

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

FILED

APR - 5 2007

CLERK, U.S. DISTRICT COURT  
EASTERN DISTRICT OF CALIFORNIA  
BY \_\_\_\_\_  
DEPUTY CLERK

UNITED STATES OF AMERICA

v.

TIEN TRUONG NGUYEN  
PLACER COUNTY JAIL  
2775 RICHARDSON DRIVE  
AUBURN, CALIFORNIA 95603

(Name and Address of Defendant)

CRIMINAL COMPLAINT

CASE NUMBER:

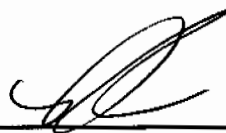
2:07 - MJ - 0102 DAD

I, the undersigned complainant being duly sworn state the following is true and correct to the best of my knowledge and belief. On or about **October 15, 2005, through January 26, 2007**, in Placer and Sacramento Counties and elsewhere, in the Eastern District of California defendant(s) did, (Track Statutory Language of Offense)

▶ **See Attachment Affidavit of Senior Special Agent Brian Korbs attached hereto as Exhibit A**

in violation of Title 18, United States Code, Sections: 371; 1029(a)(2),(a)(3), and (a)(4), 1028(a)(7), 1028A; 1030(a)(4) and 922(g)(1) and 2.

Continued on the attached sheet and made a part hereof.



Signature of Complainant SENIOR S.A. BRIAN KORBS  
UNITED STATE SECRET SERVICE

Sworn to before me, and subscribed in my presence

APRIL 5, 2007

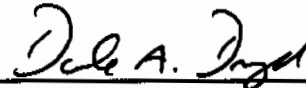
at

SACRAMENTO, CALIFORNIA

Date

City and State

DALE A. DROZD  
UNITED STATES MAGISTRATE JUDGE



Name and Title of Judicial Officer

Signature of Judicial Officer

## **AFFIDAVIT OF SSA BRIAN KORBS IN SUPPORT OF COMPLAINT**

I, Brian Korbs, a Senior Special Agent of the United States Secret Service, being duly sworn, depose and state as follows:

### **Introduction**

1. I am a Senior Special Agent (“SSA”) of the United States Secret Service (“USSS”) and have been so employed since 1984. I am currently assigned to the Sacramento Resident Office. As part of my duties, I investigate offenses involving access device fraud. In that capacity, I have received training and have become familiar with the investigation and prosecution of access device fraud, including the use of various criminal methods to perpetrate these frauds.

2. I have also received training through the U.S. Secret Service’s Electronic Crimes Special Agent Program (“ECSAP”), and I am trained and qualified to conduct forensic examinations of computers and other forms of digital evidence. I have conducted over 100 computer examinations in my career and have testified to the results of these examinations in federal court.

3. I have participated in investigations to include cases involving access device fraud, counterfeiting of access devices, identity theft, and identity document fraud. Further, I have received extensive training regarding the investigation and prosecution of access device fraud cases.

4. I am familiar with the information contained in this affidavit based on: (i) direct knowledge of each of the following facts or upon information provided to me by other law enforcement officers; (ii) interviews conducted with various individuals; and (iii) information received from third parties, such as bank investigators and victims.

5. Based on my training and experience from past counterfeit access device manufacturing investigations and consultation with other law enforcement officers regarding various counterfeit access device investigations, I am aware that fraudulent and counterfeited credit and debit card schemes involve a number of component activities consisting of:

a. The illegal obtaining of/and trafficking in valid credit and debit card account numbers, primarily Visa, MasterCard, and American Express credit card account numbers.

b. Criminals will also steal victim’s credit and debit card numbers and personal identity information by tricking true cardholders into revealing this information through the use of bogus or fake emails and websites. These fake or bogus emails or websites are often fabricated by criminals to appear to be from legitimate financial, commercial or government institutions. This criminal method is referred to as “phishing.” Criminals involved in phishing will also sell stolen

credit and debit card numbers, often in bulk, to other co-conspirators on the internet.

