

FILED
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA **AUG 17 2009**

CLERK U.S. DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA
BY  DEPUTY CLERK

UNITED STATES OF AMERICA
v.

JOSEPH HATFIELD

(Name and Address of Defendant)

CRIMINAL COMPLAINT

CASE NUMBER:
2:09 - MJ - 0242 DD

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 **February 12, 2009, through the present**, in **Sacramento County**, in the Eastern District of California defendant(s) did, (Track Statutory Language of Offense)

- ▶ **See Affidavit of Special Agent Shintaku attached hereto as Exhibit A and incorporated by reference in violation of Title 18, United States Code, Sections 1029(a)(2), (a)(3), and (a)(4).**

Continued on the attached sheet and made a part hereof.



SPECIAL AGENT KELLY SHINTAKU
UNITED STATES SECRET SERVICE

Sworn to before me, and subscribed in my presence

8/17/09

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 FOR CRIMINAL COMPLAINT

I, Kelly M. Shintaku, a Special Agent of the United States Secret Service, being duly sworn, depose and state as follows:

BACKGROUND

1. I am a Special Agent with the United States Secret Service (USSS). I have been so employed since July of 2004. I am currently assigned to the Sacramento Resident Office. I have received training at the Federal Law Enforcement Training Center in Glynco, GA and the USSS Training Facility in Beltsville, MD. In November 2005, I attended the Basic Investigations of Computer and Electronic Crimes Program (BICEP) and received my BICEP certification. As part of my duties, I investigate offenses involving access device fraud, wire fraud, and bank fraud. In these capacities, I have become familiar with the investigation and prosecution access device fraud, wire fraud and bank fraud, including the use of various criminal methods to perpetrate these frauds.

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

3. 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 card schemes involve a number of component activities consisting of:

- a) The illegal obtaining of/and trafficking in valid credit card account numbers, primarily Visa, MasterCard, and American Express credit card account numbers. The locations where these numbers are illegally obtained are commonly referred to as "points of compromise."
- b) At these "points of compromise," individuals intending to capture unauthorized credit card numbers use electronic devices commonly referred to as "skimmers" to capture credit card track data from legitimate credit card holders. These unauthorized credit card account numbers are later encoded and embossed onto counterfeit credit cards. Those individuals "skimming" commonly work at restaurants, gas stations and other stores where customers give their credit card to a cashier. Without the customer's knowledge and authorization, their credit card will be swiped with the skimmer. Information needed to counterfeit that credit card will thus be illegally obtained.
- c) The individual who captures legitimate credit card information onto a skimming may take that information and download it onto a computer to manufacture counterfeit credit cards or take it to someone who has the

capability to do so. They often use device making equipment, such as re-encoding machines. This "front-line" person often gets paid according to how many numbers they have captured on the skimmer.

- d) The number of "traffickers" between the front-line person and the counterfeit credit card manufacturer can vary. Usually each trafficker will be paid an increasing amount per credit card number on the skimmer until the skimmer is delivered to the credit card manufacturer. Sometimes, traffickers will receive counterfeit credit cards in addition to or in lieu of payment for the numbers.

CHARGES

4. I make this affidavit in support of the issuance of a Criminal Complaint and Arrest Warrant for the arrest of:

- **Joseph Hatfield, DOB 6/15/1982, FBI 897150NC9, CA DL # B9801925**

5. As described below, this affidavit sets forth probable cause to believe that **Joseph Hatfield** and others violated Title 18 U.S.C. Section 1029 (a)(2), (a)(3), (a)(4) – Access Device Fraud. Under Section 1029(a) (2), it is a felony to knowingly and with the intent to defraud, traffic in or use one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating more than \$1,000. Under Section 1029 (a)(3), it is a felony to knowingly and with intent to defraud, possess fifteen or more devices which are counterfeit or unauthorized access devices. Under section 1029(a) (4) it is a felony to knowing with intent to defraud, possess, produce, traffic in, have control or custody of, or possess device-making equipment.

6. Based on the facts set forth in this affidavit, I believe there is probable cause for a criminal complaint and warrant for the arrest of **Joseph Hatfield** for the violations set forth above.

7. 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) information received from third parties, such as bank investigators. Not all of the facts known to me are included herein; I have only included those facts necessary to show that probable cause exists to believe that **Joseph Hatfield** committed the federal violations.

