

AO 106 (Rev. 4/10) Application for a Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of Minnesota

RECEIVED

DEC 29 2010

CLERK, U.S. DISTRICT COURT
ST. PAUL, MINNESOTA

In the Matter of the Search of
675 Sarnia St., Apartment Unit #201, Winona, MN 55987

CASE NO.

10-MJ-510-JJG

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property

675 West Sarnia Street, #201, Winona, Minnesota, being a brick three story multi-family residence. The siding of the complex is red and gold brick and displays the numbers 675 in the color black on the back of the apartment. The entrance to the residence faces west onto Chippewa Street. Inside the apartment complex, the numbers 201 and the names Khoi VAN, Tram VO and Vinh DONG are displayed on the mailbox.

located in the State and District of Minnesota, there is now concealed:

See attached list of items to be seized

The basis for the search under Fed. R. Crim. P. 41(c) is:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of: Title 18, Section(s) 1343 and 1028

The application is based on these facts:

See attached Affidavit.

- ☒ Continued on attached sheet.
- ☐ Delayed notice of _ days (give exact ending date if more than 30 days;_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me, and subscribed in my presence

11/29/10 2:30 pm

Deanne J. Graham, U.S. Magistrate Judge

at

St. Paul, MN
City and State

Signature of Applicant
DANIEL D. SCHWARZ

SCANNED

DEC 29 2010

U.S. DISTRICT COURT ST. PAUL

10-MJ-510-JJG

STATE OF MINNESOTA)
) SS AFFIDAVIT OF DANIEL D. SCHWARZ
COUNTY OF WINONA)

I, Daniel D. Schwarz, being duly sworn under oath, state as follows:

1. I am a Special Agent employed by the Homeland Security Investigations (hereinafter) HSI, and I have been employed for the past 22 years. I am a graduate of the Federal Law Enforcement Training Center Criminal Investigator School and the USCS Basic Law Enforcement School. My experiences as an HSI agent has included the investigation of various federal offenses, 18 U.S.C. Sections 1956 & 1957 (Money Laundering), 18 U.S.C. Section 1028 (Identity Theft), and 18 U.S.C. Section 1343 (Wire Fraud). I have been involved and participated in various federal search and seizure warrants involving these investigations including search warrants related to computer based crimes. I have received training and have experience in general law enforcement and investigations involving violations of federal offenses, interviewing and interrogation techniques, arrest procedures, and the execution of searches and seizures. The information contained in this affidavit is based on my own personal observations, investigation and training, and, where noted, information related to me by other law enforcement officers and agents. Specifically, I have been in contact with or received information from other HSI agents in the National Cyber Crimes Center (C3) for HSI Headquarters in the Washington D.C. area who have been involved in various aspects of the investigation and case. I have personally discussed particulars of the investigation with Special Agent/Program Manager Michael Pak working in the Cyber Crimes Center.
2. I know from my training and experience that a common fraud scheme begins when a suspect uses a stolen identity to open accounts with eBay.com, a popular internet auction business; PayPal.com, a popular internet financial payment business; and various U.S. banks. I

know that all of the accounts are opened via the internet. The suspect, posing as an eBay seller under the assumed stolen identity, then advertises on eBay.com a listing of popular merchandise, such as, Rosetta Stone software, videogames, fiction and university textbooks, and Apple iTunes gift cards. These schemes often involve numerous suspects playing different roles such as computer hacker, fraud manager and controller, and money transfer mule.

3. An eBay.com buyer, who is looking for similar type merchandise as described above, bids on the eBay listing and ultimately wins the auction sale. The eBay buyer sends the payment through PayPal.com to the suspect, who is purporting to be an eBay seller. The suspect does not own or possess the listed merchandise. Instead, the suspect makes a purchase with a stolen identity and credit card information for the same merchandise won by the eBay buyer from third party internet merchant websites, such as, WWW.ROSETTASTONE.COM, WWW.AMAZON.COM, and WWW.APPLE.COM. The suspect instructs the merchant to ship the merchandise to the eBay buyer. The eBay buyer subsequently receives the merchandise that he believed he bought from the eBay.com website when in actuality the merchandise was shipped from an unrelated third party merchant. The third party merchant subsequently receives a financial loss due to credit card chargeback as a result of complaints from the true credit card holder to his credit card issuing bank. Ultimately, eBay.com and PayPal.com are exploited through the fraud. The third party merchant becomes a financial victim, and the true owner of the stolen credit card becomes an identity theft victim.

