MELINDA HAAG (CABN 132612)
United States Attorney

MIRANDA KANE (CABN 150630)
Chief, Criminal Division

MATTHEW A. LAMBERTI (DCBN 460339)
Assistant United States Attorneys

150 Almaden Boulevard, Suite 900
San Jose, California 95113
Telephone: (408) 535-5061
Facsimile: (408) 535-5066
E-Mail: Matt.Lamberti@usdoj.gov

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

SHAWN D. HOGAN,

Defendant.

No. CR 10-0495 EJD

DECLARATION OF MATTHEW A. LAMBERTI SUPPORTING THE UNITED STATES' OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

Date:	October 30, 2012
Time:	10:00 a.m.
Court:	Hon. Edward J. Davila

I, Matthew A. Lamberti, declare:

1. I am the Assistant United States Attorney assigned to prosecute the above-captioned case.

2. Attached hereto as Exhibit 1 is a true and correct copy of an application and affidavit for search warrant and a search warrant for 8465 Regents Road, #448, San Diego, California approved June 15, 2007 by Magistrate Judge Ruben B. Brooks.

3. Attached hereto as Exhibit 2 is a true and correct copy of a report prepared by various FBI agents on June 19, 2007 regarding the execution of the search warrant at 8465 Regents Road, #448, San Diego, California on June 18, 2007.

4. Attached hereto as Exhibit 3 is a true and correct copy of a floor plan for 8465 Regents Road, #448, San Diego, California, provided by Regents Court on October 15, 2012.

5. Attached hereto as Exhibit 4 is a true and correct copy of photos taken by FBI Special Agent Nathaniel Dingle on June 18, 2007 at 8465 Regents Road, #448, San Diego, California.

6. Attached hereto as Exhibit 5 is a true and correct copy of a photo taken by Special Agent Dingle on June 18, 2007 at 8465 Regents Road, #448, San Diego, California.

7. Attached hereto as Exhibit 6 is a true and correct copy of a photos taken by Special Agent Dingle on June 18, 2007 at 8465 Regents Road, #448, San Diego, California.

8. Attached hereto as Exhibit 7 is a true and correct copy of an FBI report summarizing an interview with defendant Shawn D. Hogan that took place on June 18, 2007, and which is dated June 19, 2007.

9. Attached hereto as Exhibit 8 is a true and correct copy of consent forms signed by the defendant on June 18, 2007.

10. Attached hereto as Exhibit 9 is a true and correct copy of a photo taken by Special Agent Dingle on June 18, 2007 at 8465 Regents Road, #448, San Diego, California.

11. Attached hereto as Exhibit 10 is a true and correct copy of an FBI report regarding a meeting between FBI Special Agent Todd Walbridge and the defendant on June 21, 2007, dated June 25, 2007, and a receipt for property involved in this meeting, dated June 21, 2007.

12. Attached hereto as Exhibit 11 is a true and correct copy of an FBI report regarding a meeting between Special Agent Walbridge and FBI Special Agent Travis Johnson and the defendant on August 13, 2007, dated August 15, 2007, and a receipt for property involved in this meeting, dated August 13, 2007.

13. Attached hereto as Exhibit 12 is a true and correct copy of an email exchange between FBI Special Agent Melanie Adams and the defendant on August 29, 2007.

14. Attached hereto as Exhibit 13 is a true and correct copy of an FBI report regarding a letter received by Special Agent Adams from the defendant on March 17, 2009, dated March 18, 2009, and the letter itself, dated March 10, 2009.

///

///

///

15. Attached hereto as Exhibit 14 is a true and correct copy of a blog entry posted by the defendant entitled "Ramblings Of A Wannabe Alien..." at blogs.digitalpoint.com on August 2, 2010.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed on October 16, 2012, in San Jose, California

/s/

MATTHEW A. LAMBERTI
Assistant United States Attorney

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

In the Matter of the Search of

8465 Regents Road, #448
San Diego, California 92112

SEARCH WARRANT

CASE NUMBER: '07 MJ 1396

TO: Special Agent Todd Walbridge and any Authorized Officer of the United States:

Affidavit having been made before me by Special Agent Todd Walbridge of the Federal Bureau of Investigation who has reason to believe that on the premises known as:

See Attachment A

in the Southern District of California there is now concealed a certain person or property, namely:

See Attachment B

which constitutes evidence, fruits, and instrumentalities of criminal violations of Title 18, United States Code, Section 1343 (wire fraud).

ORDERED SEALED BY COURT

I am satisfied that the affidavit and any recorded testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before June 24, 2007 (not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search in the daytime (6:00 A.M. to 10:00 P.M.) and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to Hon. Ruben B. Brooks, United States Magistrate Judge, as required by law.

Issued:

June 15, 2007 at 3:50 ~~am~~/pm at San Diego, California
RBB

Ruben B. Brooks
HONORABLE RUBEN B. BROOKS
UNITED STATES MAGISTRATE JUDGE

PENGAD-Bayonne, N.J. GOVERNMENT EXHIBIT 1

RETURN

DATE WARRANT RECEIVED	DATE AND TIME WARRANT EXECUTED	COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH

INVENTORY MADE IN THE PRESENCE OF:

INVENTORY OF PERSON OR PROPERTY TAKEN PURSUANT TO THE WARRANT

CERTIFICATION

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

Subscribed, sworn to, and returned before me this date.

U.S Judge or Magistrate Judge

Date

ATTACHMENT A
DESCRIPTION OF LOCATION TO BE SEARCHED

The SUBJECT PREMISES, 8465 Regents Road, Apartment 448, San Diego, California, 92122 is described as an apartment located inside the Regents Court Apartment Complex. The complex is a stucco, four-story structure. Apartment #448 is located in the northeast corner of the complex on the fourth (top) floor. The numbers "448" are visible next to the entrance to the residence, which is a brown door.

ATTACHMENT B

ITEMS TO BE SEIZED

The records, documents, and materials to be seized from the SUBJECT PREMISES, 8465 Regents Road, #448, San Diego, CA 92122 (the residence of Shawn Hogan and the business address of Digital Point Solutions) that constitute evidence of violations of 18 U.S.C. § 1343 (wire fraud) include:

a. Computer files, logs, programs, scripts, or source code that refer to eBay, the eBay Affiliate Program, Digital Point Solutions, Commission Junction, and/or ValueClick or that refer to or contain tools, created, used, or distributed by Shawn Hogan and/or Digital Point Solutions (DPS) through Hogan's/DPS's ad network (e.g., "geovisitors," "website-country," "fmdigger," "zone-transfer," "keywords," "co-op ad" code, "network-ad") or any other tool, script or code that contains 1x1 (or similar size) pixels or that causes forced clicks, cloaking re-directs, cookie-stuffing, cookie-tracking, tracking tags, and/or web beacons, including any computer files, logs, programs, scripts, source code, or object code related to the development of any of the above tools;

b. Letters, documents, records, notes, E-mail, diaries, journals or other written commuications regarding eBay, the eBay Affiliate Program, Digital Point Solutions, Commission Junction, and/or ValueClick, or that refer to or contain tools created, used, or distributed by Shawn Hogan, and/or Digital Point Solutions, (e.g., "geovisitors," "website-country, "fmdigger," "zone-transfer," "keywords," "co-op ad" code, "network-ad"), any other tool, script or code that contains 1x1 (or similar size) pixels or that causes forced clicks, cloaking re-directs, cookie-stuffing, cookie-tracking, tracking tags, and/or web beacons, including any computer files, logs, programs, scripts, source code, or object code related to the development of any of the above tools;

~~c. Any and all electronic data storage media relating to items (b) and (c) above, capable of storing any of the items (d) and (e) above. Such media includes, but is not limited to computer hard drives, floppy diskettes, "Zip" or "Jaz" disks, flash drives, data tapes, or CD-ROM or DVD-ROM disks;~~

d. All electronic mail stored and presently contained in or on the computers located at the SUBJECT PREMISES that pertain to:

1. The websites www.shawnhogan.com or www.digitalpoint.com;

2. The eBay Affiliate Program, Digital Point Solutions, Commission Junction, ValueClick, or cookie-stuffing or other actions related to the placement of cookies on users' computers;

3. Conversations between Shawn Hogan, Brian Dunning, Todd Dunning or others related to cookie-stuffing or other actions related to the

placement of cookies on users' computers;

4. All Internet routing and header information relating to those communications described in paragraphs d.1, d.2, and d.3, above;

e. Any and all transactional information, to include log files, of all computer activity related to eBay's Affiliate Program, Commission Junction, ValueClick, or Shawn Hogan, or to the websites, www.shawnhogan.com, www.digitalpoint.com, the IP address range 216.9.35.48 through 216.9.35.63, and Digital Point Solutions, which includes dates, time, method of connecting, port, dial-up, and/or location;

f. All business records that pertain to eBay, the eBay Affiliate Program, Commission Junction, ValueClick, Digital Point Solutions, or Shawn Hogan, or to the websites, www.shawnhogan.com, www.digitalpoint.com, including but not limited to spreadsheets, applications, subscribers' full names, buddy lists, aliases, associated and alternate e-mail addresses, all screen names, method of payment, phone numbers, addresses, and detailed billing records;

g. All files, to include log files, scripts, source code, and tools, contained on the computer devices related to the company Digital Point Solutions and the websites www.shawnhogan.com and www.digitalpoint.com and/or the IP address range 216.9.35.48 through 216.9.35.63, and/or servers for Digital Point Solutions;

h. Indicia of residence and indicia of use of computers within the residence;

i. Documents, records, communications, scripts, source code, and/or files related to computer tools created, used, or distributed by Shawn Hogan, and/or Digital Point Solutions (e.g., "geovisitors," "website-country, "fmdigger," "zone-transfer," "keywords," "co-op ad" code, "network-ad") or any other tool that may contain 1x1 (or similar size) pixels;

j. Documents, records, communications, scripts, source codes and/or files related to forcing clicks, cloaking re-directs, cookie-stuffing, cookie-tracking, tracking tags and/or web beacons;

k. Documents, records, communications, and/or files related to tracking codes to track individual ad campaigns and/or advertising on various sites, to include spreadsheets and databases maintaining such information;

l. Documents and/or files related to Digital Point Solutions Forum, http://forums/digitalpoint.com, to include names of the members and/or owners, members of the Forum that may have downloaded free tools that contain the 1x1 (or similar size) pixel, conversations within the Forum involving forcing clicks, cloaking re-directs, cookie-stuffing, cookie-tracking, tracking tags, web beacons, or other techniques to defraud;

m. Records or communications between Hogan and others concerning the lawfulness or propriety of cookie-stuffing schemes, including records or communications between Hogan and others discussing the Terms and Conditions of eBay's Affiliate program;

n. Document and/or files regarding bank accounts and financial papers of Shawn Hogan and/or Digital Point Solutions, to include but not limited to all records of deposits from eBay, Commission Junction, and/or ValueClick.