STATEMENT OF PROBABLE CAUSE

8. The investigation into fraudulent activity by an individual, later identified as **Joseph Hatfield**, began on or about 02/12/2009, when Southwest Airline Baggage Claim representatives located an unmarked black suitcase that had no identification. Justin Clarke of Southwest explained that when the suitcase was to be loaded onto an airplane

destined for Phoenix, Arizona, Southwest officials noticed that the bag did not have baggage claim tag. Thus, the suitcase was returned to the Southwest Baggage Claim area, where it was inspected for owner information. The suitcase had no luggage identification tag on the outside. According to policy, Southwest opened the bag to determine ownership.

9. When the Southwest employees Michelle G. and Rose B. opened the suitcase they saw credit cards and a credit card reader/writer that would be used to make fraudulent credit cards. They spoke with their supervisor and contacted the Sacramento County Sheriff's Office.

10. On February 13, 2009, Sacramento County Sheriff's Deputy Starr, assigned to the Sacramento International Airport, located within the County of Sacramento, examined the contents of the bag. He inventoried the contents of the bag, noting that it contained a credit card reader/writer, a counterfeit CA driver license with the name "Adam Constant" and twenty five counterfeit credit cards that were each embossed with the name Adam Constant. He also found newly purchased clothing bearing tags from Macy's and Nordstrom.

11. Southwest Representative D'Lynne G. used her database to determine that there was no Southwest Airlines passenger named "Adam Constant" on the flight to Phoenix, Arizona. Thus, the suitcase was stored in the baggage claim area.

12. On February 13, 2009, Southwest Airline's customer service received a call from a person identifying himself as **Joseph Hatfield** who reported that his black suitcase had not arrived in Phoenix, Arizona on 2/12/09. **Hatfield** stated that he would pick up the bag upon his return to Sacramento.

8/17/09 Dad
Hatfield

13. Sacramento County Sheriff's Detective Eric Pahlberg conducted a search of the name **Joseph Hatfield** DOB 06/15/1982, CA DL B9801925. Detective Pahlberg determined that ~~Joseph Pahlberg~~ has been in the Sheriff's Known Persons File since 11/18/2006. Detective Pahlberg compared the photo on the counterfeited CA License in the name of "Adam Constant" recovered from the suitcase with a the CDL photo on file for **Joseph Hatfield**. Detective Pahlberg determined that the photo on the "Adam Constant" counterfeited CDL was that of **Joseph Hatfield**. Additionally, the phone number captured by Southwest Airlines from **Joseph Hatfield** was a phone number on record for **Hatfield** with the Sacramento County Sheriff's Office.

14. Justin Clarke, Customer Service Supervisor, Ground Ops., Southwest Airlines, confirmed that on 02/12/2009, **Joseph Hatfield** flew on Southwest Airlines from Sacramento, CA, to Phoenix, Arizona. Southwest Airlines records show that a person named **Joseph Hatfield** checked luggage at the curbside Skycap in Sacramento on 2/12/09.

15. On 2/12/09 at approximately 1936 hours, Sacramento International Airport surveillance video showed **Joseph Hatfield** as he checked in at the curbside Skycap.

16. On 2/18/09, Sacramento Sheriff's Deputy Detective Eric Pahlberg, picked up the suitcase and its contents from the Sacramento International Airport. He inspected the contents. He confirmed that the account numbers embossed on the cards were each encoded on the magnetic strip. He noted that each card lacked the security feature that the first four digits of the account number should have been pre-printed on the cards. He confirmed that each card was embossed with the name "Adam Constant" as the account holder.

17. Both Detective Pahlberg and I conducted a Bank Identification Number (BIN) check of the account numbers listed below. The first six digits of an account number correspond to the bank from which the access device was issued. In this case, the BIN search results show that the banks that issued the accounts did not match the banks that were printed on the cards. Further affirming the fact that these access device cards were counterfeit. The Account Numbers are as follows:

