

UNITED STATES DISTRICT COURT
DISTRICT OF COLUMBIA

IN THE MATTER OF THE APPLICATION :
OF THE UNITED STATES OF AMERICA :
FOR A SEARCH WARRANT FOR THE : Magistrate No.08-445-M-01
PREMISES KNOWN AS :
[REDACTED] : Under Seal

FILED

DEC 18 2008

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

NANCY MAYER WHITTINGTON, CLERK
U.S. DISTRICT COURT

1. Your affiant in this matter, Donya Jackson, has been a Special Agent with the Office of the Inspector General at the Library of Congress since May 2007. Prior to her employment with the Library of Congress, your affiant was a Special Agent with the United States Secret Service since 2000. During your affiant's six year tenure with the U.S. Secret Service, she was assigned to the Criminal Investigation Division in Headquarters, and the New York Electronic Crimes Task Force based out of the New York Field Office, Brooklyn, New York. Your affiant has received training in the following subject areas: Basic Investigator Course, Interview and Interrogation, Undercover Computer Investigation Techniques, SEARCH High Tech Crimes Investigations of Computer Crimes Course, Investigation of Online Child Exploitation Course, and Search and Seizure of Electronic Evidence Techniques. Your affiant has made numerous arrests and interviewed numerous victims, witnesses, and suspects.

2. Your affiant has participated in numerous online investigations, and undercover online investigations.

3. Your affiant respectfully submits this affidavit in support of an application for a warrant to search the premises known as [REDACTED], [REDACTED] [REDACTED] ("PREMISES"). A description of the PREMISES is included in Attachment A hereto. For the reasons set forth in this affidavit, there is probable cause to believe that there is located within these premises evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1028 (Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information).

FACTS AND CIRCUMSTANCES

4. The statements in this affidavit are based on my personal investigation and on information provided by other law enforcement agents including Special Agent Pamela Hawe, of the Library of Congress Office of the Inspector General and on my experience and background as a Special Agent. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of 18 U.S.C. § 1028 are presently located at the PREMISES. See 18 U.S.C. §§ 1028(a)(2), 1028(a)(7) ("Whoever ... (2) knowingly possesses with intent to use unlawfully five or

more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents; [and/or] (7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit any unlawful activity ... shall be punished [under] this section.")

THE INVESTIGATION AND THE SUBJECT PREMISES

5. For the reasons set forth below, there is probable cause to believe that evidence of the violation of 18 U.S.C. § 1028 will be located at the PREMISES.

6. On June 6, 2008, Library of Congress ("LOC") employees G [REDACTED] H [REDACTED] and Eleanor Y [REDACTED] filed a complaint with the LOC Office of Inspector General stating that they were victims of identity theft. Further investigation showed that M [REDACTED] W [REDACTED], L [REDACTED] R [REDACTED], and L [REDACTED] T [REDACTED], three additional female LOC employees were also victims of identity theft. All five victims' identities have been compromised at the same companies (Home Depot, Target, Children's Place, and Chase Credit Services, to name a few) where credit accounts had been opened in their names without their knowledge and information pertaining to their LOC employment was used in the credit application process. I began my investigation by contacting the various stores and credit companies where these LOC employees had reported their

identification being compromised. Where possible, I obtained video footage of the instances where any individuals had applied for credit using the personal identifying information of LOC employees.

7. During the course of my investigation, I learned that on May 16, 2008, online credit applications in the names of E [REDACTED] Y [REDACTED] and M [REDACTED] W [REDACTED] were received by Chase Credit Services and Home Depot over the internet from IP Address 138.88.1.126. I also learned from Verizon Internet Service that on that date IP Address 138.88.1.126 originated and was registered to [REDACTED] [REDACTED], with email address [REDACTED].

8. During the course of my investigation, I also obtained video footage from a Target store located at 10500 Campus Way, Largo, Maryland 20774, showing a woman applying for Target credit using E [REDACTED] Y [REDACTED]'s identification information and purchasing two \$300.00 gift cards on May 16, 2008. I then obtained a photograph of [REDACTED] from the Department of Motor Vehicles ("DMV") in the District of Columbia. That DMV photograph matches the appearance of a person who can be seen in the May 16, 2008 video surveillance footage from Target in Largo, Maryland. That video further shows that while standing at the service counter and working with the same Target cashier, the suspect matching the general appearance of [REDACTED] supplied

an additional credit application using LOC employee M [REDACTED] W [REDACTED]'s identity. Two more gift cards in the amount of \$300.00 each were subsequently purchased using M [REDACTED] W [REDACTED]'s credit.

