Federal Bureau of Investigation

OCT 25 2007
Subscribed and sworn to before
me on October ____, 2007


UNITED STATES MAGISTRATE JUDGE
DEBORAH A. ROBINSON
U.S. MAGISTRATE JUDGE

ATTACHMENT A

I. Search Procedure

1. The search warrant will be presented to Yahoo!, Inc., personnel who will be directed to isolate those accounts and files described herein;
2. In order to minimize any disruption of computer service to innocent third parties, Yahoo!, Inc., employees trained in the operation of computers will create an exact duplicate of the computer accounts and files described below, including an exact duplicate of all information stored in the computer accounts or files described below;
3. Yahoo!, Inc., personnel will provide the exact duplicate of the accounts and files described below, and all information stored in those accounts and/or files to the Special Agent who serves the search warrant;
4. Law enforcement personnel will thereafter review the information stored in the accounts and files received from Yahoo!, Inc., for evidentiary purposes to determine which files and emails are responsive to the warrant.

II. Files and Accounts to be Produced

With respect to the following electronic mail addresses, domain names, and/or individual accounts:

E-Mail Accounts:

rdnmp_2007@yahoo.com
bibiana_vivi@yahoo.com
gigi_shaw123@yahoo.com
fc5vxbvxc@yahoo.com
ac5bvxcbv@yahoo.com
karjalakarjala123@yahoo.com
cucurigu_boierimari@yahoo.com
hau_gigi_be@yahoo.com
cepwelameaam@yahoo.com
gigifraierikasunt@yahoo.com

haules_mucia@yahoo.com
fan_tt_audi@yahoo.com
ksajksadksad@yahoo.com
kahnpath@yahoo.com
margareta_xxl@yahoo.com

Web Sites:

www.brdro.net
www.brd-ro.net
www.conturi-brd.net
www.cont-brdro.net
www.nou-brdro.net
www.rocont-brd.net
www.cont-brd.net
www.ro-brd.net
www.confirmare-brd.net
www.accessconturi-brd.net
www.accesscont-brd.net
www.internet-brd.net
www.brd-bnkcadou.com

1. Account information and any linked accounts, from May 1, 2006, through and including the date of this warrant, including:

- a. Names and associated e-mail addresses;
- b. Physical address and location information;
- c. Records of session times and durations;
- d. Length of service (including start date) and types of service utilized;
- e. Telephone or instrument number or other number or identity for the above-listed accounts and domain names, including any temporarily assigned network address;
- f. The means and source of payment for such service (including any credit card or bank account number);
- g. Internet Protocol addresses used by the above-listed accounts and domain names to register the accounts and domain names or otherwise initiate service;

- h. Buddy lists (or similar data), address books, group affiliations, message board usage, chat room nicknames;
- i. Any personal web space, including photo pages; and
- j. Any search queries or accumulated cookies.

2. User connection logs and communications for the above-listed accounts and any linked accounts and domain names for May 1, 2006, through and including the date of this warrant, for any connections to or from the above-listed accounts or any linked accounts and domain names. User connection logs shall include the following:

- a. Connection time and date;
- b. Disconnect time and date;
- c. Method of connection to system (e.g., SLIP, PPP, Shell);
- d. Data transfer volume (e.g., bytes);
- e. The IP address that was used when the user connected to the service;
- f. Connection information for other systems to which the user connected via the above-listed accounts or any linked accounts and domain names, including:
 - g. Connection destination;
 - h. Connection time and date;
 - i. Disconnect time and date;
 - j. Method of connection to system (e.g., telnet, ftp, http);
 - k. Data transfer volume (e.g., bytes); and
 - l. Any other relevant routing information;

3. Source or destination of any wire or electronic mail messages sent from or received by the above-listed accounts, or any linked accounts and domain names, and the

date, time, and length of the message; and

4. Any address to which the wire or electronic mail was or is to be forwarded from the above-listed accounts or any linked accounts or e-mail address.

5. The contents of wire and electronic communications, including attachments and stored files, and the contents of all files, code, and stored data associated with the web sites/domains, for the above-listed accounts and domain names, from May 1, 2006, through and including the date of this warrant, including received messages, sent messages, deleted messages, and messages maintained in trash or other folders, and all other available data, files, and computer code associated with the web domains identified above.