	Account Number (last 4 numbers)	Printed Bank	Printed Name	Bank from BIN
1	4182	Bank of America	Adam Constant	M&T Bank
2	4125	Bank One	Adam Constant	M&T Bank
3	2124	Chase	Adam Constant	GE Capital Financial Inc.
4	2520	Wachovia	Adam Constant	GE Capital Financial Inc.
5	2959	Providian National Bank	Adam Constant	GE Capital Financial Inc.
6	3205	Providian National Bank	Adam Constant	GE Capital Financial Inc.
7	4217	Washington Mutual	Adam Constant	FIA
8	4308	Chase	Adam Constant	FIA
9	9606	Providian National Bank	Adam Constant	FIA
10	9900	Providian National Bank	Adam Constant	FIA
11	8677	Providian National Bank	Adam Constant	FIA
12	3629	Wachovia	Adam Constant	FIA
13	3785	Wachovia	Adam Constant	FIA
14	7290	Washington Mutual	Adam Constant	Nordstrom FSB
15	1658	Bank of America	Adam Constant	First National Bank of Omaha
16	0456	Union Planters Bank	Adam Constant	Intrust Bank, National Association
17	0712	Union Planters Bank	Adam Constant	Intrust Bank, National Association
18	2389	Bank One	Adam Constant	None found (possibly mistyped for GE Cap
19	2121	Bank One	Adam Constant	JP MORGAN CHASE BANK

20	2617	UCB	Adam Constant	JP MORGAN CHASE BANK
21	9345	Citi	Adam Constant	COMERICA BANK
22	3214	Citi	Adam Constant	COMERICA BANK
23	4046	Union Planters Bank	Adam Constant	COMERICA BANK
24	8973	Union Planters Bank	Adam Constant	INTERNATIONAL BANK OF COMMERCE OF LAREDO
25	5007	Bank One	Adam Constant	INTERNATIONAL BANK OF COMMERCE OF LAREDO

Analysis of Fraudulent/Counterfeited Credit Cards and Purchases

18. Detective Pahlberg contacted Rohna N. of Intrust Bank and determined that account 0712 (card # 17 above) was issued by Intrust Bank. Detective Pahlberg determined the following fraudulent purchase transactions had been reported: Nordstrom, 02/12/2009, \$217.66 and Macy's, Arden Fair Mall, 02/12/2009, \$165.40.

19. Based on this information, Detective Pahlberg contacted Wade M., Loss Prevention, Nordstrom. McNally provided the electronic sales journals showing **Joseph Hatfield** attempt to use account number 2389 to make a purchase at the Nordstrom at Arden Fair Mall, located within the County of Sacramento. The card was declined. **Hatfield** presented a second card with account number 0712 (card #17 above) to purchase a pair of jeans on 02/12/2009 at 1541 hours for \$217.66. The transaction was successfully completed. A search of Nordstrom records indicates that the customer information for the alteration ticket associated with this transaction shows the customer as Adam Constant. The jeans matched a pair found in the black suitcase. In addition, surveillance video from Nordstrom shows the customer completing the purchase for the jeans was **Joseph Hatfield**.

20. Detective Pahlberg contacted Loss Prevention Manager for Macy's at the Arden Mall in Sacramento, Michelle Z. Michelle Z. provided the electronic sales journal for a transaction on 2/12/09 at 1605 hours. The transaction shows **Joseph Hatfield** using account number 0712 (card #17 above) to purchase a DKNY sweater and a bottle of perfume in the amount of \$165.40. The sweater and perfume matched items that were in the black suitcase. In addition, surveillance video from Macy's shows the customer completing the purchase for the items to be **Joseph Hatfield**.

21. Detective Pahlberg contacted Assistant VP of Financial Intelligence for Comerica Bank, Jennifer M. Jennifer M. reported that 9345 (card #21 above) was a valid card number issued by Comerica Bank and not Citibank. Jennifer M. stated the following fraudulent transactions occurred on 2/11/09:

- Wal-Mart - \$424.66
- Safeway - \$430.59

- Safeway - \$425.49
- Walgreens - \$463.59

22. Based on this information, Detective Pahlberg contacted the Loss Prevention Manager for Walgreens Denver Floyd and the Walgreens Store Manger Anthony G.. Walgreens Store Manger Giannini provided the electronic sales journal and surveillance video related to the transaction on card number 9345 (card #21 above) on 2/11/09 at Walgreens. Upon viewing the surveillance video, Detective Pahlberg observed **Joseph Hatfield** using account 9345 (card #21 above) to purchase four \$100 Visa gift cards and other merchandise at the Walgreens store located at 6325 Fair Oaks Blvd, Carmichael, CA

23. On 7/1/09, Detective Pahlberg and other local law enforcement from the Sacramento Hi-Tech Crimes Task Force executed at State of California issued Warrant to Search **Joseph Hatfield** and 5951 Riverside Blvd, #211, Sacramento, CA 95831, among other people, places, and things.