o. Records regarding financial expenditures of monies paid to Hogan/Digital Point Solutions from eBay, Commission Junction, and/or Value Click, to include purchases or sales of assets such a vehicles, property, jewelry, computer equipment, or other assets related to Shawn Hogan and/or Digital Point Solutions since December 2003.

p. Records regarding any other websites affiliated with Shawn Hogan or Digital Point Solutions since December 2003;

q. Records or communications between Hogan and/or Digital Point Solutions and others discussing any contracts, requests for services, letters of engagement, investigative plans, or invoices related to services provided to or for eBay, and/or the eBay Affiliate Program and/or Commission Junction and/or ValueClick;

r. Records or communications between Hogan and/or Digital Point Solutions and others discussing the names and identities of all individuals and third parties who were used to procure, or to attempt to procure websites, advertisements, tools and scripts related to cookie stuffing related to eBay or any e-commerce company;

DEFINITIONS

a. The terms "records," "documents," "materials," "programs," "files," "logs," "scripts," "source code," "object code," "communications," "notes," or "applications" include all of the items in whatever form and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

1. Computer Hardware

Computer hardware consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. This includes any data-processing devices (such as central processing units, memory typewriters, self-contained "laptop" or "notebook" computers, Personal Digital Assistants (PDAs), or "Blackberries"); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, compact flash cards, smart media cards and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

2. Computer Software

Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way it works. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs, utilities, compilers, interpreters, and communications programs).

3. Computer-related Documentation

Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

4. Computer Passwords and Other Data Security Devices

Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

5. Computers

The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

COMPUTER SEARCH PROTOCOL

a. Agents executing this search warrant will employ the following procedures regarding computers that may be found on the premises which may contain information subject to seizure pursuant to this warrant:

Forensic Imaging

1. After securing the premises, the executing agents will consult with a computer specialist to determine the feasibility of obtaining forensic images of electronic storage devices while on-site. The feasibility decision will be based upon the number of devices, the nature of the devices and the volume of data to be imaged. The preference is to image on-site if it can be done in a reasonable amount of time and without jeopardizing the integrity of the data and the safety of the agents. The number and type of computers and other devices and the number, type, and size of hard drives are of critical importance. It can take several hours to image a single hard drive — the bigger the drive, the longer it takes. As additional devices and hard drives are added, the length of time that the agents must remain on-site can become overly intrusive, dangerous, and impractical.

2. If it is not feasible to image the data on-site, the computer equipment and any peripherals will be seized and transported off-site for imaging. Once a verified image has been obtained, the owner of the equipment will be notified and the equipment returned within thirty (30) days of seizure absent further application to this court.

3. A forensic image is an exact physical copy of the hard drive or other media. It is essential that a forensic image be obtained prior to conducting any search of the data for information subject to seizure pursuant to this warrant. A forensic image captures all of the data on the hard drive or other media without the data being viewed and without changing the data in any way. This is in sharp contrast to what transpires when a computer running the common Windows operating system is started, if only to peruse and copy data — data is irretrievably changed and lost. Here is why: When a Windows computer is started, the operating system proceeds to write hundreds of new files about its status and operating environment. These new files may be written to places on the hard drive that may contain deleted or other remnant data. That data, if overwritten, is lost permanently. In addition, every time a file is accessed, unless the access is done by trained professionals using special equipment, methods and software, the

operating system will re-write the metadata for that file. Metadata is information about a file that the computer uses to manage information. If an agent merely opens a file to look at it, Windows will overwrite the metadata which previously reflected the last time the file was accessed. The lost information may be critical.

4. Special software, methodology, and equipment is used to obtain forensic images. Among other things, forensic images normally are "hashed," that is, subjected to a mathematical algorithm to the granularity of 1038 power, an incredibly large number much more accurate than the best DNA testing available today. The resulting number, known as a "hash value" confirms that the forensic image is an exact copy of the original and also serves to protect the integrity of the image in perpetuity. Any change, no matter how small, to the forensic image will affect the hash value so that the image can no longer be verified as a true copy.

Forensic Analysis

5. After obtaining a forensic image, the data will be analyzed. Analysis of the data following the creation of the forensic image is a highly technical process that requires specific expertise, equipment and software. There are literally thousands of different hardware items and software programs that can be commercially purchased, installed and custom-configured on a user(s computer system. Computers are easily customized by their users. Even apparently identical computers in an office environment can be significantly different with respect to configuration, including permissions and access rights, passwords, data storage and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

6. Analyzing the contents of a computer, in addition to requiring special technical skills, equipment and software also can be very tedious. It can take days to properly search a single hard drive for specific data. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. As mentioned above, the computer may have stored information about the data at issue: who created it, when it was created, when was it last accessed, when was it last modified, when was it last printed and when it was deleted. Sometimes it is possible to recover an entire document that never was saved to the hard drive if the document was printed. Operation of the computer by non-forensic technicians effectively destroys this and other trace evidence. Moreover, certain file formats do not lend themselves to keyword searches. Keywords search text. Many common electronic mail, database and spreadsheet applications do not store data as searchable text. The data is saved in a proprietary non-text format. Microsoft Outlook data is an example of a commonly used program that stores data in a non-textual, proprietary manner; ordinary keyword searches will not reach this data. Documents printed by the computer, even if the document never was saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. Similarly, faxes sent to the computer are stored as

graphic images and not as text.

7. Analyzing data on-site has become increasingly impossible as the volume of data stored on a typical computer system has become mind-boggling. For example, a single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now capable of storing more than 100 gigabytes of data and are commonplace in new desktop computers. And, this data may be stored in a variety of formats or encrypted. The sheer volume of data also has extended the time that it takes to analyze data in a laboratory. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. Even perusing file structures can be laborious if the user is well-organized. Producing only a directory listing of a home computer can result in thousands of pages of printed material most of which likely will be of limited probative value.

8. Based on the foregoing, searching any computer or forensic image for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained; criminals can mislabel and hide files and directories, use codes to avoid using keywords, encrypt files, deliberately misspell certain words, delete files, and take other steps to defeat law enforcement. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear necessary to locate and retrieve digital evidence within the scope of this warrant.

9. All forensic analysis of the imaged data will be directed exclusively to the identification and seizure of information within the scope of this warrant.

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

In the Matter of the Search of

8465 Regents Road, #448
San Diego, California 92112

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

CASE NUMBER: '07 MJ 1396

I, Todd Walbridge,. being duly sworn depose and say:

I am a Special Agent of the Federal Bureau of Investigation and have reason to believe that on the property or premises known as:

See Attachment A

in the Southern District of California there is now concealed a certain person or property, namely:

See Attachment B

which is:

Evidence, fruits of crime, property designed for use or used in committing criminal offenses including violations of Title 18, United States Code, Section 1343 (wire fraud). The facts to support a finding of probable cause are as follows:

See attached Affidavit of Todd Walbridge continued on the attached sheet and made a part hereof. _X_ Yes _____ No

TODD WALBRIDGE
Special Agent
Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence
June 15, 2007 at San Diego, California:

Ruben Brooks

HON. RUBEN B. BROOKS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
DESCRIPTION OF LOCATION TO BE SEARCHED

The SUBJECT PREMISES, 8465 Regents Road, Apartment 448, San Diego, California, 92122 is described as an apartment located inside the Regents Court Apartment Complex. The complex is a stucco, four-story structure. Apartment #448 is located in the northeast corner of the complex on the fourth (top) floor. The numbers "448" are visible next to the entrance to the residence, which is a brown door.

ATTACHMENT B

ITEMS TO BE SEIZED

The records, documents, and materials to be seized from the SUBJECT PREMISES, 8465 Regents Road, #448, San Diego, CA 92122 (the residence of Shawn Hogan and the business address of Digital Point Solutions) that constitute evidence of violations of 18 U.S.C. § 1343 (wire fraud) include:

a. Computer files, logs, programs, scripts, or source code that refer to eBay, the eBay Affiliate Program, Digital Point Solutions, Commission Junction, and/or ValueClick or that refer to or contain tools, created, used, or distributed by Shawn Hogan and/or Digital Point Solutions (DPS) through Hogan's/DPS's ad network (e.g., "geovisitors," "website-country," "fmdigger," "zone-transfer," "keywords," "co-op ad" code, "network-ad") or any other tool, script or code that contains 1x1 (or similar size) pixels or that causes forced clicks, cloaking re-directs, cookie-stuffing, cookie-tracking, tracking tags, and/or web beacons, including any computer files, logs, programs, scripts, source code, or object code related to the development of any of the above tools;

b. Letters, documents, records, notes, E-mail, diaries, journals or other written commuications regarding eBay, the eBay Affiliate Program, Digital Point Solutions, Commission Junction, and/or ValueClick, or that refer to or contain tools created, used, or distributed by Shawn Hogan, and/or Digital Point Solutions, (e.g., "geovisitors," "website-country, "fmdigger," "zone-transfer," "keywords," "co-op ad" code, "network-ad"), any other tool, script or code that contains 1x1 (or similar size) pixels or that causes forced clicks, cloaking re-directs, cookie-stuffing, cookie-tracking, tracking tags, and/or web beacons, including any computer files, logs, programs, scripts, source code, or object code related to the development of any of the above tools;

c. ~~Any and all electronic data storage media relating to items (b) and (c) above, capable of storing any of the items (d) and (e) above. Such media includes, but is not limited to computer hard drives, floppy diskettes, "Zip" or "Jaz" disks, flash drives, data tapes, or CD-ROM or DVD-ROM disks;~~ ✓

d. All electronic mail stored and presently contained in or on the computers located at the SUBJECT PREMISES that pertain to:

1. The websites www.shawnhogan.com or www.digitalpoint.com;

2. The eBay Affiliate Program, Digital Point Solutions, Commission Junction, ValueClick, or cookie-stuffing or other actions related to the placement of cookies on users' computers;

3. Conversations between Shawn Hogan, Brian Dunning, Todd Dunning or others related to cookie-stuffing or other actions related to the

placement of cookies on users' computers;