4. Lastly, after the eBay buyer sends the money to the suspect's PayPal.com account, the fraud manager or controller utilizes his U.S. based money transfer co-conspirator, who is often called a money transfer "mule," to transfer the illegal funds from PayPal to various U.S. bank

accounts. Ultimately, the "mule" then wires the illegal funds from various U.S. bank accounts to other domestic bank accounts or to overseas bank accounts. Most of the money transfers are conducted via the internet from computers under the control of the fraudster or the mules.

OPERATION EMULE INVESTIGATION

5. I have been working with HSI Senior Special Agent (SSA) Michael Pak who is assigned to the National Cyber Crimes Center (C3) for HSI Headquarters in the Washington, D.C. region. He has extensive experience investigating internet financial fraud and money laundering activities. SSA Pak is familiar with overseas criminal fraud rings that control an extensive criminal "mule" network based in the United States. SSA Pak relayed the following information to me:

- a) In September 2009, the Cyber Crimes Center (C3) initiated Operation eMule, an HSI investigative initiative targeting transnational cyber crime. HSI C3 is investigating this underground economy involving international criminal rings based in Vietnam that are committing Internet financial fraud against ecommerce and express mail courier sectors. The criminal ring makes online purchases from ecommerce merchants using stolen credit card information and then utilizes an elaborate network of mules based in the United States. HSI agents determined that mules are used to send stolen shipments of computers and other high-tech equipment or transfer illegal funds derived from fraud to Vietnam.
- b) Computer hackers and fraudsters including the money transfer mules often utilize proxy internet protocol (IP) addresses in order to mask the true location of their computer connection. SSA Pak is aware that a vast majority of the accounts in this investigation opened with eBay, PayPal, and various U.S. banks involves the use of proxy IP addresses.

- c) The underground economy involves an elaborate network of individuals playing various roles such as computer hackers, sellers of stolen personal identity, credit card and other financial information, fraud managers and facilitators, and mules/re-shippers. The communication is conducted through a secured Internet website accessed by vetted members only. The illicit funds and high end electronic merchandise that are part of the Vietnam Underground Economy are estimated to exceed hundreds of millions of dollars. The illicit funds and stolen merchandise are then laundered and/or re-shipped through an extensive network of U.S. based ethnic Vietnamese "mules" to Vietnam.
- d) The resulting fraud based on the stolen personal and financial identity results in a credit card chargeback loss to the ecommerce merchants due to unauthorized charges. The unauthorized charge is usually filed by the true owner of the compromised credit card to the owner's credit card issuing bank. The bank then notifies the ecommerce merchant that there was an unauthorized transaction and therefore the bank was charging back the fraudulent amount to the ecommerce merchant.
- e) Lastly, the cyber crime is conducted extensively over the internet. The computer hackers or fraudsters based overseas either hack personal computers and computer databases, or purchase stolen personal and financial information from underground websites. Subsequently, eBay, PayPal, email, and U.S. bank accounts are opened remotely on the Internet from Vietnam via proxy IP addresses. Due to the advancement of online banking, the suspects also readily use online banking to transfer illicit funds derived from the fraud from internet bank account to traditional bank account.

IDENTIFICATION OF A CYBER CRIME RING

6. According to SA PAK, he reviewed hundreds of eBay, PayPal and bank account records involving the aforementioned fraud scheme and money laundering activities of a fraud ring operating between Vietnam and the United States that involves the utilization of an extensive money transfer mule ring in the U.S. Based on the investigation, SSA Pak has identified several money transfer mules, who are international exchange students from Vietnam and are studying at various universities in the U.S. Two of the suspected members are as follows:

a) **Tram VO**

- i. F1 Student Visa International exchange student from Vietnam
- ii. Attending Winona State University, Winona, Minnesota

b) **Khoi VAN**

- i. F1 Student Visa International exchange student from Vietnam
- ii. Attending Winona State University, Winona, Minnesota

7. Currently, both Tram VO (VO) and Khoi VAN (VAN) reside at the address **675 West Sarnia St., Apartment Unit #201, Winona, MN 55987**. This information was verified through surveillance of the address where HSI special agents observed that VO and VAN's names were listed on the apartment unit #201 mailbox. Bank records indicated that VO listed her mailing address at 675 Sarnia St., Apartment Unit #201. Furthermore, U.S. Postal Inspector Joe Wolf of the Postal Inspection Service Cyber Intelligence Division confirmed that VO and VAN made address change requests to the U.S. Postal Service for all mails to be routed to 675 Sarnia St., Winona, MN from their previous address at 303 Winona St., Winona, MN.