24. During the execution of the State Search Warrant, Officers and Detectives recovered in excess of 100 Access Devices – some were compromised by fraudulent transactions and some were re-encoded in the same manner set forth above. Some of the cards had the name “Adam Constant” embossed on the front. These cards were again checked by Officers and determined to be counterfeit.

25. Detective Clausen of the Hi-Tech Crimes Task Force recovered a Mastercard Logo card bearing number 2070 with the name Adam Constant embossed on the front. When Detective Clausen examined the card, he noted that the card lacked security features, to include, a four digit BIN number, a Mastercard hologram, a three digit card validation code. He also noted that the front of the card indicated it was issued by Bank One. However, when he conducted a BIN check, he determined the card number was issued by the International Bank of Commerce in Laredo, TX.

26. Based on this information, Detective Clausen contacted the bank and spoke with Fraud Investigator Julia Humphries. Humphries advised the card number was a valid International Bank of Commerce in Laredo number. She stated that the account was closed after a receipt of fraudulent activity on the account. Humphries stated this was a business account and the name Adam Constant was not associated with the account.

Conclusion

27. Based on my training and experience in conducting access device fraud investigations, I believe that the defendant’s conduct affected interstate commerce. Many of the stores he entered in which he used the counterfeit access device card to make purchases conduct business on a national level. As a result, 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. The transactions route through a complex network of terminals and databases which reside outside of the state of California. For example, the counterfeit access device card which

was issued by the International Bank of Commerce in Laredo, TX, is a bank which operates outside the state of California. It has branches throughout Texas and Oklahoma. Comerica Bank which issued the access device number used in the fraudulent transactions set forth in paragraphs 19 & 20, is a national financial institution which is headquartered in Dallas, TX. It conducts business throughout the nation.

28. In addition, based on my knowledge, training, and experience, **Joseph Hatfield** is extremely sophisticated in the art of access device fraud. He had credit cards that were embossed with compromised access device numbers. He had credit cards that were encoded on the magnetic strip to match the front of the card which shows that the cards were made using a magnetic encoding machine and embossing machine. In addition, **Joseph Hatfield** had a counterfeit California Driver's License which bore his photo but was in the name of Adam Constant. Adam Constant is the name which corresponds to the name on the counterfeit access device cards.

29. Based on my knowledge, training, and experience, I know that devices such as the card reader/writer found in the black suitcase recovered at the Sacramento International Airport which belonged to **Joseph Hatfield** can be used to re-encode data located on the magnetic strip.

30. Based on my knowledge, training, and experience, I know that the fraudulent charges posted to the access device number accounts listed above are in excess of \$1000.00. I know based on surveillance photos, **Joseph Hatfield's** possession of the counterfeit access devices in his black suitcase and in the name of Adam Constant, and the counterfeit CA DL in the name of Adam Constant but bearing a photo of **Joseph Hatfield's** which was also located in the black suitcase; that **Joseph Hatfield** was the one using various counterfeit access device numbers listed above to purchase merchandise and gift cards at stores.

31. Based on the foregoing, I respectfully submit that there is probable cause to believe **Joseph Hatfield** violated Title 18 U.S.C. Section 1029 (a)(2), (a)(3), (a)(4) – Access Device Fraud. Under Section 1029(a) (2), it is a felony to knowingly and with the intent to defraud, traffic in or use one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating more than \$1,000. Under Section 1029 (a)(3), it is a felony to knowingly and with intent to defraud, possess

///

///

///

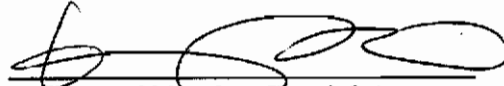
///

///


fifteen or more devices which are counterfeit or unauthorized access devices. Under section 1029(a) (4) it is a felony to knowingly with intent to defraud, possess, produce, traffic in, have control or custody of, or possess device-making equipment.

I therefore request the Court grant me authorization to arrest via Criminal Complaint **Joseph Hatfield DOB 6/15/1982, FBI 897150NC9, CA DL # B9801925.**

I swear under penalty of perjury that the above facts are true and correct to the best of my knowledge and belief.


Kelly M. Shintaku, Special Agent
United States Secret Service

Reviewed and approved as to form


Robin Taylor
Assistant U.S. Attorney

Subscribed and sworn to before me this 17th day of August 2009, at Sacramento, California.


Honorable Dale A. Brozd
United States Magistrate Judge