4. All Internet routing and header information relating to those communications described in paragraphs d.1, d.2, and d.3, above;

e. Any and all transactional information, to include log files, of all computer activity related to eBay's Affiliate Program, Commission Junction, ValueClick, or Shawn Hogan, or to the websites, www.shawnhogan.com, www.digitalpoint.com, the IP address range 216.9.35.48 through 216.9.35.63, and Digital Point Solutions, which includes dates, time, method of connecting, port, dial-up, and/or location;

f. All business records that pertain to eBay, the eBay Affiliate Program, Commission Junction, ValueClick, Digital Point Solutions, or Shawn Hogan, or to the websites, www.shawnhogan.com, www.digitalpoint.com, including but not limited to spreadsheets, applications, subscribers' full names, buddy lists, aliases, associated and alternate e-mail addresses, all screen names, method of payment, phone numbers, addresses, and detailed billing records;

g. All files, to include log files, scripts, source code, and tools, contained on the computer devices related to the company Digital Point Solutions and the websites www.shawnhogan.com and www.digitalpoint.com and/or the IP address range 216.9.35.48 through 216.9.35.63, and/or servers for Digital Point Solutions;

h. Indicia of residence and indicia of use of computers within the residence;

i. Documents, records, communications, scripts, source code, and/or files related to computer tools created, used, or distributed by Shawn Hogan, and/or Digital Point Solutions (e.g., "geovisitors," "website-country, "fmdigger," "zone-transfer," "keywords," "co-op ad" code, "network-ad") or any other tool that may contain 1x1 (or similar size) pixels;

j. Documents, records, communications, scripts, source codes and/or files related to forcing clicks, cloaking re-directs, cookie-stuffing, cookie-tracking, tracking tags and/or web beacons;

k. Documents, records, communications, and/or files related to tracking codes to track individual ad campaigns and/or advertising on various sites, to include spreadsheets and databases maintaining such information;

l. Documents and/or files related to Digital Point Solutions Forum, http://forums/digitalpoint.com, to include names of the members and/or owners, members of the Forum that may have downloaded free tools that contain the 1x1 (or similar size) pixel, conversations within the Forum involving forcing clicks, cloaking re-directs, cookie-stuffing, cookie-tracking, tracking tags, web beacons, or other techniques to defraud;

m. Records or communications between Hogan and others concerning the lawfulness or propriety of cookie-stuffing schemes, including records or communications between Hogan and others discussing the Terms and Conditions of eBay's Affiliate program;

n. Document and/or files regarding bank accounts and financial papers of Shawn Hogan and/or Digital Point Solutions, to include but not limited to all records of deposits from eBay, Commission Junction, and/or ValueClick.

o. Records regarding financial expenditures of monies paid to Hogan/Digital Point Solutions from eBay, Commission Junction, and/or Value Click, to include purchases or sales of assets such a vehicles, property, jewelry, computer equipment, or other assets related to Shawn Hogan and/or Digital Point Solutions since December 2003.

p. Records regarding any other websites affiliated with Shawn Hogan or Digital Point Solutions since December 2003;

q. Records or communications between Hogan and/or Digital Point Solutions and others discussing any contracts, requests for services, letters of engagement, investigative plans, or invoices related to services provided to or for eBay, and/or the eBay Affiliate Program and/or Commission Junction and/or ValueClick;

r. Records or communications between Hogan and/or Digital Point Solutions and others discussing the names and identities of all individuals and third parties who were used to procure, or to attempt to procure websites, advertisements, tools and scripts related to cookie stuffing related to eBay or any e-commerce company;

DEFINITIONS

a. The terms "records," "documents," "materials," "programs," "files," "logs," "scripts," "source code," "object code," "communications," "notes," or "applications" include all of the items in whatever form and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

1. Computer Hardware

Computer hardware consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. This includes any data-processing devices (such as central processing units, memory typewriters, self-contained "laptop" or "notebook" computers, Personal Digital Assistants (PDAs), or "Blackberries"); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, compact flash cards, smart media cards and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

2. Computer Software

Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way it works. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs, utilities, compilers, interpreters, and communications programs).

3. Computer-related Documentation

Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

4. Computer Passwords and Other Data Security Devices

Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

5. Computers

The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

COMPUTER SEARCH PROTOCOL

a. Agents executing this search warrant will employ the following procedures regarding computers that may be found on the premises which may contain information subject to seizure pursuant to this warrant:

Forensic Imaging

1. After securing the premises, the executing agents will consult with a computer specialist to determine the feasibility of obtaining forensic images of electronic storage devices while on-site. The feasibility decision will be based upon the number of devices, the nature of the devices and the volume of data to be imaged. The preference is to image on-site if it can be done in a reasonable amount of time and without jeopardizing the integrity of the data and the safety of the agents. The number and type of computers and other devices and the number, type, and size of hard drives are of critical importance. It can take several hours to image a single hard drive — the bigger the drive, the longer it takes. As additional devices and hard drives are added, the length of time that the agents must remain on-site can become overly intrusive, dangerous, and impractical.

2. If it is not feasible to image the data on-site, the computer equipment and any peripherals will be seized and transported off-site for imaging. Once a verified image has been obtained, the owner of the equipment will be notified and the equipment returned within thirty (30) days of seizure absent further application to this court.

3. A forensic image is an exact physical copy of the hard drive or other media. It is essential that a forensic image be obtained prior to conducting any search of the data for information subject to seizure pursuant to this warrant. A forensic image captures all of the data on the hard drive or other media without the data being viewed and without changing the data in any way. This is in sharp contrast to what transpires when a computer running the common Windows operating system is started, if only to peruse and copy data — data is irretrievably changed and lost. Here is why: When a Windows computer is started, the operating system proceeds to write hundreds of new files about its status and operating environment. These new files may be written to places on the hard drive that may contain deleted or other remnant data. That data, if overwritten, is lost permanently. In addition, every time a file is accessed, unless the access is done by trained professionals using special equipment, methods and software, the

operating system will re-write the metadata for that file. Metadata is information about a file that the computer uses to manage information. If an agent merely opens a file to look at it, Windows will overwrite the metadata which previously reflected the last time the file was accessed. The lost information may be critical.

4. Special software, methodology, and equipment is used to obtain forensic images. Among other things, forensic images normally are "hashed," that is, subjected to a mathematical algorithm to the granularity of 1038 power, an incredibly large number much more accurate than the best DNA testing available today. The resulting number, known as a "hash value" confirms that the forensic image is an exact copy of the original and also serves to protect the integrity of the image in perpetuity. Any change, no matter how small, to the forensic image will affect the hash value so that the image can no longer be verified as a true copy.

Forensic Analysis

5. After obtaining a forensic image, the data will be analyzed. Analysis of the data following the creation of the forensic image is a highly technical process that requires specific expertise, equipment and software. There are literally thousands of different hardware items and software programs that can be commercially purchased, installed and custom-configured on a user(s computer system. Computers are easily customized by their users. Even apparently identical computers in an office environment can be significantly different with respect to configuration, including permissions and access rights, passwords, data storage and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

6. Analyzing the contents of a computer, in addition to requiring special technical skills, equipment and software also can be very tedious. It can take days to properly search a single hard drive for specific data. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. As mentioned above, the computer may have stored information about the data at issue: who created it, when it was created, when was it last accessed, when was it last modified, when was it last printed and when it was deleted. Sometimes it is possible to recover an entire document that never was saved to the hard drive if the document was printed. Operation of the computer by non-forensic technicians effectively destroys this and other trace evidence. Moreover, certain file formats do not lend themselves to keyword searches. Keywords search text. Many common electronic mail, database and spreadsheet applications do not store data as searchable text. The data is saved in a proprietary non-text format. Microsoft Outlook data is an example of a commonly used program that stores data in a non-textual, proprietary manner; ordinary keyword searches will not reach this data. Documents printed by the computer, even if the document never was saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. Similarly, faxes sent to the computer are stored as

graphic images and not as text.

7. Analyzing data on-site has become increasingly impossible as the volume of data stored on a typical computer system has become mind-boggling. For example, a single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now capable of storing more than 100 gigabytes of data and are commonplace in new desktop computers. And, this data may be stored in a variety of formats or encrypted. The sheer volume of data also has extended the time that it takes to analyze data in a laboratory. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. Even perusing file structures can be laborious if the user is well-organized. Producing only a directory listing of a home computer can result in thousands of pages of printed material most of which likely will be of limited probative value.

8. Based on the foregoing, searching any computer or forensic image for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained; criminals can mislabel and hide files and directories, use codes to avoid using keywords, encrypt files, deliberately misspell certain words, delete files, and take other steps to defeat law enforcement. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear necessary to locate and retrieve digital evidence within the scope of this warrant.

9. All forensic analysis of the imaged data will be directed exclusively to the identification and seizure of information within the scope of this warrant.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Todd Walbridge, Special Agent of the Federal Bureau of Investigation (FBI), being duly sworn, hereby declare as follows:

OVERVIEW AND AGENT BACKGROUND

1. I am an "investigative or law enforcement officer of the United States," within the meaning of Section 2510(7) of Title 18, United States Code, that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516, Title 18, United States Code.

2. I am employed as a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so for over three and a half years. I am currently assigned to the San Diego Division. Since that time, I have received training in general law enforcement and in cyber investigations including crimes committed utilizing computers and computer networks, such as hacking, denial of service attacks, and malicious code. I have experience in investigations concerning white collar crime matters within the Criminal Division of the FBI. I have participated in criminal investigations involving hacking, bank fraud, investment fraud, bank robberies, fugitives, and kidnappings. Prior to my employment as a Special Agent, I was employed in the computer technology field for over eight years.

3. As part of an ongoing FBI investigation, I make this affidavit in support of an application by the United States of America for a warrant to search for evidence, fruits, and instrumentalities of criminal activity located at the following locations:

a. the residence of Shawn Dean Hogan (hereafter "Hogan") and the business address of Digital Point Solutions at 8465 Regents Road, Apartment #448, San Diego, California, 92122 ("the SUBJECT PREMISES 1");

b. the residence of Brian Andrew Dunning (hereafter "Dunning") and the business address of Kessler's Flying Circus and Thunderwood Holdings located at 15 High Bluff, Laguna Niguel, California, 92677 ("the SUBJECT PREMISES 2");

c. the location of the servers for web hosting services utilized by Dunning at Rackspace.com, d/b/a Rackspace Managed Hosting, which is located at 9725 Datapoint Drive, Suite 100, San Antonio, Texas, 78229 ("the SUBJECT

PREMISES 3").

