

UNITED STATES DISTRICT COURT

District of Arizona

AUSA

In the Matter of the Seizure of  
(Address or brief description of property or pre-  
mises to be seized)

The Entire Monetary Balance of the Prepaid Cards  
at The Bancorp Bank Identified in Attachment A1

The Bancorp Bank  
405 Silverside Road, Suite 105  
Wilmington, Delaware 19809

APPLICATION AND AFFIDAVIT  
FOR SEIZURE WARRANT

Case Number: 08-3397MB

I, Michael P. Fleischmann, being duly sworn depose and say:

I am a Special Agent of the Internal Revenue Service - Criminal Investigation and have reason to believe that in the District of Arizona there is now certain property which is subject to forfeiture to the United States, namely (describe the property to be seized)

The Entire Monetary Balance of the Prepaid Cards at The Bancorp Bank Identified in Attachment A1

which is (state one or more bases for seizure under the United States Code)

Property which constitutes or is derived from proceeds traceable to any specified unlawful activity as defined in 18 U.S.C. §§ 1956(C)(7) and 1961(1), and a conspiracy to commit such offenses; and is subject to seizure pursuant to 18 U.S.C. §§ 981(a)(1)(C) and 982, and 28 U.S.C. § 2461.

The facts to support a finding of Probable Cause for issuance of a Seizure Warrant are as follows:

See attached Affidavit incorporated by reference herein.

Continued on the attached sheet and made a part hereof.  Yes  No

Approved by AUSA Reid Pixler



Signature of Affiant

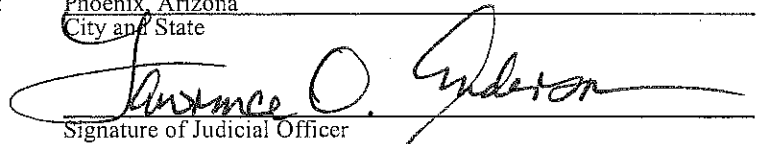
Sworn to before me, and subscribed in my presence

August 22, 2008  
Date

at

Phoenix, Arizona  
City and State

LAWRENCE O. ANDERSON  
Name and Title of Judicial Officer  
U.S. MAGISTRATE JUDGE

  
Signature of Judicial Officer

ATTACHMENT A1

The Bancorp Bank  
405 Silverside Road, Suite 105  
Wilmington, Delaware 19809

Routing Number	Account Number
031101169	9200100023411
031101169	9200100023494
031101169	9200100036900
031101169	9200100038294
031101169	9200100038302
031101169	9200100111745
031101169	9250100010315
031101169	9250100010323
031101169	9250100114679
031101169	9250100117284
031101169	9250100117292
031101169	9250100119876
031101169	9250100119884
091409568	9200100020045
091409568	9200100020359

AGENT

AFFIDAVIT  
AFFIDAVIT IN SUPPORT OF SEIZURE WARRANTS

INTRODUCTION

Your affiant, Michael P. Fleischmann, Special Agent with the Internal Revenue Service - Criminal Investigation (IRS-CI), Phoenix Field Office, being duly sworn and deposed, states the following:

1. Your affiant is submitting this affidavit in support of an application seeking the issuance of seizure warrants, in connection with a joint IRS-CI, Federal Bureau of Investigation (FBI), and United States Postal Inspection Service (USPIS) investigation for the items to be seized set forth in respective Attachments A1-A6, hereby incorporated by reference herein. This investigation has resulted in the issuance of search warrants specifically including the following locations:

- a. 431 El Camino Real; Apartment 1122; Santa Clara, California, 95050
- b. Storage Unit No. A-47, located at CBD Indoor Mini, 570 Cinnabar Street  
San Jose, California 95110

This investigation, including evidence obtained as the result of these searches, has lead to the discovery of the items to be seized listed in respective Attachments A1-A6 which represent property, real or personal, which constitutes or is derived from proceeds traceable to specified unlawful activity as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1) or a conspiracy to commit such offenses and are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C). As an aid to the consideration of this Affidavit, Attachment B - Description of Acronyms, is also being provided and is hereby incorporated by reference herein.

2. Your affiant has been actively involved in the investigation of a yet to be fully identified individual who has assumed the name Steven Travis Brawner, a.k.a. Travis Rupard, a.k.a. Patrick Stout, and a.k.a. the Hacker (herein after the "Hacker"); and others yet unknown. The individual is presently in federal custody and has chosen to not provide law enforcement with his true name. However, based upon analysis of his fingerprints he has been associated with the name of Daniel Rigmaiden who has a criminal history in California which will be detailed below.

a. The information contained in this affidavit is based on your affiant's personal knowledge, information your affiant received from other law enforcement officials assisting in the investigation, and information your affiant has gathered from other sources as noted throughout this affidavit. This affidavit does not purport to set forth all of your affiant's knowledge or efforts with respect to the investigation of this case.

b. Your affiant previously submitted multiple affidavits in support of prior search warrants for the above residential address of 431 El Camino Real; Apartment 1122; Santa Clara, California, 95050. Magistrate Judge Howard R. Lloyd, Northern District of California, San Jose Division, authorized warrant No. 08-70460 (HRL) on July 30, 2008, which permitted the initial entry into the premises. Magistrate Judge Patricia V. Trumbull, Northern District of California, San Jose Division, authorized a second warrant on August 4, 2008, warrant No. 08-70503 (PVT), which permitted the seizure of additional items from the subject apartment. During the course of the search of the subject apartment, the location of the above-noted storage unit was discovered. Based upon this additional information, another search warrant was obtained from Magistrate Judge Patricia V. Trumbull on August 4, 2008, warrant No. 08-70502 (PVT), for the storage unit.

c. A grand jury in Phoenix, Arizona, has returned a sealed felony indictment against Steven Travis Brawner, a.k.a. Travis Rupard, a.k.a. Patrick Stout, and an arrest warrant has been executed, in case number CR-08-814-PHX-DGC.