c. Criminals may also steal credit, debit and personal identity information from financial or commercial institutions by gaining unauthorized access to the institution's computers. This method is commonly referred to as "hacking." Through this method, criminals can sometimes steal thousands of credit, debit and customer profiles and then either use this stolen information for themselves or sell this information, oftentimes via the internet, to other criminals.

d. Co-conspirators will then oftentimes electronically encode the stolen credit and debit card numbers onto counterfeit credit cards using a computer and an electronic encoding device.

e. The number of "traffickers" between the front-line person and the counterfeit credit card manufacturer can vary. Sometimes, traffickers will receive counterfeit credit cards in addition to or in lieu of payment for the numbers or payment is made using various methods of online (internet) currency such as EGold. Other times traffickers in stolen credit and debit cards can pay one another using traditional money transfer methods such as Western Union, Moneygram and the Federal Reserve bank to bank wire transfer method.

f. Once the fraudulent or counterfeit credit cards are made, they can be sold, used personally by the manufacturer, given to conspirators as payment for illegally obtaining numbers, or given to "shoppers." Shoppers are individuals who illegally use the cards to buy high-dollar items such as electronics, gift certificates or gift cards, or other items such as jewelry that have resale value. These items may be returned to the manufacturer or sold so that part of the proceeds is returned to the manufacturer. These counterfeit credit and debit cards are also oftentimes used to withdraw cash by criminals from Automatic Teller Machines (ATM's).

6. I make this affidavit in support of the issuance of a criminal complaint and arrest warrant against:

Tien Truong Nguyen aka Tim Nguyen (aka "Nguyen").

7. Based on the information set forth herein, there is probable cause to believe, and I do believe, that from in or about October 15, 2005 through January 26, 2007, defendant Nguyen committed violations of Title 18 U.S.C. Section 371 – Conspiracy; Sections 1029 (a) (2), (a) (3), and (a) (4) – Access Device Fraud; 1028 (a) (7) – Fraud and Related Activity in Connection with Identification Information; Section 1028A – Aggravated Identity Theft; Section 1030(a)(4) – Fraud and Related Activity in Connection with Computers; Section 922(g)(1) -- Felon in Possession of a Firearm; and Section 2 - Aiding and Abetting.

- a. A Dell Laptop Computer "Latitude" Serial Number 8P530B1;
- b. A Toshiba Laptop Computer "M-45" With Black thumb drive Serial Number 26234221Q;
- c. A Hewlett Packard Laptop Computer "Pavilion DV1000" Serial Number CNF5382K5T;
- d. Two black USB Thumb Drives; and
- e. A Dell Computer Model 470 Ser: 37NQC61.

11. A preliminary forensic examination of these computers and electronic devices shows that Nguyen: (A) was communicating with others, including individuals in Eastern Europe, to acquire credit card and debit card numbers, social security numbers, and other personal identification information; (B) possessed fragments of fraudulently created Web sites and e-mail, purporting to be from companies such as PayPal, seeking updates of credit card and other personal information; (C) possessed thousands of e-mail addresses of potential victims, which may have been used to carry out the "phishing" scheme; (D) thousands of pages of customer information which appears to have been taken from companies, such as eBay; Western Union, and others.

Among the specific items I found on Nguyen's computers are:

- a. Hundreds of files (lists) of credit card numbers, many with Personal Identification Numbers (PINs) as well as the true cardholders name, address, email address, password, bank account information, social security number, driver's license number, telephone number, etc. Collectively, it appears that these lists contain potentially tens of thousands of compromised credit card numbers, bank account numbers and stolen identities.
- b. Files containing what appear to be fictitious websites of known financial institutions that have been victimized through phishing schemes. These website folders include such institutions such as eBay in San Jose, California; Fairwinds Credit Union located in Florida; Heritage Bank located in Olympia, Washington; the Honolulu City and County Employees Credit Union in Hawaii; and others.
- c. Software that is used with credit card encoding devices, that is, devices that are used to encode the magnetic stripes on the back of credit and debit cards with stolen account numbers.
- d. Lists of what appears to be thousands of email addresses, some of which are segregated by state that appear to be used for sending fraudulent email solicitations.