Each of the SUBJECT PREMISES is described in the applicable Attachment A. As set forth herein, probable cause exists to believe that the items described in the applicable Attachment B, which items constitute evidence, fruits, and/or instrumentalities of the violations of Title 18, United States Code, Section 1343 (wire fraud) are present at the applicable SUBJECT PREMISES. In sum, it is alleged that Hogan and Dunning used an executable script[1/] within a1x1 pixel[2/] to "cookie stuff"[3/] in order to fraudulently obtain payments from eBay through eBay's

Affiliate program.

4. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained during my participation in this investigation; knowledge obtained from other FBI agents and individuals; oral and written communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

[1/] Script is another term for a macro or batch file, a script is a list of commands that can be executed without user interaction. A script language is a simple programming language with which you can write scripts.

[2/] A 1x1 pixel is often a transparent graphic image (also known as a "web beacon," "web bug," or "pixel tag") used in combination with a cookie that is placed on a website or in an e-mail that is used to monitor the behavior of the user visiting the website or sending the e-mail. When the HTML code for the web beacon points to a site to retrieve the image, it can at the same time pass along information such as the Internet Protocol address of the computer that retrieved the image, the time the web beacon was viewed and for how long, and the type of browser that retrieved the image.

[3/] "Cookie stuffing" can be defined as setting a cookie on a user's computer without a real "click" by that user.

SUBJECT PREMISES

5. The SUBJECT PREMISES 1 is located at 8465 Regents Road, Apartment #448, San Diego, California, 94122 and is described as an apartment located inside the Regents Court Apartment Complex. The complex is a stucco, four-story structure. Apartment #448 is located in the northeast corner of the complex on the fourth (top) floor. The numbers "448" are visible next to the entrance to the residence, which is a brown door.

6. The SUBJECT PREMISES 2 is located at 15 High Bluff, Laguna Niguel, California, 92677. The SUBJECT PREMISES 2 is described as a single family residence with a light brown tile roof. The residence has light brown stucco with light brown wood trim. In front of the residence is a three car garage with brick pillars on either side. On the brick pillar on the right side is the number "15."

7. The SUBJECT PREMISES 3 is the location of servers utilized by Brian Dunning at web hosting service provider, Rackspace.com, d/b/a Rackspace Managed Hosting, located at 9725 Datapoint Drive, Suite 100, San Antonio, Texas, 78229 described as the servers hosting www.briandunning.com, www.thunderwood.com, www.wholinked.com, profilemaps.info and/or IP addresses 72.32.11.26 and 72.32.102.215 or any account in the name of Brian Dunning and/or Kessler's Flying Circus.

8. Each of the SUBJECT PREMISES is described in the applicable Attachment A.

APPLICABLE STATUTE

9. Title 18, United States Code, Section 1343 states:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this

title or imprisoned not more than 20 years, or both.

BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND E-MAIL

10. The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

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

a. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information;

b. Internet Service Providers ("ISPs"): Most individuals and businesses obtain access to the Internet through businesses known as Internet Service Providers ("ISPs").

c. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods;

d. Internet Protocol Address ("IP address"): An Internet Protocol address is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots (e.g., 149.101.10.40). Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. Internet service providers ("ISPs") assign IP addresses to their customers' computers. An ISP might assign a different IP address to a customer each time the customer makes an Internet connection (so-called "dynamic IP addressing"), or it might assign an IP address to a customer permanently or for a fixed period of time (so-called "static IP addressing"). The IP address used by a computer attached to the Internet is unique for the duration of a particular session; that is, from connection to disconnection. ISP's typically log their customers' connections, which means that the ISP can identify which of their customers was assigned a specific IP address during a particular session.

e. A co-location facility is a company, usually a web service company, which offers a customer a secure place to physically house their hardware and equipment as opposed to locating it in their offices or warehouses where the potential for fire, theft, or vandalism is much greater. These facilities usually provide secured cage or cabinet, regulated power, dedicated Internet connection and security.

f. A web hosting service provider is in the business of providing server space, web services, and file maintenance for websites controlled by individuals or companies that do not have their own web servers. Many ISPs, such as America Online, will allow subscribers a small amount of server space to host a personal web page. Other commercial ISPs will charge the user a fee depending on the complexity of the site being hosted.

g. E-mail is a popular form of transmitting messages and/or files in an electronic environment between computer users. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may allow users to post and read messages and to communicate via electronic means. When an individual computer user sends e-mail, it is initiated at the user's computer, transmitted to the subscriber's mail server, then transmitted to its final destination;

h. Any e-mail that is sent to a subscriber is stored in the subscriber's "mail box" on the provider's servers until the subscriber deletes the e-mail or the subscriber's mailbox exceeds the storage limits preset by the e-mail provider. If the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on the provider's servers indefinitely;

i. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to the servers of the e-mail provider, and then transmitted to its end destination. Users have the option of saving a copy of the e-mail sent. Unless the user specifically deletes the e-mail from the e-mail account, the e-mail can remain on the system indefinitely. The sender can delete the stored e-mail message thereby eliminating it from the e-mail box maintained at the e-mail provider, but that message will remain in the recipient's e-mail box unless the recipient deletes it as well or unless the recipient's account is subject to account size limitations;

j. A subscriber can store files, including e-mails and image files, on servers maintained and/or owned by the e-mail provider; and e-mails and image files stored on a e-mail provider server by a subscriber may not necessarily be located in the subscriber's home computer. The subscriber may store e-mails and/or other files on the provider's server for which there is insufficient storage space in the subscriber's computer and/or which he/she does not wish to maintain in the computer in his/her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the e-mail provider's server.

k. Data that is processed by a computer may be written to the computer's internal hard drive or other storage medium even if the user does not intentionally save the information. Other storage medium may include compact discs ("CDs"), digital video disks ("DVDs"), floppy diskettes, thumb drives, pocket hard drives, external hard drives and flash drives. For example, a computer operating system may take random data out of working memory and use it to "pad" files on a computer hard drive during the storage process.

l. Electronic information can remain on computer storage media, such as internal and external hard drives, pocket drives, thumb drives, CDs, DVDs, diskettes, and flash drives, for an indefinite period of time. Even when a computer user attempts to delete records from a computer storage medium, the records may still exist and be recovered through computer forensic techniques

m. Computer files may be easily moved from computer to computer, using direct wire connections or through the use of storage media such as floppy diskettes, CDs, DVDs, diskettes, thumb drives, pocket drives, flash drives and USB drives.

n. A server is a centralized computer that provides services for other computers connected to it via a network. The other computers attached to the server are sometimes called "clients." Notably, server computers can be physically stored in any location: it is common for a network's server to be located hundreds (even thousands) of miles away from the client computers.

o. A domain is a group of Internet devices that are owned or operated by a specific individual, group, or organization. Devices within a domain are assigned IP addresses within a certain range of numbers, and are usually administered according to the same set of rules and procedures.

p. A domain name identifies a computer or group of computers on the Internet, and corresponds to one or more IP addresses within a particular range. Domain names are typically strings of alphanumeric characters, with each "level" of the domain delimited by a period, (e.g., Computer.networklevel11.network12.com). A domain name can provide information about the organization, ISP, and physical location of a particular network user.

SUMMARY

12. In June 2007, the FBI in San Jose, California, initiated an investigation into an alleged Internet fraud scheme being perpetrated by Shawn Dean Hogan, of Digital Point Solutions, and Brian Dunning, of Kessler's Flying Circus, against eBay through eBay's Affiliate program. EBay is the world's largest online marketplace enabling trade on a local, national, and international basis. EBay personnel informed agents of the FBI that, in order to "drive" people to its website, eBay developed an Affiliate program. According to eBay personnel, the Affiliate program is a key marketing enabler, whereby eBay works with third-party marketers to drive Internet traffic to eBay and then be compensated by eBay. The affiliate sends visitors to eBay.com (or any international site of eBay) from a website associated with the affiliate, and does so (in theory) by suggesting (in some way) that the visitor "click" on a link to eBay's website. If these visitors thereafter become new active users on eBay by setting up an account or make a purchase on eBay (within specified time periods), the affiliate will be compensated. The compensation is a tiered payment structure that rewards increased performance. In other words, the more traffic driven by the affiliate to eBay, the more money the affiliate will earn for each transaction or new active user. Compensation is based on the number of new account users or the percentage of the revenue from sales. For instance, if one to forty-nine of the people the affiliate caused to visit eBay became new users, the affiliate would receive $25.00 per new user. Likewise, if the visitors the affiliate caused to visit eBay won a bid for an item costing between $0 and $99.99, the affiliate

would receive 50% of the revenue earned by eBay on that transaction. There is an automated tracking infrastructure to confirm that an affiliate who directed a user to eBay and the user returns within a certain time period and wins a bid or makes a purchase will receive compensation.

13. EBay personnel told FBI agents that in order to track this process, when a visitor is referred ro eBay from an affiliate site, eBay "drops" a "cookie" on the visitor's computer so that if the visitor signs up as a new eBay user within 30 days of being directed to eBay by the affiliate, or if the visitor makes a purchase within approximately 7 days of being directed to eBay by the affiliate, the affiliate will receive credit and compensation from eBay under the Affiliate program.

14. Based on my training and experience, I know that a "cookie" is a file that is generated by a website when a user on a remote computer accesses it. The cookie is sent to the user's computer and is placed (or "dropped") on that user's computer, usually in files/folders labeled "Internet" or "Temporary Internet Files." The cookie includes information such as user preferences, connection information such as time and date of use, records of user activity including files accessed or services used, or account information. The cookie is then accessed by the website on subsequent visits to that website by the user in order to better serve the user's particular needs and preferences.

15. According to eBay, the way the cookie works in the eBay Affiliate situation is that the cookie dropped by eBay contains a Publisher Website ID ("PID"), which identifies the Affiliate member that directed the particular user to the eBay site. Therefore, if and when that particular user comes back to eBay in the future, this cookie will be accessed by eBay's system. If that user signs up as a new eBay member within 30 days of the user's initial visit to eBay, or if this user buys on eBay during the user's initial access to the eBay site or during subsequent accesses during a specified period (approximately 7 days), the cookie that is accessed by eBay at that time contains the identifying information (i.e., the PID) of the Affiliate that originally directed the user to eBay. EBay's automated tracking process does the analysis to validate that the originally set cookie and the event cookie (i.e., the cookie that memorializes the registration or purchase event) contain the same PID. This ensures that the affiliate receives the credit and appropriate compensation from eBay through the Affiliate program.