9. I also obtained video surveillance footage from that same Target store for May 30, 2008. That video footage shows a suspect matching the general appearance of [REDACTED] applying and receiving Target credit in the names of LOC employees' L [REDACTED] T [REDACTED] and L [REDACTED] R [REDACTED] while using the same Target cashier from the May 16, 2008 incident at the Largo, Maryland, location.

10. I also obtained video surveillance footage from Home Depot, 6691 Frontier Road, Springfield, Virginia 22150, in connection with an incident that occurred there on May 17, 2008. That video shows a suspect using E [REDACTED] Y [REDACTED]'s Home Depot credit to purchase two \$2,500 Home Depot gift cards. Based on the DMV photograph that I obtained, the suspect in the May 17, 2008 video from Home Depot appears to be [REDACTED].

11. On May 18, 2008, a fraudulent Victoria Secret's credit card purchase in the name of E [REDACTED] Y [REDACTED] was placed over the internet from IP Address 138.88.1.126, which is registered to [REDACTED]

[REDACTED]. During my investigation, I learned from United Parcel Service that those items purchased over the internet on May 18, 2008, were delivered on May 21, 2008, to [REDACTED]' home address located at [REDACTED]

[REDACTED]. The confirmatory email address given by
'the purchaser for the Victoria Secret website purchase was
[REDACTED]

12. During my investigation I have also learned that on May
27, 2008 and May 30, 2008, credit applications in the names of
G [REDACTED] H [REDACTED] and L [REDACTED] R [REDACTED] were received by GAP Credit
Services and Home Depot over the internet from IP Address
141.156.187.214. Verizon Internet Service provided that on that
date the IP Address 141.156.187.214 originated and was registered
to [REDACTED]
[REDACTED].

12b. I also learned that on May 28, 2008, a credit
application in the name of LOC employee G [REDACTED] H [REDACTED] was
received by Chase Credit Services from IP Address 69.143.158.220
at 9:24 pm. Comcast Internet Service provided that on that date
IP Address 69.143.158.220 originated and was registered to K [REDACTED]
Y [REDACTED], [REDACTED]
[REDACTED].

This apartment is one floor above [REDACTED]
apartment. Comcast also provided [REDACTED] as the contact
phone number for K [REDACTED] Y [REDACTED] with the address [REDACTED]
[REDACTED]

A search on the Accurint
database shows the most recent address for K [REDACTED] Y [REDACTED] is [REDACTED]
[REDACTED]

12c. I also learned during this investigation that during

May 2008 [REDACTED] used the cellular phone number ([REDACTED])
[REDACTED] I have obtained and reviewed call records for that
cellular phone which reveal at least five phone calls between
[REDACTED] telephone and K [REDACTED] Y [REDACTED]'s telephone number between
May 18 and May 29, 2008. Sprint suspended [REDACTED] cell
phone in June 2008.

REQUEST TO SEARCH THE PREMISES

13. In light of the foregoing information, and based on my
experience and training, I submit that there is probable cause to
believe that the PREMISES contains evidence concerning violations
of 18 U.S.C. § 1028. Specifically, any computers or computer
equipment at the PREMISES are likely to be the primary means of
accessing the Internet for purposes of collecting identification
materials and anonymously ordering merchandise using false
identification and therefore may be seized "as the means of
committing [the] criminal offense" pursuant to Federal Rule of
Criminal Procedure 41(b)(3) along with data storage devices such
as diskettes, thumb drives and other devices upon which
identification documents and purchase information can be stored.
The items to be seized are described in Attachment B hereto.

METHODS TO BE USED TO SEIZE AND SEARCH COMPUTERS AND COMPUTER-RELATED EQUIPMENT IN THE PREMISES

14. Based upon my training, experience, and information

related to me by agents and others involved in the forensic examination of computers and other electronic media, I know that electronic data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes, and memory chips. I also know that searching computerized information for evidence or instrumentalities of a crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve data from the system or phone in a laboratory or other controlled environment. This is true for the following reasons:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased,

compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the PREMISES. 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. Storage devices capable of storing up to 100 gigabytes of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of millions of pages of data.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg"

often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or instrumentalities of a crime.