- e. Extensive files containing the text of online chat conversations between Nguyen and other co-conspirators. One such file of Yahoo chat conversations is approximately 25 megabytes in size and when converted to a Microsoft word document consists of over 16,000 pages.

THROUGH BJK/020

12. A review of a portion of the Internet "chat" and/or instant messages shows Nguyen, using the moniker "denisektran," communicating with third parties. This user name is tied to Nguyen through (1) his admission that he used it; (2) the fact that the chat was found on his computer; and (3) personal information in the chat messages.

13. For example, on or about November 10, 2006, Nguyen engaged in a lengthy exchange with "anthonyod01" (identity unknown) in which they discuss the exchange of e-mail addresses from Virginia.edu, and other information, for money. These e-mails are used to carry out the phishing fraud.

14. I also found a large number of similar messages on Nguyen's computer between Nguyen, and others, in which credit card and other personal information was exchanged. These communications also contain information about fraudulent Web pages used to carry out fraud.

#### **GE Capital/Wal-Mart Fraud**

15. As part of the conspiracy and the fraud, Nguyen, and others, both known and unknown to the government, used the fraudulently obtained credit card numbers, and other personal identification information, to obtain instant credit through GE Capital, and to make fraudulent purchases of gift cards and merchandise.

16. Specifically in or about September 2006, I became involved in an investigation involving suspects using hundreds of victims' personal information to obtain instant credit at Wal-Mart stores throughout California. During this investigation I learned that several suspects were involved in the case to include Tien Nguyen. Specifically, I learned that Tien Nguyen was helping provide other suspects with stolen personal identification information in which to obtain credit in victims' names.

17. On January 26, 2007, an arrest warrant issued by the Placer County Superior Court for Nguyen for his involvement in the Wal-Mart instant credit fraud. This warrant was obtained by Detective Jim Hudson of the Placer County Sheriff's Department and charged Nguyen with violating the California Penal Statute for identity theft.

18. Continuing on January 26, 2007, Placer County Sheriff detectives and I located Nguyen at his residence in Sacramento and he was taken into custody. Nguyen consented to a search of his residence that resulted in the seizure of nearly fifty (50) counterfeit credit cards and several computer systems, some of which were on and actively working. Placer County Detectives and I also located and seized thousands of dollars in merchandise that appeared to have been purchased with counterfeit credit

cards. Also seized was what appeared to be clear plastic laminate used to make counterfeit California driver's licenses. These items were seized by the Placer County Sheriff's Department and entered into evidence. These evidentiary items have been stored at the Placer County Sheriff's Department since they were seized from Tien Nguyen's residence on January 26, 2007.

19. Following his arrest on January 26, 2007, and after waiving his Miranda Rights, Tien Nguyen admitted to Placer County Detective Jim Hudson and I that he was responsible for providing the original suspects in the Wal Mart instant credit fraud investigation with the stolen personal information in which to obtain credit. The credit was obtained by entering personal information into a self-service kiosk/terminal hosted by GE Capital at Wal-Mart stores in Northern California. This terminal was a protected computer of GE Capital in so far as it was connected to the Internet and part of a secured system operated by GE Capital. This terminal caused wire transmissions to other protected computers of GE Capital, in Ohio, which processed the request and issued the instant credit.

20. Tien Nguyen also told Detective Hudson and I that he uses victims' credit card numbers and makes counterfeit credit cards to obtain cash and merchandise. Tien Nguyen further admitted that he uses his computers to communicate with other criminals to obtain stolen identity and credit card information.

21. Prior to Tien Nguyen's arrest on January 26, 2007, the Placer County Detectives and I learned that Nguyen and the other co-conspirators had used computers to communicate and transfer stolen personal information. The computers and thumbdrives seized incident to the arrest of Nguyen were found in the bedroom of this residence that was used by Tien Nguyen. A forensic examination of another co-conspirator's computer provided the scope of the Tien Nguyen's involvement in the fraud. This forensic examination showed that the fraud covers co-conspirators and victims from throughout the United States and from abroad.