16. EBay advised that, in 2006, it had a total of 32,867 members in the Affiliate

program. However, only an average of 5,263 of those members produced at least one transaction in 2006. There were 26,266 members in the eBay Affiliate program from January 2007 until June 8, 2007. Approximately 6,083 of those members produced at least one transaction to date in 2007. In 2006, the eBay Affiliate program paid out $70,779,455 in compensation to affiliate members. Digital Point Solutions (which is owned by Shawn Hogan) received $10,489,467 in compensation from the eBay affiliate program in 2006. This was approximately 15% of eBay's total payout. Kessler's Flying Circus (which is owned by Brian Dunning) received $2,696,438 in compensation from eBay's Affiliate program in 2006. From January to April 2007, the eBay Affiliate program paid out $28,440,456 in compensation to affiliate members. During that same time period, Digital Point Solutions earned $4,183,695 in eBay affiliate program compensation; Kessler's Flying Circus earned $2,164,355 in compensation through the program. The top ten affiliates' (not including DPS and Kessler's) average total payout was approximately $3,386,904 per year. Digital Point Solutions owned by Shawn Hogan is the number-one producing eBay Affiliate account in the Affiliate Program, and Brian Dunning's Kessler's Flying Circus eBay Affiliate account is the number-two producing account in the program.

17. EBay personnel also informed agent of the FBI that, in order to be a member of the eBay Affiliate program, a user signs up through an eBay third party vendor named Commission Junction ("CJ") to obtain an eBay affiliate account. CJ's parent company is ValueClick, Inc. EBay uses CJ to register affiliates, assist them with their accounts, and monitor their activity to ensure quality control and compliance with the rules and regulations governing the program. Specifically, the eBay Affiliate Global Program Terms and Conditions states in regard to "tracking tags" that the affiliate user will not deliver any eBay-related cookies or other tracking tags to the computers of the affiliate's user that are merely viewing the affiliate user's advertisements or while the Affiliate user's applications are merely active or open.

18. Further, the eBay Affiliate Global Program Terms and Conditions list the following as a prohibited operation: sending unsolicited information or material to another computer, and/or diverting the user to another site not requested by the user.

19. Accordingly, the Terms and Conditions of eBay's Affiliate program prohibit

affiliates from dropping eBay-related cookies on users' computers if those users do not actually "click through" and connect with eBay's website.

20. During the course of its investigation, the FBI also obtained CJ documentation from eBay that indicates CJ also requires its clients to accept the terms of its Publisher or Advertisers Service Agreements (PSA or ASA respectively) before they join. The PSA informs publishers that certain behavior is not acceptable and is grounds for removal from the network, (i.e., generating unwarranted clicks manually or through technology, using undisclosed or inaccurately disclosed software). In CJ's Overview of Network Quality, CJ prohibits "forced clicks" or "cookie stuffing" and defines it as follows: Publisher places a referral cookie without the end user taking an affirmative action (clicking on the link or offer). Multiple forced clicks performed on a single session over a short period of time is referred to as cookie stuffing. Under CJ's agreements, both DPS and Kessler's are "publishers."

FACTS SUPPORTING PROBABLE CAUSE

Digital Point Solutions and Shawn Dean Hogan

21. Records provided by eBay indicate that Digital Point Solutions ("DPS") joined as an eBay affiliate on December 10, 2003 through eBay's third party Affiliate partner Commission Junction ("CJ"). According to eBay, the DPS affiliate account is the number-one ranked account for performance in the eBay Affiliate program, representing an average of 15% of the eBay U.S. total payment for the Affiliate program in 2006. From January through April 2007, DPS represents an average of 15% of the eBay U.S. total payment for the Affiliate program.

22. Public records from Dun & Bradstreet indicate that DPS began in 1993 and that the owner of the company is Shawn Hogan. DPS is located at 8465 Regents Road, Apartment 448, San Diego, California, 94122, (SUBJECT PREMISES 1) telephone 858-452-3696, website www.digitalpoint.com, DUNS number 94-701-0831 and is in the computer software line of business. DPS recently filed for incorporation in California and was incorporated on May 14, 2007 with registration ID# C2998539.

23. According to California Employment Development Department, there is no record

of employment for Shawn Dean Hogan, born September 1, 1975 with the social security account number assigned to Hogan.

24. FBI San Francisco obtained a California Department of Motor Vehicle Driver's License photograph for Shawn Dean Hogan with a listed address of 8465 Regents Road, Apartment 448, San Diego, California, 94122 (SUBJECT PREMISES 1). Records provided by eBay indicate the home address for eBay affiliate Shawn Hogan is 8465 Regents Road, Apartment 448, San Diego, California, 94122.

25. Records from T-mobile indicate that Shawn Hogan is the subscriber of cellular telephone 619-723-1589 with a billing address of 8465 Regents Road, Apartment 448, San Diego, California., 92122, home telephone 858-452-3696. Hogan, born September 1, 1975 established this account in December 2006.

26. In June 2006, FBI San Francisco Special Agents interviewed Christine Kim ("Kim"), former employee of CJ and current employee of eBay involved in the Affiliate program. Kim worked at CJ from late 2003 to mid-October 2005. She began as an account representative for the eBay accounts and then became a Program Manager for the eBay Affiliate accounts managed by CJ. Kim managed the top 5 to 10 accounts, which included the accounts for Hogan and Dunning. She indicated that she knows Hogan personally and professionally, and she indicated that he is extremely knowledgeable about computers and computer programming and was involved in developing software. Kim advised agents that Hogan owns and operates his own companies by himself. In the past, Hogan owned and operated a company known as Opti Gold, which Kim believed was involved in database software and software licensing. Kim also stated that Hogan owns a company named Digital Point Solutions, which he operates from his apartment located at 8465 Regents Road, San Diego, California (SUBJECT PREMISES 1). She believed Hogan started DPS five or ten years ago. Kim told FBI agents that Hogan has an Apple MAC Desktop 64, at least two Windows PC desktops that he uses for testing applications related to his businesses, an Apple MAC Power book laptop, a Blackberry Pearl, an XBox, and a webcam at his apartment. Kim also believed that Hogan has a T1 telephone line running into his apartment.

27. Kim advised she is also aware that Hogan houses his servers for DPS at a co-location facility. She is aware that about one year ago, Hogan purchased ten new "blade" servers from Dell Computer for approximately $30,000. Kim is not sure what he did with his already existing Apple servers that she had been told by Hogan were in the co-location facility, i.e., whether he replaced those with the new servers or added the new servers to the existing servers. She believed that Hogan configured the new Dell blade servers at home and was not sure if one server may still be located at the residence. Kim stated that she had been in Hogan's apartment in November 2006 and was positive that Hogan worked from home and most likely remotely accessed his servers from that location. She believed that he had the technical skills to install a quick erase or exit button or reformat of his servers if he believed it was needed for immediate response. She thought he might even be able to do this from his Blackberry phone.

28. Kim indicated that Hogan was considered notorious in the programming world. At one time, she had heard a rumor that he had pirated software applications with a fake "key." She indicated Hogan began a co-operative ad network, but in order to sign up the user had to copy and paste Hogan's codes unto the user's website.

29. Kim advised Hogan created a Digital Point Forum on his website, www.digitalpoint.com which became a best-practices-sharing forum for ad marketing and other tools. For instance, about a year ago, Hogan wrote a tool called "geovisitors" that enables the user of the tool to see where all the visitors to a website are from geographically on a map. Kim believed Hogan did this by using an image tag. Hogan had told Kim that the first time a visitor clicked on his "geovisitors" tool the visitor would see an eBay advertisement and apparently visitors complained about it. Hogan also told Kim that he had designed self-optimizing algorithms so that when a visitor clicked on a link, he could obtain demographics to tailor his ad links. Kim advised that Hogan has developed an extremely powerful ad network, which is a massive network of advertisers that provide linkage to other members and websites.

30. Based on investigation by the FBI, there are other tools that are available for download from www.digitalpoint.com (e.g., website-country, fmdigger, zone-transfer, keywords, ad

network, and coop ads/dp coop) which may also be perpetuating this cookie stuffing scheme. From May 29, 2007 through June 4, 2007, there was a discussion thread on forums.digitalpoint.com in which a participant in the thread was inquiring as to whether ad network and/or coop ads was forcing clicks and dropping cookies with publisher information for Digital Point Solutions on visitors' machines. Another participant responded, "Shawn is getting plenty of eBay affiliate revenue if this is true."

31. Kim told agents that Hogan knows Dunning and had told her that Dunning stole his tool "geovisitors." Kim indicated that Dunning had developed a tool named "profilemaps" that Dunning developed for use on www.myspace.com. Kim indicated that an eBay logo appears with a button on the "profilemaps" tool, Hogan told her that this tool Dunning created was like his "geovisitors" tool.

Location of Hogan's Servers

32. Through public source tracking using Network Solutions, agents were able to resolve the domain name www.digitalpoint.com and a home website www.shawnhogan.com to the Internet Protocol (IP) address range 216.9.35.48 through 216.9.35.63. through public source information, these IP addresses were traced to NetHere, Inc. which is a co-location facility and web hosting service provider located at 4134 Voltaire Street, San Diego, California, 92107. NetHere, Inc. provides web-hosting, E-Commerce, Internet Access, Network services and co-location facilities.

Report Regarding Suspicious Cookie Activity by DPS in 2004/2005

33. Kim advised that while she was employed by CJ, sometime between late 2004 and early 2005, she received information about possible fraudulent activity on Hogan's DPS eBay affiliate account from Ben Kopetti who was the compliance manager for CJ. Kim indicated that Kopetti had received information regarding this activity from an outside contractor, Ben Edelman. Edelman performed quality control for eBay and eBay's Affiliate program through CJ by providing monthly reports of possible fraudulent activity. Edelman reported that Hogan's DPS eBay affiliate account had cookie-like behavior. Because Kim was Hogan's/DPS's account manager at CJ, Kopetti provided Kim the details and a copy of Edelman's report. Kim decided to talk directly to Hogan about the matter, since Hogan would contact her a few times a week and explain what he was doing with his advertisements and

how he was attracting traffic. When Kim approached Hogan about the matter, he explained that it was just a small scripting error and that he would fix it immediately. Kim advised that Hogan was apologetic and was quick in resolving the issues. Nothing further was reported to Kim regarding this matter, and she believed that Hogan must have fixed the errors.