8. Previously, during 2008 through early 2010, VO and VAN resided at the address 303

Winona St., Winona, MN 55987. This information was verified with Winona University registration records, bank records, U.S. Customs records and open source public records.

9. SSA Pak confirmed additional associations between VO and VAN through:
 - a. Both VO and VAN are associated with numerous PayPal accounts that were opened with the same stolen identities.
 - b. VO and VAN made numerous international bank wire transfers to the same beneficiaries in Vietnam.
10. Investigation revealed that VO and VAN are international exchange students, VO and VAN are currently admitted into the United States under a F1 student visa. Under an F1 student visa, VO and VAN are only allowed to work on University sponsored employment to support their studies and related expenses. They are restricted from engaging in employment outside of the University system. VO and VAN are suspected of violating their F1 student visa requirements through their involvement in this fraud scheme and operating an unlicensed money transfer business while attending the Winona University in Winona, Minnesota.
 - a. VO listed two email addresses on her U.S. State Department student visa applications: **Tvohuynhngoc08@winon.edu** and **Meoconluoi26011988@gmail.com**.

IDENTITY THEFT AND WIRE FRAUD

eBay and PayPal Information

11. eBay and PayPal are corporations headquartered in San Jose, California. eBay's operations center is in Salt Lake City, Utah. PayPal's operations center is located in Omaha,

Nebraska. When a subscriber opens an account with eBay or PayPal on the internet, the registration information is transmitted via the internet to the operations centers maintained in Salt Lake City, Utah and Omaha, Nebraska.

12. The investigation revealed that VO and VAN are associated with numerous PayPal accounts.

Identity Theft Victims – Associated with VO

13. Listed are three examples of identity theft involving eBay and PayPal, and Tram VO:

<u>eBay Account Name</u>	<u>PayPal Account Name</u>	<u>Location of ID. Theft Victim</u>
1) eusse_software	Nelly Eusse	Baltimore, MD
2) itunes.card.store	Francis Reed	Denver, CO
3) Un- identified	Susan Kim	Mountain View, CA

Nelly Eusse – Baltimore, Maryland

14. HSI agents reviewed the PayPal account, which is also known by the email address EUSSESOFTWARE@GMAIL.COM, which was opened in the name of Ms. Nelly Eusse and social security number XXX-XX-X277. The PayPal account received a total of \$102,156.66 in funds related to numerous eBay auctions of merchandise such as Rosetta Stone software, videogames, fiction and university textbooks and Apple iTunes gift cards. The Rosetta Stone software transactions ranged from approximately \$399.99 to \$499.99 per unit, which is about \$100 less than the retail price. It is believed that this lowered offered price was purposely done in order to attract buyers. There were three bank accounts on file: Premier Bank Account #XXXXXXXX773, Wells Fargo Bank Account #XXXXXXXX441, and Wells Fargo Bank Account #XXXXXXXX151.

15. HSI agents contacted Rosetta Stone as part of the investigation. HSI agents provided

Rosetta Stone with the names of the eBay buyers from the EUSSESOFTWARE@GMAIL.COM account. Rosetta Stone, Inc. Investigation Manager Jason Calhoun confirmed that Rosetta Stone shipped merchandise to the eBay buyers and that Rosetta Stone received credit card chargebacks on those purchases because the credit card charges were not authorized by the true credit card owner.

16. The name Tram VO was listed on the PayPal account opened under Ms. Nelly Eusse. VO's name was listed under the "Credit Card Statement" and "Business Statement" sections. The address of 303 Winona St., Winona, MN 55987 was also listed as the last active business address for the account. This address was the residence listed by Tram VO on her Winona University registration and Wells Fargo Bank accounts.

17. On June 14, 2010, Special Agents (SA) David Liu and Keely Maiden located and interviewed Ms. Nelly Eusse in Baltimore, Maryland regarding the eBay, PayPal, and Wells Fargo bank accounts that were opened using her name and social security number. Ms. Eusse advised that she has never opened an eBay or PayPal account. She has never had a Wells Fargo Bank account. She only banks at Bank of America and a Credit Union through her place of work. Ms. Eusse advised that she has never sold Rosetta Stone software or any merchandise on the internet. She further explained that approximately two (2) years ago, she was contacted by eBay and Wachovia Bank regarding suspected fraudulent online transactions using her stolen identity. She made a police report regarding the Wachovia Bank incident and resolved the fraudulent online transactions with eBay. Lastly, she advised that she does not know anyone named Tram VO.