15. In searching for data capable of being read, stored, or interpreted by a computer, law enforcement personnel executing the applicable Search Warrant will employ the following procedure:

a. Upon securing the PREMISES, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will search and seize any computers, computer equipment, and storage devices and transport these items to an appropriate law enforcement laboratory for review as to whether these items contain contraband. Because of the lengthy period of time necessary to perform a complete search of all

material contained in any computers, computer equipment and storage devices, it would not be feasible to conduct this search on the PREMISES, and seizure is necessary so that the preservation of data is not jeopardized. The computers, computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

b. If upon the search of the computers, computer equipment, and storage devices it is determined that the computers, computer equipment, and storage devices do not contain contraband, an instrumentality of the offense, a fruit of the criminal activity, or evidence of the offense specified above, then the computer personnel will return the cell phones, computer equipment and storage devices to the PREMISES.

c. The analysis of electronically stored data may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); "opening" or reading the first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately

hidden files; and performing electronic "key-word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

16. Any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the offense specified above.

17. In searching the data, the computer personnel may examine all of the data contained in the cell phones, computers, computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the data falls within the list of items to be seized as set forth in this affidavit.

18. If the computer personnel determine that the cell phones, computers, computer equipment and storage devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(b), the Government will return these items.

19. In order to search for data from computers, computer equipment and storage devices, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

a. any computers, computer equipment, and storage device capable of being used to commit, further or store evidence of the offense listed above;

b. any computers and computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;

c. any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, cameras, and videocameras;

d. any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

e. any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage

devices, or data to be searched;

f. any physical keys, encryption devices, dongles, and similar physical items that are necessary to gain access to the computer equipment, storage devices, or data; and

g. any passwords, password files, test keys, encryption codes, or other information necessary to access the cell phones, computer equipment, storage devices, or data.

CONCLUSION

20. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that there has been a violation of 18 U.S.C. § 1028, and that evidence of that crime exists inside of the premises described herein.

21. Your affiant believes that evidence of violations of 18 U.S.C. § 1028, listed in Attachment B to this Affidavit, which is incorporated herein by reference, are concealed at the PREMISES. Rule 41 of the Federal Rules of Criminal Procedure authorizes the government to seize and retain evidence and instrumentalities of a crime for a reasonable time, and to examine, analyze, and test them.

22. Based upon my knowledge, training and experience, and consultations with law enforcement experts, I know that searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment.

23. Your affiant, therefore, respectfully requests that the attached warrants be issued authorizing the search and seizure of

the items listed in Attachment B.

SPECIAL AGENT DONYA JACKSON
LIBRARY OF CONGRESS
OFFICE OF THE INSPECTOR GENERAL

Sworn and subscribed before me
this ____ day of July, 2008

THE HONORABLE DEBORAH A. ROBINSON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The premises to be searched is located at [REDACTED]
[REDACTED], and is described
as a three-story garden style apartment complex. The front door
is glass, with the number [REDACTED] located on the green overhang on
top of the entry way. [REDACTED] is located at the top of
the second flight of stairs as you enter the front glass door.
The premises is adjoining approximately eight more garden
apartments each that is numbered over the entry way. There is a
small parking area shared by all tenants.

ATTACHMENT B

ITEMS TO BE SEARCHED AND SEIZED

Evidence and proceeds relating to identity theft including, but not limited to, the following:

- A.) Seize all computers, monitors, keyboards, printers, cables, modems, software, hardware, instruction manuals, password documents, encryption and password codes and other computer equipment and accessories, and their stored information, and to remove said computer equipment from its location for a thorough examination at a controlled site; this includes records, documents, and materials in any form that are stored in electronic or magnetic form on hard drives, compact disks, zip disks, magnetic tapes or floppy disks, and;
- B.) Seize all cell phones, pagers, telephone records and bills that might evidence phone calls to and from co-conspirators/banks/victims, and seize any of these records that might be pertinent to this investigation, and;
- C.) Examine any fax machines, caller ID terminals, pagers, printers, scanners, embossing machines, encoding machines, typewriters, manual or electronic equipment or components, i.e. Personal Computers, used to print and store information, and seize any such items that appear to be pertinent to this investigation.