34. It should be noted that eBay personnel advised FBI agents Ben Edelman is an outside contractor for eBay who provides monthly reports regarding the activities of eBay affiliates to the person running quality control for the eBay Affiliate program. This monthly report is then forwarded by eBay to the CJ compliance person. The purpose is to have CJ duplicate Edelman's efforts and provide warnings, sanctions, and/or suspensions to the eBay affiliates participating in any fraudulent activity. In looking for fraud, Edelman casts his net very wide, and Edelman's reports contain descriptions of some activities by eBay affiliates that can be described as "gray" (i.e., not clearly "black" or "white") and that eBay might not consider a violation per se of the Affiliate program terms and conditions (e.g., cloaking redirects).[4]

Report of Possible DPS Fraudulent Activity in January 2006

35. According to Kim (who was given this information by Dan Burkhart, the head of eBay's Affiliate program, when Kim was supervised by Burkhart), in January 2006, Burkhart received a telephone message from a person later identified as Todd Dunning who indicated that he knew of a

[4] Cloaking is a technique used by some web sites to deliver one page to a search engine for indexing while serving an entirely different page to everyone else. There are opposing views as to whether or not cloaking is ethical. Opponents see it as a bait-and-switch, where a Web server is scripted to look out for search engines that are "spidering" in order to create an index of results. The search engine thinks it is selecting a prime match to its requests based on the meta tags that the site administrator has input. However, the search results is misleading because the meta tags do not correspond to what actually is on the page. Some search engines, such as Lycos, Hotbot, and Excite, even ban cloaked Web Sites. Proponents of cloaking assert cloaking is necessary in order to protect the meta data, as only the spider is supplied with the meta tags.

person who was blatantly cheating on the eBay Affiliate program and bragging to Todd Dunning's brother (Brian Dunning) about all of the money he was making by placing a 1x1 pixel and forcing an eBay cookie with his affiliate information. Burkhart then contacted Todd Dunning, who told him that the person committing the fraud was Shawn Hogan who owns Digital Point Solutions. According to Todd Dunning, Hogan was using a 1x1 pixel to force a cookie to be placed with his affiliate information, even though the user did not click to redirect to the eBay site.

36. After receiving this telephone call, eBay personnel asked eBaty's outside contractor, Ben Edelman, to check out Hogan's DPS affiliate traffic. Edelman did not find anything at that time, but he did recall reporting an activity similar to what was described in a prior report months before, and he felt it would be very difficult to detect again. Kim, who was then working for eBay with the Affiliate program, talked with Edelman about the prior incident from late 2004/early 2005 and the telephone call from Todd Dunning in January 2006. Kim advised FBI agents that Edelman told her that he did not think that the activity he discovered regarding Hogan when he wrote the initial report would have been a scripting error. However, since Edelman could not find anything suspicious regarding Hogan's traffic after eBay received the telephone call from Todd Dunning, eBay determined that Todd Dunning's complaint was most likely the result of competitive fighting between Todd and/or Brian Dunning and Hogan, who were believed to know each other.

Report Regarding Possible DPS Fraudulent Activity in May 2007

37. In May 2007, Compliance Specialist David Lam of CJ's United Kingdom office notified Kim with the eBay Affiliate program and Jennifer Burnett, Program Quality Manager, CJ United States, that the eBay affiliate Digital Point Solutions ("DPS") was forcing clicks[5] by users and therefore cookie stuffing[6] in order to fraudulently obtain commissions and compensation from eBay. This time,

[5] Commission Junction's Overview of Network Quality defines a "forced click" as the placement of a referral cookie without the end user taking an affirmative action (clicking on the link or offer).

[6] Commission Junction's Overview of Network Quality defines "cookie stuffing" as multiple (continued...)

after some investigation, eBay technical staff were able to duplicate the cookie-stuffing process from the screen shots provided by CJ United Kingdom of Hogan's DPS account provided by CJ. The eBay technical staff also initiated an investigation into Dunning's activities as result of being able to validate the fraud from Hogan's account and were able to validate similar cookie-stuffing behavior from Dunning's Kessler's Flying Circus account. A description of the steps taken by eBay in investigating this fraudulent activity is set out in the sections titled, "Technical Analysis of the Fraudulent Activity" and "Installation of a Trip-Wire" below.

Kessler's Flying Circus and Brian Dunning

38. According to information provided to the FBI by eBay personnel, Brian Dunning joined as an eBay affiliate on November 11, 2004 through CJ using www.briandunning.com. EBay indicated that this affiliate account used by Dunning was a lower-tiered account that eBay does not believe was involved in this fraudulent activity involving cookie-stuffing utilizing a 1x1 pixel to force access to eBay's homepage without the user's knowledge. EBay indicated that while this account does not appear to be involved in the current scheme involving the 1x1 pixel, the account has certainly had other suspicious activity flagged.

39. EBay personnel also advised FBI agent that Dunning later set up an eBay affiliate account through CJ under the name Kessler's Flying Circus ("Kessler's") on April 22, 2005, which became the second-ranked account for performance in the eBay Affiliate program. Kessler's compensation in the eBay Affiliate program represented 3% of the total U.S. payment for the Affiliate program in 2006. From January to April 2007, Kessler's compensation in the program represented 7% of the eBay total U.S. payment.

40. Public records indicate that Brian Dunning may be operating under the possible fictitious business name Kesslers Flying Circus, located at 15 High Bluff, Laguna Niguel, California, 92677 (SUBJECT PREMISES 2). The file date was April 15, 2005, file number 20056025410 in the

[6](...continued)
forced clicks performed on a single session over a short period of time.

State of California, and the owner is listed as Brian Dunning at 15 High Bluff, Laguna Niguel, California, 92677.

41. Records from the California Employment Development Department indicate that Brian A. Dunning, born December 29, 1965, with a social security account number assigned to Dunning, was employed by Thunderwood Holdings, Inc., located at 20 Cresta Blanca, Orinda, California, 84563, telephone 925-368-7441 in the first through the fourth quarters of 2006 and in the first quarter of 2007. According to public source records, Thunderwood Holdings, Inc. was incorporated in the State of California on December 9, 2002 and the status is active. The registered agent is Brian Andrew Dunning at 15 High Bluff, Laguna Niguel, California, 92677. Brian Andrew Dunning is also listed as the President located at the same address (SUBJECT PREMISES 2).

42. FBI San Francisco obtained a California Department of Motor Vehicle Driver's License photograph of Brian Andrew Dunning with a listed address of 15 High Bluff, Laguna Niguel, California, 92677. Records provided by eBay indicate the home address for eBay affiliate Brian Dunning is 15 High Bluff, Laguna Niguel, California, 92677 (SUBJECT PREMISES 2).

43. Kim also knows Dunning from her employment at CJ. She managed Dunning's eBay affiliate account while at CJ. She is aware that Dunning has worked on software development and is also fairly knowledgeable in regard to computer programming, although he is not as technical as Hogan. Kim told FBI agents that Dunning works from home. Kim had heard the Dunning has his sister helping him detect and remove pornography from his sites and may have another engineer helping him with enhancements to www.wholinked.com. Kim indicated that Hogan and Dunning knew each other and Hogan gave Dunning ideas. She believes it is possible that Hogan would have told Dunning about Hogan's use of the cookie-stuffing scheme using the 1x1 pixel.

44. Kim recalled that, while she was employed by CJ and managing Dunning's affiliate account, the account had some strange behavior similar to a mouse-movement-induced redirect to eBay. Kim indicated after she asked Dunning about this activity, the activity stopped. She indicated that Dunning resided in Laguna Niguel, California and possibly in Alieso Viejo, California before that. Kim also advised Dunning had created a widget called "wholinked.com," which he posted for use on

blogs that was designed to provide the user a list of sites linked to your site. In addition, Kim indicated Dunning also created a tool called "profilemaps" that maps everyone who visits your profile on www.myspace.com. This tool can be obtained at the domain profilemaps.info.

Location of Dunning's Servers

45. Through public source tracking using Network Solutions, agents were able to resolve the domain name for www.briandunning.com, www.thunderwood.com, www.wholinked.com and profilemaps.info to a web hosting service provider named www.rackspace.com located at 9725 Datapoint Drive, Suite 100, San Antonio, Texas, 78229 (SUBJECT PREMISES 3). A web hosting service provider is in the business of providing server space, web services, and file maintenance for websites controlled by individuals or companies that do not have their own web servers. Many ISPs, such as America Online, will allow subscribers a small amount of server space to host a personal web page. Other commercial ISPs will charge the user a fee depending on the complexity of the site being hosted. Additionally, the IP addresses associated with these domains are 72.32.11.26 and 72.32.102.215, which are also, according to ARIN[4], resolved to www.rackspace.com.

46. Based on my experience and training, I know that individuals conducting illegal and fraudulent activities can use web hosting services in order to distance themselves from the criminal activity. Web hosting service providers may have many servers located in several areas not physically near the user accessing these services, which may make it more difficult for law enforcement to find where the computer files and evidence of crime are stored. In this case, Dunning resides in Laguna Niguel, California, and it appears that the web hosting services he is using to host his websites www.briandunning.com, www.wholinked.com, and profilemaps.info are provided by a company located in San Antonio, Texas.

47. Further, I know that individuals and/or companies that utilize web hosting and co-location facilities typically access these facilities remotely to work from their offices or a home office

[4] ARIN is the American Registry for Internet Numbers. ARIN is a non-profit corporation that allocates Internet Protocol resources in the United States and Canada.

if they live in a different location than the server facility. In this manner, computer files, records and other evidence of crimes committed through computer servers may be located on the servers of the web-hosting company or in the co-location facility, or on the computers in the office or home office of the person remotely accessing these servers.

48. AT&T records indicate that Dunning has an active account with DSL Internet service using a dynamic IP address. This account is billed to him at 15 High Bluff, Laguna Niguel, California, 92677 which began in March 2003. Based on my training and experience, I know that the Internet can be used to connect to web hosting service providers who are physically located in a different city than the city where the user resides and/or works.