Francis Reed – Mountain View, California

18. HSI agents reviewed the PayPal account, which is also known as itunescardstores@gmail.com, which was opened in the name of Ms. Francis Reed and social security number XXX-XX-X 387 for any financial transactions. The PayPal account received a total of \$3,380.76 in funds related to numerous eBay auctions of merchandise such as Apple iTunes gift cards. There were two bank accounts on file: Tram VO, Bank of America Account #XXXXXXXXXX684 and Tram VO, Wells Fargo Bank Account #XXXXXXXX914. The name Tram VO was listed on the PayPal account opened under Ms. Francis Reed. VO's name was listed under the "Credit Card Statement" and "Business Statement" sections. The address of 303 Winona St., Winona, MN 55987 was also listed as the last active business address for the account.

19. On September 21, 2010, Special Agent Andreas Melissaratos telephonically interviewed Ms. Francis Reed regarding the eBay, PayPal, Bank of America, Wells Fargo, and Google email accounts opened using her name and social security number. Ms. Reed advised that she did not open the eBay, PayPal, Bank of America, Wells Fargo, and Google email accounts. Ms. Reed explained that she was aware that her identity and personal information had been compromised about two (2) years ago. She does not know anyone named Tram VO.

Susan Kim – Denver, Colorado

20. HSI agents reviewed the PayPal account, which is also known as Thomas.linn4@gmail.com, opened in the name of Ms. Susan Kim and social security number XXX-XX-X143 for any financial transactions. The PayPal account received a total of \$3,473.96

in funds related to numerous eBay auctions of merchandise such as videogames and a computer. A Capitol One account #XXXXXXX626 in the name of Susan Kim was listed on the PayPal account.. The name Tram VO was listed on the PayPal account opened under Ms. Susan Kim. VO's name was listed under the "Credit Card Statement" and "Business Statement" sections. The address of 303 Winona St., Winona, MN 55987 was also listed as the last active business address for the account."

21. On September 21, 2010, SA Melissaratos telephonically interviewed Ms. Susan Kim regarding the PayPal, Capital One Bank, and Google email accounts opened using her name and social security number. Ms. Kim advised that she did not open the PayPal, Capital One Bank and Google email accounts. She does not know anyone named Tram VO.

Identity Theft Victims – Associated with VAN

22. Listed are three examples of identity theft involving eBay and PayPal, and VAN:

<u>eBay Account Name</u>	<u>PayPal Account Name</u>	<u>Location of ID. Theft Victim</u>
1) hhsusan00	Susan Higginbotham	Bemidji, MN
2) Un- identified	Alice Weaver	Franklin Furnace, OH
3) pray_software	Nikita Pray	Washington, DC

Susan Higginbotham – Bemidji, Minnesota

23. HSI agents reviewed the PayPal account, which is also known by the email address HHSUSAN98@GMAIL.COM, opened in the name of Ms. Susan Higginbotham and social

security number XXX-XX-X 855. The PayPal account received a total of \$50,740.00 in funds related to numerous eBay auctions of merchandise such as Rosetta Stone software. As described in Paragraph 15, these transactions were confirmed fraudulent by Rosetta Stone, Inc. There were two bank accounts on this PayPal account: Susan Higginbotham, Capital One Bank Account #XXXXXXXX735 and Khoi VAN, Bank of America Account #XXXXXXXXXX514.

24. The name Khoi VAN was listed on the PayPal account opened using Ms. Susan Higginbotham. VAN was listed under the "Credit Card Statement" and "Business Statement" sections. The address of 303 Winona St., Winona, MN 55987 was also listed as the last active business address for the account. This address was the residence listed by Khoi VAN in his Winona University school registration record as described in detail in paragraph 8.

25. On August 9, 2010, SA David Liu spoke with Ms. Susan Higginbotham telephonically regarding the PayPal account opened using her name and social security number. Ms. Higginbotham relayed that she filed a police report in 2009 to report her identity theft. She also stated that she has never sold or received any Rosetta Stone products. She has only used eBay about three years ago to sell and buy items that are around \$20.00 or less. She has never used a Gmail email address. In January 2009, Ms. Higginbotham received a letter from Wachovia Bank in reference to a new account opened in her name. She also received four letters from Capital One in reference to direct banking online accounts. She contacted Identity Theft Shield on January 29, 2009 regarding the letters.