22. Based on my training and experience in conducting access device fraud investigations, I believe that the defendant's conduct affected interstate commerce. The defendant conspired in fraud in which stolen personal information, among other things, was used to obtain instant credit through GE Capital, which operates throughout the United States. Further, the defendant and others stole credit cards and made fraudulent purchases using cards issued by banks operating outside of California. Additionally, when an unauthorized credit card is used it causes a financial transaction between the bank and other business entities, such as the issuing bank for the card, and the clearing center processing the transactions, which effects interstate commerce.

#### **Felon in Possession Charge**

23. On January 26, 2007, I know that Nguyen, a felon, was found to unlawfully possess a shotgun. In particular, during the search at Nguyen's residence, a Remington 870 Magnum Express, Serial Number D950177M, shotgun was found in

Nguyen's bedroom. In addition to the shotgun, also in plain view, were approximately 10 rounds of Remington 12 gauge shotgun shells, both slugs and buckshot.

24. The firearm was located in the room occupied by Nguyen, and was kept standing vertically behind his computer stand against the wall. The ammunition was found in a box a few feet away from the firearm. The room was occupied and controlled by Nguyen. Only male clothing and personal items belonging to Nguyen were found in the bedroom. Thus, although others resided in the residence, Nguyen appeared to be the sole occupant of the bedroom. Further, although Nguyen's girlfriend was staying at the house, she had just arrived from Southern California and had her luggage still packed.

25. On March 27, 2007, I determined that according to the California Department of Justice computerized criminal history database Nguyen (CII number A1067xxxx) had at least one felony conviction, namely an offense punishable by more than one year in prison, namely:

1999, Orange County, California, Violations of the California Penal Code Section 496(A), (Receiving Stolen Property); 476 (Make/Pass Fictitious Check); 502.7(B)(1) (Fraudulent Use of a Telephone or Telegraph); and California Health and Safety Code Section 11377(A) (Possession of Controlled Substance).

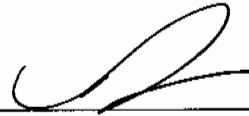
In addition, in 2002, Nguyen violated his parole and he was remanded to custody.

26. On March 27, 2007, I spoke with Special Agent Sara Lewis of the Sacramento office of the Bureau of Alcohol, Tobacco and Firearms (ATF). Special Agent Lewis told me that this Remington 870 shotgun was manufactured in Ilion, New York and that the ammunition was manufactured in either Lonoke, Arkansas or in Connecticut. Based on this information, I am informed and believe that the shotgun and ammunition possessed by Nguyen, traveled in and affected interstate commerce.

### **Conclusion**

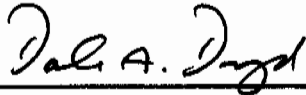
27. Based on the above information, I believe there is probable cause that Nguyen has violated Title 18 U.S.C. Section 371 – Conspiracy; Sections 1029 (a) (2), (a) (3), and (a) (4) – Access Device Fraud; 1028 (a) (7) – Fraud and Related Activity in Connection with Identification Information; Section 1028A – Aggravated Identity Theft; Section 1030(a)(4) – Fraud and Related Activity in Connection with Computers; Section 922(g)(1) -- Felony in Possession of a Firearm; and Section 2 - Aiding and Abetting.

Wherefore, this Affiant respectfully requests that the court issue an arrest warrant for Nguyen. I swear under penalty of perjury that the above facts are true and correct to the best of my knowledge.



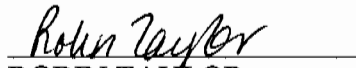
\_\_\_\_\_  
Brian Korbs, Senior Special Agent  
United States Secret Service

Sworn to before me this 5<sup>th</sup> day of April 2007



\_\_\_\_\_  
HONORABLE DALE A. DROZD  
UNITED STATES MAGISTRATE JUDGE  
EASTERN DISTRICT OF CALIFORNIA

Approved as to Form



\_\_\_\_\_  
ROBIN TAYLOR  
Assistant United States Attorney