Possible Cookie Stuffing/Forced Clicks by Affiliates Associated with Dunning

49. In Edelman's monthly report dated February 5 to February 27, 2007, indicated activity of cookie stuffing by www.wholinked.com. This report indicated the affiliate at www.wholinked.com was using JavaScript embedded in third parties' sites to force clicks on eBay affiliate links in 1x1 pixel images. In this report, Edelman indicated that, in investigating the matter, he had loaded www.dnainvestments.com on a clean computer. In his report, Edelman indicated he was surprised to see that it dropped an eBay cookie without his clicking on any link to eBay. Edelman's reports further stated that packet log analysis showed that traffic flowed as follows: From www.dnainvestments.com to www.passportinvestor.com which embedded a JavaScript called "wholinked.com/wordpress.js," which set out a 1x1 pixel image tag that redirected to a CJ affiliate link (PID 1740639). Edelman also stated in this report that this PID is one he reported in August 2006 for a web of web spam sites that also perform cookie stuffing. PID 1740639 belongs to Dunning's Kessler's account.

50. In his August 2006 report, Edelman described conducting a general cookie-stuffing test. Edelman searched "eBay registration" at MSN. He found that result number 14 was www.hacth2008.org/ebay/ebay_registration.php. Upon clicking through to this page, Edelman was immediately taken directly to the eBay website via an affiliate link: www.qksrv.net/click-1673599. Edelman indicated this is standard cookie stuffing by invoking an affiliate link and setting affiliate

pixel with the file extension "GIF"[5] then loads onto that user's computer. The pixel file goes through a "gating" function in which a computer script checks for various conditions before it executes. For instance, eBay has determined that the gating function determines the IP address of the user. If the IP address is one that is associated with eBay or CJ, then nothing occurs and the process ends. Similarly, eBay has determined that there is a frequency cap that prevents execution if the user has been to the site before. If these criteria are successfully met (i.e., the user's IP address is not associated with either eBay or CJ and the user has not been to the site before), then the pixel executes and calls the Affiliate's server (e.g., www.digitalpoint.com). A redirect to the Affiliate server is then initiated. Another redirect occurs to http://rover.eBay.com to pull an eBay homepage in text thereby simulating a click redirect (but the eBay home page does not load on the user's computer). Then a server at www.eBay.com sends the cookie with the Affiliate's PID to the user's computer even though the user never clicked to be redirected to www.eBay.com nor ever left the original website associated with the affiliate. Now, this user has a cookie from eBay set on the user's computer that contains the affiliate PID of DPS. If this user thereafter goes to www.eBay.com (either directly or from another eBay affiliate's site) and sets up a user account or makes a purchase within a specified time period, DPS will be compensated by eBay. DPS would have obtained this compensation fraudulently because placing cookies on user's computers in this fashion violates the terms and conditions of the Affiliate program because the user never actually "clicked through" to eBay at the time that DPS caused the initial cookie to be placed on that user's computer.

54. According to eBay personnel, the technical team at eBay determined that this 1x1 pixel is placed on sites linked to Hogan's Digital Point Solutions ad-network. The eBay technical team, based on their analysis, believe that any site that downloaded any of Hogan's free tools from his website www.digitalpoint.com will have the 1x1 pixel on that website. Hogan's free tools include geovisitors, ad-network and others. It appears as though the 1x1 pixel GIF file has a different name for each website

[5] Gif stands for graphics interchange format which is a bit-mapped graphics file format used by the World Wide Web, Compuserve and many Bulletin Board Systems.

but that each GIF calls to Hogan's servers at http://www.digitalpoint.com, to include but not limited to http://ads.digitalpoint.com or http://forums.digitalpoint.com each time the GIF passes the gating function and executes. Based of their technical analysis, the eBay technical team has told FBI agents that they believe the GIF which is executing and redirecting to Hogan's company website www.digitalpoint.com pulls up a "script" that causes the cookie-stuffing.

55. As mentioned previously, the company Digital Point Solutions is assigned a range of IP addresses 216.9.35.48 through 216.9.35.63. The website www.shawnhogan.com points to a URL with an IP address within the range of IP addresses assigned to Digital Point Solutions. The website www.digitalpoint.com also points to a URL that resolves within the range of IP addresses assigned to Digital Point Solutions. According to the eBay technical team every time the 1x1 pixel executes, a redirect occurs to some part/section of www.digitalpoint.com, (i.e., http://forums.digitalpoint.com, http://ads.digitalpoint.com, http://geo.digitalpoint.com, http://www.digitalpoint.com/tools/geovisitors). In my training and experience, websites can reference and refer to other URLs which could correspond to other IP addresses (e.g., another IP address within the range of IP addresses assigned to the company).

56. After duplicating the cookie stuffing being done by Hogan's DPS account, the eBay technical team also initiated an investigation into Dunning's Kessler's affiliate account and proved similar cookie-stuffing activity. In summary, eBay determined that a user who downloads Dunning's tool has a similar cookie placed on the user's computer, even though the user never actually "clicked through" or viewed eBay's website. This cookie setting by Dunning's tool created the same result for Kessler's affiliate account as the cookie setting performed by Hogan's DPS affiliate account. The eBay technical team determined that the cookie-stuffing activity stems from a tool named profilemaps.info. This tool calls forth a 1x1 pixel which ends in the extension "GIF." Similarly to the DPS activity, this GIF loads and redirects to eBay where a cookie is then dropped with Dunning's Kessler's affiliate PID. The eBay technical team told FBI agents that profilemaps.info will force a stuffed cookie to be loaded if the user downloads the actual tool or if the user accesses a myspace homepage in which that user had downloaded the tool created by Dunning called profilemaps.info.

57. In addition, the eBay technical team told FBI agents that a user who downloads

a tool created by Dunning (located at www.wholinked.com) will have a 1x1 pixel (which ends in the extension "GIF") execute and cause what appears to be a redirection to eBay.com which then forces a cookie to be stuffed and loaded on the user's computer with the PID from Dunning's Kessler's account. As mentioned above, profilemaps.info points to a URL associated with IP address 72.32.102.215. The domain names www.thunderwood.com and www.briandunning.com resolve to the same IP address. Both of these domains are registered to Brian Dunning at 15 High Bluff, Laguna Niguel, California, 92677 and he is listed as both the technical and administrative contact for these domains at 9258-368-7441 or brian@briandunning.com. The IP address has been traced to a web hosting service provider in San Antonio, Texas named Rackspace Managed Hosting. Similarly, www.wholinked.com has been traced to IP address 72.32.11.26 which is also serviced by Rackspace Managed Hosting.

58. Based on my training and experience, individuals who are committing fraud or attempting to deceive use multiple websites to initiate and perpetuate their fraud. In this investigation, it appears that Dunning is utilizing two tools profilemaps.info and www.wholinked.com, which appear to be at two different IP addresses that also hosts other domains which are linked to Dunning. This investigation has discovered several domains and websites used by the subject wherein it appears they are not directly related on the surface (i.e., www.thunderwood.com). However, it is very likely given that these sites may also contain the information sought. For instance, profilemaps.info points to a URL which goes to the same IP address as www.thunderwood.com, and www.briandunning.com and both of these domains are registered and serviced technically by Dunning. Therefore, Dunning could place various parts of the computer code which makes the tool profilemaps.info operate anywhere within either of these websites or in other folders/files on the servers that host that IP address. The same is true for the tool www.wholinked.com.

Confirmation fo the Fraudulent Activity by Installation of "Trip-wire"

59. EBay personnel informed FBI agents that, on June 7, 2007 at approximately noon, eBay technical staff installed a "trip-wire" to determine fraudulent traffic. The trip-wire finished rolling out globally at 6:42 p.m. on June 7, 2007. The goal of eBay's trip-wire analysis was to conclusively determine that certain Affiliates (specifically, those associated with Hogan and Dunning) were falsely

taking credit for "driving traffic" (defined as Internet users who come to eBay) and for subsequent revenue events and, thus, fraudulently getting paid out on a percentage of revenue that occurred as a result of this traffic. As described in more detail above, it appeared to eBay that these Affiliates were falsely taking credit for driving this traffic by having their computer programs mimic users coming to the eBay site by marking the users' machines with a tag ("cookie stuffing") that is used by eBay to give Affiliates credit for these events. However, when this fraudulent activity occurs, the users never actually came to the eBay.com homepage (www.ebay.com) and never saw the images that are viewed by humans on the page.

60. In order to establish that Hogan's and Dunning's Affiliates were performing this type of cookie stuffing, eBay installed a "trip-wire." The trip-wire that eBay installed was a special image on eBay's home page that allowed eBay to evaluate every visit to www.ebay.com <http://www.ebay.com/> and to identify if the special image on the page was actually viewed by a human (i.e., whether the image was actually loaded unto a computer screen for display). If the visit showed that a request was made to www.ebay.com <http://www.ebay.com/> without this image being shown, eBay then knew that a machine made this request to the home page merely for the purpose of getting eBay's servers to serve up a "cookie" and a human did not actually view the page. Ebay was able to decipher which Affiliate drove this false traffic based on the PID contained in the cookie which was set by eBay. The evidence obtained by eBay showed that a vast majority of the traffic driven to www.ebay.com <http://www.ebay.com/> by Hogan's and Dunning's Affiliates did not have this special image viewed and thus, was a machine making these requests.

61. The trip-wire is set up to collect the date and time, the IP address of the user receiving the cookie, and the affiliate PID, among other information. EBay utilizes a third party IP lookup table to map the Country and/or State from which the user that is receiving the stuffed cookie is located.

62. An analysis of the trip-wire by eBay indicates that on June 8, 2007, 97% of the traffic directed from Hogan's DPS account was fraudulent in that the special image was not accessed. On June 9, 2007, 98% of the traffic directed from Hogan's DPS account was fraudulent. On both June

8th and 9th, 2007, 98% of Dunning's traffic from his Kessler's account was fraudulent. Below are a few examples of the traffic directed from Hogan's and Dunning's accounts:

63. On June 7, 2007, at approximately 12:33:17:82, the trip-wire captured a cookie stuffed with information for the affiliate using PID 2225635 being sent from the eBay San Jose server to IP address 82.56.96.207. The user of this IP is located in Michigan. PID 2225635 is assigned to Hogan's DPS account.

64. In June 8, 2007, at approximately 12:52:40:72, the trip-wire captured a cookie stuffed with information for the affiliate using PID 2028993 being sent from the eBay San Jose server to IP address 172.174.248.28 which resolves to a customer utilizing the ISP America Online located in Virginia. PID 2028993 is assigned to Dunning's Kessler's account.

65. On June 8, 2007, at approximately 12:58:17:00, the trip-wire captured a cookie stuffed with information for the affiliate using PID 2225634 being sent from the eBay San Jose server to IP address 68.57.17.17. The user of this IP address is located in Pennsylvania. PID 2225634 is assigned to Hogan's DPS account.