26. On February 25, 2009, Higginbotham filed a police report and indicated in the report she only banks with Security Bank and First National Bank. Higginbotham has Identity Theft Shield through her work place and this company is handling her identity theft issues. She reported no

loss of money in reference to the identity theft. She also affirmed in a sworn statement that she has never conducted sales of any Rosetta Stone Software or Merchandise online or otherwise, nor has (s)he ever used a PayPal account to receive proceeds from sales of Rosetta Stone products.

Alice Weaver – Franklin Furnace, Ohio

27. Ms. Weaver's PayPal Account, which is also known by the email address ALICEWEAVER58@HOTMAIL.COM was created on November 22, 2008 in the name of Alice Weaver and social security number XXX-XX-X 306. A total of \$2,342.00 was received into this account. There was a Capital One Bank Account #XXXXXXXX454 under the name Alice Weaver listed on the PayPal account. The name Khoi VAN was listed in the "Credit Card Statement Name" section. The name Khoi VAN and the address 303 Winona St., Winona St., Winona, MN 55987 was also listed in the "Active Business" section.

28. On September 20, 2010, SA Melissaratos telephonically interviewed Ms. Alice Weaver regarding a PayPal, Capital One Bank, Hotmail, and Yahoo email accounts opened using her name and social security numbers. Ms. Weaver advised that she was not aware of the existence of these accounts. She did not open any of the accounts listed above. She filed a police report in early 2009 complaining about her identity theft. She does not know anyone named Khoi VAN.

Nikita Pray – Washington, D.C.

29. HSI agents reviewed the PayPal account, which is also known by the email address PRAYSOFTWARE@GMAIL.COM, opened February 14, 2009 in the name of Nikita Pray and social security number XXX-XX-X 421. A total of \$9,199.77 was received into this account. A

Premier Savings Bank Account #XXXXXXX461 under the name of Nikita Pray was listed on the PayPal account. Khoi VAN was listed in the "Credit Card Statement Name" and in the "Active Business" as Khoi VAN, 303 Winona St. Winona, MN 55987.

30. On September 20, 2010, SA Melissaratos telephonically interviewed Ms. Nikita Pray regarding the eBay, PayPal, Premier Savings Bank, and Google email accounts opened using her name and social security number. Ms. Pray advised that she was not aware nor did she authorize the opening of the accounts. She does not know anyone named Khoi VAN.

31. PayPal records indicated that VO is connected to at least fifty six (56) PayPal accounts that were opened under identity theft victim names located throughout the U.S. The PayPal records showed that VO's name and address at 303 Winona St. was listed on the fifty six (56) PayPal accounts. The total funds received in the 56 PayPal accounts exceeded \$247,000. A majority of the funds were associated with the sale of Rosetta Stone software, which were confirmed by Rosetta Stone Investigation Manager Jason Calhoun for fraud.

32. HSI agents reviewed twenty four (24) eBay accounts that were connected to the fifty six (56) PayPal accounts. The eBay accounts were opened under the same identity theft victim names.

33. HSI agents reviewed PayPal and eBay Account records pertaining to Khoi VAN, who is suspected to be working with VO as money transfer "mule." The PayPal records indicated that VO is connected to at least three hundred ten (310) PayPal accounts that were opened under identity theft victim names of located throughout the U.S. The total funds received in the 310 PayPal accounts exceeded approximately \$1,000,000. The records showed that VAN at 303 Winona St., Winona, Minnesota 55987 was also listed on the same three hundred ten (310)

PayPal accounts.

34. Approximately one hundred fifty seven (157) eBay accounts were connected to the three hundred ten (310) PayPal accounts. The eBay accounts were opened under the same identity theft victim names.

35. Rosetta Stone Investigation Manager Jason Calhoun confirmed Rosetta Stone suffered financial losses from credit card chargebacks that exceeded over \$1 million dollars as a result of this fraud scheme nationwide. I believe that VO and VAN were involved in a significant portion of the \$1 million dollars in chargebacks to Rosetta Stone as outlined previously in the fraud scheme.

PayPal Records – VO and VAN's Appeal on Account Restrictions

36. On November 3, 2009 a facsimile was sent to PayPal in Omaha, Nebraska regarding Ms. Nelly Eusse's PayPal account, which is often referred to by the email address EUSSESOFTWARE@GMAIL.COM. The facsimile included a passport photocopy, utility bill and bank statement. PayPal had previously frozen the account due to suspected fraudulent activity and the records were submitted in an attempt to lift the hold on the account. Listed on the fax cover sheet was the name Tram VO and referred to the PayPal account EUSSESOFTWARE@GMAIL.COM. The comment section included the description:

