
**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA : Hon. Steven C. Mannion
 : :
 : Mag. No. 13-6080 (SCM)
 : :
DUY TRUONG : **CRIMINAL COMPLAINT**


I, Russell A. Ficara, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.



Russell A. Ficara, Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,
June 5, 2013 at Newark, New Jersey

HONORABLE STEVEN C. MANNION
UNITED STATES MAGISTRATE JUDGE



Signature of Judicial Officer

ATTACHMENT A

From in or about 2007 through the present, in the District of New Jersey, and elsewhere,
defendant

DUY TRUONG

did knowingly and intentionally conspire and agree with others to devise a scheme and artifice to defraud financial institutions, and to obtain any of the moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, those financial institutions, by means of false and fraudulent pretenses, representations, and promises, contrary to Title 18, United States Code, Section 1344.

In violation of Title 18, United States Code, Section 1349.

ATTACHMENT B

I, Russell A. Ficara, a Special Agent with the Federal Bureau of Investigation (“FBI”), have knowledge of the following facts based upon: (a) my investigation; (b) discussions with witnesses and other law enforcement agents; (c) review of over 1,100 bank accounts; and (d) searches of e-mail accounts, residences, offices, and drop addresses. Because this Complaint is being submitted for the limited purpose of establishing probable cause, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts which I believe are necessary to establish probable cause.

INTRODUCTION

1. The FBI and law enforcement agencies in Vietnam, the United Kingdom, and elsewhere have been investigating a massive conspiracy that worked as one of the largest resellers of stolen credit card data in the world. The co-conspirators included defendant DUY TRUONG and others (collectively, the “Co-Conspirators”). The Co-Conspirators used a website and email accounts to sell data relating to more than 1.1 million stolen credit cards, as well as stolen personal identifying information (“PII”) for victims around the world, including in New Jersey. Losses attributable to these stolen cards are estimated to exceed \$200 million in total.

BACKGROUND

2. The At all times relevant to this Complaint:
- a. Goods and services were purchased through the Internet using credit cards (“Online Purchases”).
 - b. To make an Online Purchase, a purchaser was required to provide certain personal identifying information (“PII”) about the purchaser, including the purchaser’s name and address, and certain information about the credit card, including the credit card number, the expiration date of the credit card, and the card verification value (“CVV”), which was the number normally found on the reverse of the credit card.
 - c. After an Online Purchase was completed, the vendor often maintained the purchaser’s PII, provided during the course of the Online Purchase, on computer servers belonging to the vendor. If so stored, the purchaser’s PII was ordinarily secured by the vendor, including through encryption of the relevant information.
 - d. Defendant TRUONG served as one of the leaders of the conspiracy, and resided in Vietnam.

THE CONSPIRACY

3. The conspiracy was based in Vietnam, and specialized in obtaining PII that had

been provided to retailers who sold goods and services online, and whose customers paid for these goods and services through Online Purchases. The co-conspirators included defendant TRUONG and others (collectively, the “Co-Conspirators”). The Co-Conspirators illegally obtained a variety of PII belonging to customers who had made Online Purchases, including the purchasers’ names, addresses, credit card information, and social security numbers, among other types of information.

4. Once the Co-Conspirators had obtained the PII, they then sold this data on a per-victim basis. The data related to a single, identifiable, victim was referred to as a “dump.”

5. The Co-Conspirators used e-mail accounts (the “Fraud E-Mail Accounts”) and a website located at www.mattfeuter.biz and www.mattfeuter.com (the “Fraud Website”) to facilitate their crimes.

6. Other individuals seeking to illegally purchase victims’ credit card information (“Dump Purchasers”) either accessed the Fraud Website, or sent the Co-Conspirators an e-mail to the Fraud E-Mail Accounts. Via the Fraud Website or the Fraud E-Mail Accounts, Dump Purchasers requested a certain number of dumps.

7. The Co-Conspirators selling the dumps, including defendant TRUONG, charged a fee for each dump sold. This fee varied from approximately \$1 to approximately \$300 per dump, depending on the victim’s country of origin and the completeness of the information being sold, among other factors. These fees were paid via wire transfer services, such as Western Union and Liberty Reserve.