66. On June 9, 2007, at approximately 12:05:03:90, the trip-wire captured a cookie stuffed with information for the affiliate using PID 2326993 being sent from the eBay San Jose server to IP address 87.74.32.80. The user of this IP address is located in England. PID 2326993 is assigned to Dunning's Kessler's account.

67. On June 9, 2007, at approximately 12:56:10:87, the trip-wire captured a cookie stuffed with information for the affiliate using PID 2225635 being dropped by the eBay San Jose server on IP address 71.210.107.53. The user of this address is located in Arizona. PID 2225635 is assigned to Hogan's DPS account.

68. On June 10, 2007, at approximately 18:36:38:97, the trip-wire captured a cookie stuffed with information for the affiliate using PID 2225634 being dropped from the San Jose server on IP address 203.101.184.6. The user is located in Pakistan. PID 222634 is assigned to Hogan's DPS account.

69. On June 11, 2007, at approximately 12:18:31:84, the trip-wire captured a cookie

stuffed with information for the affiliate using PID 2225634 being dropped by the San Jose server on IP address 206.40.234.218. The user of this IP address is located in Utah. PID 2225634 is assigned to Hogan's DPS account.

70. On June 11, 2007, at approximately 12:23:44:06, the trip-wire captured a cookie stuffed with information for the affiliate using PID 2326993 being dropped by the San Jose server on IP address 88.105.18.148. The user of the IP address is located in Essex, England. PID 2326993 is assigned to Dunning's Kessler's account.

71. All of these cookies were dropped by an eBay server located in San Jose, California. Each of these cookies was sent to a computer assigned an IP address that is geographically located (according to eBay and their third party vendors) either in a state other than California or in a country other than the United States. Moreover, eBay's information regarding these users indicates that each of the users resides outside of California. Accordingly, each of these cookies was sent by means of wire communication over the Internet in interstate or foreign commerce. Further, each of these wire communications was in furtherance of either Hogan's or Kessler's scheme to defraud because, if the user receiving the cookie goes to eBay within specified time periods and either registers as a new user with eBay or makes a purchase, Hogan or Kessler will receive payment from eBay pursuant to eBay's Affiliate program, even though the user in question had not actually "clicked through" to eBay from websites that were part of Hogan's or Kessler's network when each of the cookies described above was sent out from eBay's server . Accordingly, even if the user independently went to eBay or went to eBay from another affiliate and either registered or bought and item, Hogan and Dunning would receive credit for that event.

Analysis of Fraud Prior to Trip-Wire

72. EBay was able to provide data that indicates the fraudulent cookie stuffing began much further back than when the trip-wire began. For instance, eBay has reported that for Hogan's DPS account with PID 2225635, from December 2006 until May 2007, approximately 97% of the sessions allegedly directed by this affiliate PID never went beyond the "landing page." The "landing page" is the first page that a user goes to on a web site. Based on eBay's analysis of eBay's users' patterns of

activity, this is an extremely high percentage. That is, commonly a much greater number of people who "click through" to eBay's website from an affiliate would be expected to click on one or more links on eBay's homepage or perform a search for an item, whether or not that user ever actually registered with eBay or bought an item. For Hogan's DPA account with PID 2225634, for the same time period, approximately 96% of the sessions never go beyond the landing page. Dunning's Kessler's account with PIDs 2028993, and 2326993, from March 2007 through May 2007, approximately 96% of the sessions never go beyond the landing page. The eBay statistics also reflect that DPS has a very large number of sessions with only eBay server events wherein the user never gets to the landing page (actual homepage for eBay.com).

COMPUTER SEARCH PROTOCOL

73. With the approval of the Court in signing this warrant, agents executing this search warrant will employ the following procedures regarding computers that may be found on the premises which may contain information subject to seizure pursuant to this warrant:

Forensic Imaging

a. After securing the premises, the executing agents will consult with a computer specialist to determine the feasibility of obtaining forensic images of electronic storage devices while on-site. The feasibility decision will be based upon the number of devices, the nature of the devices and the volume of data to be imaged. The preference is to image on-site if it can be done in a reasonable amount of time and without jeopardizing the integrity of the data and the safety of the agents. The number and type of computers and other devices and the number, type, and size of hard drives are of critical importance. It can take several hours to image a single hard drive — the bigger the drive, the longer it takes. As additional devices and hard drives are added, the length of time that the agents must remain on-site can become overly intrusive, dangerous, and impractical.

b. If it is not feasible to image the data on-site, the computer equipment and any peripherals will be seized and transported off-site for imaging. Once a verified image has been obtained, the owner of the equipment will be notified and the equipment returned within thirty (30) days of seizure absent further application to this court.

c. A forensic image is an exact physical copy of the hard drive or other media. It is essential that a forensic image be obtained prior to conducting any search of the data for information subject to seizure.pursuant to this warrant. A forensic image captures all of the data on the hard drive or other media without the data being viewed and without changing the data in any way. This is in sharp contrast to what transpires when a computer running the common Windows operating system is started, if only to peruse and copy data — data is irretrievably changed and lost. Here is why: When a Windows computer is started, the operating system proceeds to write hundreds of new files about its status and operating environment. These new files may be written to places on the hard drive that may contain deleted or other remnant data. That data, if overwritten, is lost permanently. In addition, every time a file is accessed, unless the access is done by trained professionals using special equipment, methods and software, the operating system will re-write the metadata for that file. Metadata is information about a file that the computer uses to manage information. If an agent merely opens a file to look at it, Windows will overwrite the metadata which previously reflected the last time the file was accessed. The lost information may be critical.

d. Special software, methodology, and equipment is used to obtain forensic images. Among other things, forensic images normally are "hashed," that is, subjected to a mathematical algorithm to the granularity of 1038 power, an incredibly large number much more accurate than the best DNA testing available today. The resulting number, known as a "hash value" confirms that the forensic image is an exact copy of the original and also serves to protect the integrity of the image in perpetuity. Any change, no matter how small, to the forensic image will affect the hash value so that the image can no longer be verified as a true copy.

Forensic Analysis

e. After obtaining a forensic image, the data will be analyzed. Analysis of the data following the creation of the forensic image is a highly technical process that requires specific expertise, equipment and software. There are literally thousands of different hardware items and software programs that can be commercially purchased, installed and custom-configured on a user(s computer system. Computers are easily customized by their users. Even apparently identical computers in an office environment can be significantly different with respect to configuration, including permissions and access rights, passwords, data storage and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

f. Analyzing the contents of a computer, in addition to requiring special technical skills, equipment and software also can be very tedious. It can take days to properly search a single hard drive for specific data. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. As mentioned above, the computer may have stored information about the data at issue: who created it, when it was created, when was it last accessed, when was it last modified, when was it last printed and when it was deleted. Sometimes it is possible to recover an entire document that never was saved to the hard drive if the document was printed. Operation of the computer by non-forensic technicians effectively destroys this and other trace evidence. Moreover, certain file formats do not lend themselves to keyword searches. Keywords search text. Many common electronic mail, database and spreadsheet applications do not store data as searchable text. The data is saved in a proprietary non-text format. Microsoft Outlook data is an example of a commonly used program that stores data in a non-textual, proprietary manner; ordinary keyword searches will not reach this data. Documents printed by the computer, even if the document never was saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. Similarly, faxes sent to the computer are stored as graphic images and not as text.

g. Analyzing data on-site has become increasingly impossible as the volume of data stored on a typical computer system has become mind-boggling. For example, a single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now capable of storing more than 100 gigabytes of data and are commonplace in new desktop computers. And, this data may be stored in a variety of formats or encrypted. The sheer volume of data also has extended the time that it takes to analyze data in a laboratory. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. Even perusing file structures can be laborious if the user is well-organized. Producing only a directory listing of a home computer can result in thousands of pages of printed material most of which likely will be of limited probative value.

h. Based on the foregoing, searching any computer or forensic image for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained; criminals can mislabel and hide files and directories, use codes to avoid using keywords, encrypt files, deliberately misspell certain words, delete files, and take other steps to defeat law enforcement. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear necessary to locate and retrieve digital evidence within the scope of this warrant.

i. All forensic analysis of the imaged data will be directed exclusively to the identification and seizure of information within the scope of this warrant.

CONCLUSION

74. Based upon the information above, I have probable cause to believe that evidence, contraband, fruits, and/or instrumentalities of violations of Title 18, United States Code, Section 1343, (wire fraud) exists at the applicable SUBJECT PREMISES as set forth in more detail in Attachment B.

75. In summary, there is probable cause to believe that Hogan has committed wire fraud by utilizing computers at his residence and/or in conjunction with computers and/or servers associated with his business Digital Point Solutions. There is probable cause to believe that Hogan has created several free computer tools that are available to be downloaded from his web sites www.digitalpoint.com and www.shawnhogan.com which infect the visitor with a 1x1 pixel containing an unknown script that in turn places a cookie stuffed with Hogan's eBay DPS account affiliate information. It is believed that approximately 97% of Hogan's DPS affiliate directed traffic to eBay is fraudulent. Hogan has been paid approximately $28 million by eBay. Hogan is allegedly computer knowledgeable in regards to software development and languages and works from his residence (SUBJECT PREMISE 1) where he has a least two windows PCs which he utilizes for "testing" and

several other MAC computers. His web sites are hosted by a co-location facility with web hosting services named NetHere and there is probable cause to believe that the tools which are downloaded and contain the 1x1 pixel with script that forces the cookie stuffing is located on these servers. In all of the tests done to validate the cookie stuffing explained above, the 1x1 redirects to Hogan's website www.digitalpoint.com unbeknownst to the user.

76. Similarly, there is probable cause to believe that Dunning committed wire fraud. Dunning has created free computer tools which are downloadable, www.wholinked.com and profilemaps.info, which are linked by IP address to his website www.briandunning.com and www.thunderwood.com. All of the domains and IPs from which Dunning's free computer tools may be accessed are located on the servers of Rackspace.com (SUBJECT PREMISE 3) which are located in San Antonio, Texas. Dunning owns his own businesses and works from his residence (SUBJECT PREMISE 2). Dunning is also involved in computer programing and software and there is probable cause to believe he might be working on, testing, and revising script from his computers at his residence. It is believed that approximately 96% of the traffic Dunning directs from his Kessler's affiliate account to eBay is fraudulent. Dunning has been paid approximately $7 million for the fraudulent cookie stuffing with his Kessler's eBay affiliate account.

//

//

//

//

//

//

//

//

//

//

//