**"Please review my ID, Utility Bill and available the funds for withdraw
Thank you"**

37. On October 17, 2009 a facsimile was sent to PayPal in Omaha, Nebraska regarding Ms. Susan Higganbothom's PayPal account, which is often referred to by the email address

HHSUSAN98@GMAIL.COM. The facsimile included a passport photocopy, utility bill and bank statement. PayPal had previously frozen the account due to suspected fraudulent activity and the records were submitted in an attempt to lift the hold on the account. Listed on the fax cover sheet was also the name KHOI VAN and referred to the PayPal account HHSUSAN98@GMAIL.COM. The comment section included the description:

**“Hello
My account has been limited more 180 days
Please review my document and available for withdraw fund or send a check
to my address
303 Winona St. Winona, MN 55987
Thank you”**

38. HSI agents reviewed the facsimiles. SSA Pak determined that the fax documents were generated using a fax software called GFI FAX maker. SSA Pak checked the website address www.gfi.com and learned the following information about the software's features:

“GFI FAXmaker is a leading fax server for small to medium-sized enterprises. It makes sending and receiving faxes an efficient, simple and cost effective process and solves the problems with manual faxing: printing out the document, walking to the fax machine, waiting for the fax to go through, not to mention the cost of fax machine supplies and repair. GFI FAXmaker allows users to send and receive faxes directly from their email client.”

39. Based on the forgoing description of the fax software, it appears that VO and VAN generated the fax documents from their computers.

40. HSI agents reviewed the documents that were included in the facsimiles from VO and VAN and determined that the documents submitted by VO and VAN appeared to be fraudulent.

a) Copy of U.S. passports

HSI agents reviewed the copy of the U.S. Passports submitted by VO and VAN and determined that based on several features, they appeared fraudulent. Both passports listed the passport holder as Nelly Eusse and Susan Higganbothom respectively, however, the signatures showed the identical name "Michelle." This signature was unique because it appeared to be identical on both documents and there was no last name on the signature block.

b) Utility Bills from the Winona Water Authority

HSI agents reviewed the copies of the Winona Water Authority utility bill submitted by VO and VAN. The listed name on the bill submitted by VO was Nelly Eusse, at 303 Winona St., Winona, MN 55987. VAN used the same utility bill and changed the name to Susan Higganbothom.

c) Bank of America Statements

HSI agents reviewed the copies of the Bank of America statements submitted by VO and VAN and determined that they were fraudulent. The two statements were identical except for the name. The statement submitted by VO had the name Nelly Eusse and the statement submitted by VAN had the name Susan Higganbothom. The names listed on the top section under "Prepared for:" appeared to be added as they did not match the general font and typeface on the rest of the document.

MONEY LAUNDERING ACTIVITIES

41. VO opened at least 26 bank accounts at Wells Fargo, Capital One, Eastwood and HSBC

Banks and transferred funds from PayPal accounts that were opened with identity theft victims' names into these bank accounts. The total funds deposited amongst the accounts total approximately \$352,676 dollars. Funds totaling \$196,700 dollars were then wire transferred overseas to Vietnam and Canada.

42. VAN opened at least 6 Wells Fargo and Eastwood Bank accounts and transferred funds from PayPal accounts that were opened with identity theft victims' names into these bank accounts. The total funds deposited amongst the accounts total approximately \$523,617 dollars. The funds totaling \$480,020 dollars were then wire transferred overseas to Vietnam.

43. HSI agents determined that there were several bank checks that were addressed to VO at the address 675 West Sarnia St., Apt 201, Winona, MN. The last check sent and deposited into VO's Eastwood account was on September 13, 2010.

Specifics Regarding the Seizure and Searching of Computer Systems

44. Based on my own experience and consultation with other agents who have been involved in the search of computers and retrieval of data from computer systems and related peripherals, and computer media, there are several reasons why a complete search and seizure of information from computers often requires seizure of all electronic storage devices, as well as all related peripherals, to permit a thorough search later by qualified computer forensic agents or experts in a laboratory or other controlled environment.

45. Computer storage devices, such as hard disks, diskettes, tapes, laser disks, compact discs, and DVDs, can store the equivalent of hundreds of thousands of pages of information. Additionally, when an individual seeks to conceal information that may constitute criminal

evidence, that individual may store the information in random order with deceptive file names. As a result, it may be necessary for law enforcement authorities performing a search to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This review and sorting process can take weeks or months, depending on the volume of data stored, and would be impossible to attempt during a search on site; and

46. Searching computer systems for criminal evidence is a highly technical process, requiring specialized skill and a properly controlled environment. The vast array of computer hardware and software available requires even those who are computer experts to specialize in some systems and applications. It is difficult to know before a search what type of hardware and software are present and therefore which experts will be required to analyze the subject system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code imbedded in the system as a booby trap), a controlled environment is essential to its complete and accurate analysis.

47. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not

actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

SUMMARY

48. HSI agents confirmed that VO and VAN controlled an unusually large number of eBay and PayPal accounts that were opened with stolen identities of U.S. victims. VO and VAN also received illicit funds in these PayPal accounts that were derived from fraud exceeding over \$247,000 and \$ 1,000,000 dollars, respectively.

49. VO and VAN also opened and operated an unusually large number of bank accounts with Wells Fargo Bank, Capital One Bank, Eastwood Bank and HSBC Bank. VO and VAN circulated approximately \$1 million dollars just through their Wells Fargo Bank accounts alone. Based on the aforementioned information, there is reason to believe that all of the funds were

derived from fraud.


50. HSI agents determined that a majority of the eBay, PayPal and banking activities were conducted online to further the illegal fraud and money transfer activities through the use of computers and the internet. SA Melissaratos verified with Don Walski, who is a security manager at Winona University, that all registered students at Winona University are issued laptop computers.

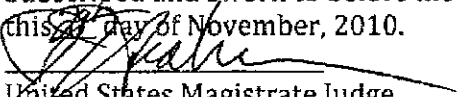
51. Based on my training and experience, a large scale fraudulent scheme such as this requires the use of a personal computer. These computers and peripherals travel with the suspects when they move to a new address.

CONCLUSION

52. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that at the residence of 675 West Sarnia St. Apartment #201, Winona, MN there exists evidence, contraband, fruits, and instrumentalities of violations of Title 18 U.S.C. 1341 (wire fraud), 1028 (identity theft), and 1956 & 1957 (money laundering), and 371 (conspiracy), among other federal crimes.

FURTHER YOUR AFFIANT SAYETH NAUGHT.


DANIEL D. SCHWARZ, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me.
this 27 day of November, 2010.

United States Magistrate Judge

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of Minnesota

In the Matter of the Search of
675 Samia St., Apartment Unit #201, Winona, MN 55987

CASE NO.

10-MJ-510-JJG

SEARCH AND SEIZURE WARRANT

TO: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the State and District of Minnesota:

675 West Samia Street, #201, Winona, Minnesota, being a brick three story multi-family residence. The siding of the complex is red and gold brick and displays the numbers 675 in the color black on the back of the apartment. The entrance to the residence faces west onto Chippewa Street. Inside the apartment complex, the numbers 201 and the names Khoi VAN, Tram VO and Vinh DONG are displayed on the mailbox.

The person or property to be searched, described above, is believed to conceal: See attached list of items to be seized.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before December 9, 2010.

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Jeanne J. Graham.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for days (not to exceed 30).

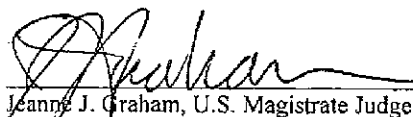
☐ until, the facts justifying, the later specific date of .

Date and Time Issued

11/29/10 2:30pm

at St. Paul, MN

City and State




Jeanne J. Graham, U.S. Magistrate Judge

SCANNED

DEC 28 2010

U.S. DISTRICT COURT ST. PAUL

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

RETURN		
Case No.:	Date and time warrant executed: 12/01/10 8:15 A.M.	Copy of warrant and inventory left with: Tram Vo, Khoi Van
Inventory made in the presence of: Tram Vo		
Inventory of the property taken and name of any person(s) seized: Please see Attached document.		
CERTIFICATION		
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.		
Date: 12/22/2010	 Executing officer's signature	
	DANIEL SCHWARTZ, Special Agent Printed name and title	
Subscribed, sworn to, and returned before me this date.		
 U.S. Judge or Magistrate		12/22/10 Date

IMMIGRATION AND CUSTOMS ENFORCEMENT - INVESTIGATIONS

Copy Distribution
 White Case File
 Canary Subject
 Pink SP File

EVIDENCE INVENTORY AND RECEIPT

PAGE 1 OF 1

Case Number M5020R10M50010
 Date/Time Search Initiated 12/1/2010 0900
 Date/Time Search Terminated 12/1/2010
 Subject(s) Name TRAM VO + KHOI VAN
 Address of Seizure 675 WEST SARKHA STREET APT 201 WINONA, MN 55987