8. Each wire transfer service transaction was assigned a specific transaction number, often called a “Money Transfer Control Number,” or “MTCN.”

9. The Co-Conspirators’ methods of selling illegally-obtained PII varied depending on whether a Dump Purchaser was communicating with the Co-Conspirators through a Fraud E-Mail Account or through the Fraud Website.

10. If a prospective Dump Purchaser sought to purchase illegally-obtained victim PII from the Co-Conspirators through a Fraud E-Mail Account, the Co-Conspirator, including defendant TRUONG, sent an e-mail to the prospective Dump Purchaser and provided a name to whom the wire transfer was to be made out. The Dump Purchaser then replied via e-mail to one of the Fraud E-Mail Accounts and included an MTCN, representing the money that the Dump Purchaser had wired to the name provided by the Co-Conspirator. Once the Dump Purchaser provided the MTCN number for the dumps sought, the Co-Conspirator would e-mail back, from the Fraud E-Mail Account, the requested number of dumps to the Dump Purchaser.

11. By contrast, if a Prospective Dump Purchaser sought to purchase illegally-obtained victim PII from the Co-Conspirators through the Fraud Website, the prospective Dump Purchaser first had to register as a user on the Fraud Website by creating an account using login

credentials, including a username and a password. The prospective Dump Purchaser could then browse the Fraud Website for particular credit cards, including choosing to obtain victim PII from particular regions of the world, or victim PII from particular credit card issuers. The prospective Dump Purchasers would then go to a “checkout” screen, and enter in their Liberty Reserve number. The costs of the dump purchase would be debited from the Dump Purchaser’s Liberty Reserve account.

12. The Dump Purchaser would either incur fraudulent charges on the victims’ credit cards himself, or resell dumps to yet other downstream purchasers. In either event, the victims’ credit cards incurred, cumulatively, more than \$200 million in fraudulent charges as part of the scheme and artifice to defraud.

CONNECTING THE DEFENDANTS TO THE CONSPIRACY

13. As part of a related case, an individual (hereinafter “CD-1”) pled guilty to participating in a credit card fraud scheme, and agreed to cooperate with law enforcement. As part of CD-1’s cooperation, CD-1 participated in meetings with individuals who claimed to have access to stolen credit card numbers, but who needed someone who could make the actual credit cards. CD-1 responded that CD-1 would be able to take the numbers and create credit cards.

14. During a subsequent meeting, one of these individuals sat next to CD-1 and used a laptop to log into an e-mail account. CD-1 observed that this e-mail account contained numerous e-mails from the e-mail account mattfeuter123@gmail.com (the “Feuter 123 Gmail Account”). The e-mails from the Feuter 123 Gmail Account contained the names, addresses, credit card numbers, expiration dates and CVVs of third parties. The investigation has revealed that this information belonged to unwitting identity theft victims. CD-1 copied down credit card information from one e-mail pertaining to numerous victims.

15. Pursuant to duly-authorized search warrants, law enforcement officers examined the contents of the Feuter 123 Gmail Account. This search uncovered a vast quantity of information relating to the conspiracy, and that the Feuter 123 Gmail Account was a primary Fraud E-mail Account used in the scheme to defraud. In the Feuter 123 Gmail Account, over 150,000 e-mails were recovered and reviewed. The search of the Feuter 123 Gmail Account led law enforcement officers to dozens of other e-mail accounts with which the Feuter 123 Gmail Account communicated, including augustino267@gmail.com (the “Augustino Gmail Account”) and ho.robby@gmail.com (the “Ho Robbie Gmail Account”). Within these e-mail accounts, law enforcement officers found more than 1.1 million unique credit card numbers, including information relating to numerous victims residing in New Jersey.

16. Also as part of the investigation, law enforcement officers executed a search warrant on a Facebook account belonging to defendant TRUONG (the “TRUONG Facebook Account”). The TRUONG Facebook account included photographs of defendant TRUONG, references to defendant TRUONG’s real name, and references to the conspiracy, including messages posted by Dump Purchasers to defendant TRUONG relating to stolen credit card

information that defendant TRUONG had sold to the Dump Purchasers.