Item #	Description of Evidence	Found By	Location Found
1	RECORDS (5 BAGS)	S/A PETERSON	BEDROOM 2
2	SHREDDERS RECORDS	S/A PETERSON	BEDROOM 2
3	CD-R (3 EA)	S/A PETERSON	BEDROOM 2
4	SD CARD 4 GB	S/A PETERSON	BEDROOM 2
5	MICRO SD CARD 128GB	S/A PETERSON	BEDROOM 2
6	APACER THUMB DRIVE	S/A PETERSON	BEDROOM 2
7	APPLE MAC BOOK PRO	S/A PETERSON	BEDROOM 2
8	MICRO SD CARD / ADP	S/A PETERSON	BEDROOM 2
9	DELL VOSTRO 320 PC	S/A PETERSON	BEDROOM 2
10	SEAGATE 6 GB USB DRIVE	S/A PETERSON	BEDROOM 2
11	2 GB USB THUMB DRIVE MACHOED IBM	S/A PETERSON	BEDROOM 1
12	APACER USB THUMB DRIVE V1 STRAP-VAN	S/A PETERSON	BEDROOM 1
13	SAN DISK 8 GB MP3 PLAYER	S/A PETERSON	BEDROOM 1
14	INSIGNIA MEDIA PLAYER	S/A PETERSON	BEDROOM 1
15	SEAGATE 500 GB USB HARD DRIVE	S/A PETERSON	BEDROOM 1
16	MAC BOOK PRO -VAN	S/A PETERSON	BEDROOM 1
17	BLACKBERRY STORM 2	S/A PETERSON	BEDROOM 1

By

(Agent's Signature)

DAN SCHWARTZ

Received By

TRAM VO

Date

12/01/10

Time

2:30 pm

Date

12/01/2010

Time

2:30 PM.

ITEMS TO BE SEIZED

- a. Books, records, receipts, tallies, journals, notes, ledgers, money orders, wire transfer receipts and other documents relating to domestic and international banking.
- b. Computers, hand-held wireless devices, facsimile machines to operate their business and store the records of their business activities.
- c. Documentation provided by state and federal agencies, including instruction pamphlets, documentation regarding filing and reporting requirements, training and certification, as well as documentation and correspondence from various state and federal agencies, including the IRS and the Department of Homeland Security Financial Data Center and FINCEN
- d. Records of all customer accounts and names, as well as transactions, such as money orders or cashier's checks issued or purchased on behalf of customers, checks cashed, and domestic and international wire transfer logs, book, ledgers and invoices evidencing such financial transactions. Other records that are kept include all documentation from other money remitting companies and other financial institutions or individuals with whom a financial relationship may exist or are utilized to assist in or complete the money transfers for customers.
- e. Maintain sums of U.S. Currency on the premises of their businesses.
- f. Notes, records of disbursement to and receipts of payments from various customers, including those involving unreported cash transactions and international transfers, as well as documentation regarding the sale and purchase of money orders.
- g. Banking records, including cancelled checks and all receipts, wire transfer applications and receipts, check cashing and wire transfer logs, keys and documentation for safe deposit boxes, money wrappers, used and new stored value cards, loan applications and lines of credit, both for their businesses as well as for their personal accounts.
- h. Documentation evidencing ties to the property and business, including business licenses and permits, rental, purchase or lease agreements, utility and telephone bills.

Specifics Regarding the Seizure and Searching of Computer Systems

Based on my own experience and consultation with other agents who have been involved in the search of computers and retrieval of data from computer systems and related peripherals, and computer media, there are several reasons why a complete search and seizure of information from computers often requires seizure of all electronic storage devices, as well as all related peripherals, to permit a thorough search later by qualified computer forensic agents or experts in a laboratory or other controlled environment:

Computer storage devices, such as hard disks, diskettes, tapes, laser disks, compact discs, and DVDs, can store the equivalent of hundreds of thousands of pages of information. Additionally, when an individual seeks to conceal information that may constitute criminal evidence, that individual may store the information in random order with deceptive file names. As a result, it may be necessary for law enforcement authorities performing a search to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This review and sorting process can take weeks or months, depending on the volume of data stored, and would be impossible to attempt during a search on site; and

Searching computer systems for criminal evidence is a highly technical process, requiring specialized skill and a properly controlled environment. The vast array of computer hardware and software available requires even those who are computer experts to specialize in some systems and applications. It is difficult to know before a search what type of hardware and software are present and therefore which experts will be required to analyze the subject system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code imbedded in the system as a booby trap), a controlled environment is essential to its complete and accurate analysis.

Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends

less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.