17. Review of the TRUONG Facebook Account together with the e-mail accounts described above demonstrated that defendant TRUONG controlled the Feuter 123 Gmail Account, the Augustino Gmail Account, and the Ho Robbie Gmail Account.

a. First, the Augustino Gmail Account was used to register the TRUONG Facebook Account, and the Augustino Gmail Account was referenced in the TRUONG Facebook Account as a way to contact defendant TRUONG.

b. Second, the same telephone number was used to register the Ho Robbie Gmail Account as the TRUONG Facebook Account.

c. Third, law enforcement officers compared the internet protocol ("IP") information associated with the TRUONG Facebook Account with the Feuter 123 Gmail Account, the Augustino Gmail Account, and the Ho Robbie Gmail Account. This review revealed that the TRUONG Facebook Account and the three e-mail accounts were frequently accessed from the same IP addresses at the same times.

d. Fourth, on or about December 31, 2010, defendant TRUONG posted a specific quote on the TRUONG Facebook Account, which read:

"I wish you Health...
So you may enjoy each day in Comfort.
I wish you the love of friends and family...
And Peace within your heart.
I wish you the Beauty of nature...
That you may enjoy the work of God.
I wish you the wisdom to choose priorities...
For those things that really matter in life.
I wish you Generosity so you may share...
All good things that come to you.
I wish you Happiness and Joy...
And Blessings for the New Year.
I wish you the best of everything...
That you so well deserve."

Beginning on or about January 3, 2011, each and every e-mail sent from the Feuter 123 Gmail Account used this exact quote as a "footer," or signature, at the end of the e-mails.

18. The e-mails in the Feuter 123 Gmail Account, the Augustino Gmail Account, and the Ho Robbie Gmail Account demonstrated that TRUONG communicated with dozens of other e-mail accounts in furtherance of the conspiracy. More specifically, TRUONG obtained credit card and other personal identifying information relating to thousands of victims, and then sold this information to others.

19. Just a couple of examples are listed below:

a. On or about May 11, 2012, the Feuter 123 Gmail Account was used to send an e-mail with the stolen identity and credit information for several individual victims within the United States to a Dump Purchaser. The PII sent by the Feuter 123 Gmail Account including the credit card numbers, CVV numbers, expiration dates, first and last names, e-mail addresses, physical addresses, telephone numbers, and IP numbers of approximately five victims.

b. On or about September 21, 2012, the Ho Robbie Gmail Account was used to send an e-mail with several stolen identities and credit card information for individual victims within the United States to a Dump Purchaser. The PII sent by the Ho Robbie Gmail Account included the credit card numbers, CVV numbers, expiration dates, first and last names, e-mail addresses, physical addresses, and telephone numbers of approximately 4 victims.

20. The Feuter 123 Gmail Account, Ho Robbie Gmail Account, and Augustino Gmail Account also contained hundreds of e-mails from Dump Purchasers, each including an MTCN or equivalent wire transfer tracking number.

21. Moreover, the Feuter 123 Gmail Account included dozens of e-mails from Dump Purchasers, seeking to have credits added to their accounts on the Fraud Website (which, of course, shared the same name, "Matt Feuter," with the Feuter 123 Gmail Account). In these e-mails, Dump Purchasers included MTCNs that had been sent to the Co-Conspirators.

22. Law enforcement officers obtained all of the information associated with each MTCN, as part of this investigation, and determined where the money for these MTCNs was retrieved. This analysis revealed that the vast majority of the MTCNs sent to the Feuter 123 Gmail Account, the Ho Robbie Gmail Account, the Augustino Gmail Account, and numerous other e-mail accounts associated with the conspiracy were retrieved at a single Western Union location in or around Ho Chi Minh City, Vietnam. In total, the amounts retrieved from this Western Union from MTCNs associated with the conspiracy exceeded \$1.9 million.