3. IRS-CI, FBI, and the USPIS are presently investigating the "Hacker" and others known and unknown for possible violations for the following criminal statutes:

- a. 18 U.S.C. § 286 – Conspiracy to Defraud the Government;
- b. 18 U.S.C. § 287 – False, Fictitious or Fraudulent Claims;
- c. 18 U.S.C. § 371 – Conspiracy;
- d. 18 U.S.C. § 1028 – Fraud Related to Identity Information;
- e. 18 U.S.C. § 1028A – Aggravated Identity Theft;
- f. 18 U.S.C. § 1029 – Fraud with Access Devices;
- g. 18 U.S.C. § 1341 – Mail Fraud;

- h. 18 U.S.C. § 1343 – Wire Fraud;
- i. 18 U.S.C. § 1030 – Computer Abuse and Fraud;
- j. 18 U.S.C. § 981(a)(1)(C) Forfeiture of property, real or personal, which constitutes or is derived from proceed traceable to any specified unlawful activity as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 961(1) or a conspiracy to commit such offenses;
- k. 28 U.S.C. § 2461.

There is probable cause to believe that the “Hacker”, has committed the above mentioned offenses collectively hereinafter referred to as “the Specified Federal Offenses;”

#### AFFIANT’S BACKGROUND AND EXPERIENCE

4. Your affiant is a Special Agent with IRS-CI and has been so employed since March 2005. As a special agent with IRS-CI, your affiant’s duties and responsibilities include conducting criminal investigations of individuals and business entities that have allegedly violated federal criminal statutes set forth in Titles 18, 26, and 31 of the United States Code.

5. Your affiant has a Bachelor of Science in Business Administration in Finance and Accounting from the University of Arizona. Your affiant graduated from the Criminal Investigator Training Program and the IRS-CI Special Agent Basic Training Program at the Federal Law Enforcement Training Center, Glynco, Georgia, which encompassed detailed training in conducting criminal and financial investigations. Your affiant is familiar with IRS-CI procedures in conducting search warrants and has participated in the execution of multiple search warrants for financial records.

6. Your affiant is a Certified Public Accountant (CPA) in the State of Arizona.

7. In order to gain additional information regarding fraudulent income tax refund schemes, your affiant consulted IRS-CI Special Agent Denise Medrano. Special Agent Medrano has been a special agent with IRS-CI since September 2001, and has participated in numerous criminal investigations relating to financial crimes. Special Agent Medrano was assigned as the Phoenix Field Office Questionable Refund Program (QRP) Coordinator from 2005 through 2007. As the QRP Coordinator, she received

ongoing specialized training with respect to the identification and investigation of fraudulent tax refund schemes.

### THE SCHEME

8. The investigation in this matter is a joint investigation involving IRS-CI, FBI, and the USPIS. The investigation to date has revealed the existence of a sophisticated scheme to fraudulently obtain tax proceeds filed in the name of innocent third parties and deceased individuals, and illegally obtain the proceeds from these tax returns. The primary subject of this investigation, the "Hacker," operated in the United States and was involved in acquiring identity information of deceased and living individuals, including their social security numbers, and using that information to conduct a bulk tax filing scheme, and directing the deposit of the proceeds of those fraudulent tax returns to bank accounts and debit cards where the funds could be accessed by the "Hacker" and co-conspirators.

9. For tax year 2006, refunds totaling approximately \$1,112,040.00 were falsely claimed via these electronically filed returns. Based on the significant similarities associated with the IP addresses, return format, and e-mail addresses, the IRS Fraud Detection Center located in Austin, Texas (AFDC) identified approximately 1,272 returns, 175 IP addresses, and 73 bank accounts which are believed to be linked to this scheme for tax year 2007. As of June 26, 2008, refunds totaling approximately \$2,133,824.00 have been falsely claimed via these electronically filed returns for the 2007 tax year.

#### A. Electronic Filing of Income Tax Returns

10. The Internal Revenue Service (IRS) encourages taxpayers to prepare and electronically file (e-file) their Federal income tax returns. Taxpayers can submit their returns via e-file through authorized IRS e-file providers. Each authorized IRS e-file provider is assigned one or more Electronic Filing Identification Numbers (EFIN), which the IRS uses to identify and monitor e-file provider activity. The IRS Electronic Tax Administration (ETA) administers the e-file program.

11. The Free File program is a free federal tax preparation and electronic filing program for eligible taxpayers developed through a partnership between the IRS and the Free File Alliance LLC, a group of private sector tax software companies. Since Free File's debut in 2003, more than 15.4 million returns have been prepared and e-filed through the program. Free File allowed taxpayers with an Adjusted Gross Income (AGI) of \$52,000.00 or less in 2006, and \$54,000.00 or less in 2007, to e-file their federal tax returns for free. Approximately 70 percent of all taxpayers (95 million taxpayers) are eligible to electronically file their income tax returns under the Free File program.

12. Many e-file providers offer home use web-based tax preparation software applications. The application allows the end-user to self-prepare a tax return on their home computer and electronically transmit the tax return via the Internet by means of a personal computer and modem. After the e-file provider receives the information from the end-user, the e-file provider electronically files the tax return with the IRS, thereby completing the electronic filing process. In order for the end-user to connect and transmit an e-filed return over the Internet, the end-user must have access to the Internet via an Internet Service Provider (ISP).

13. Once the customer obtains an IP address and logs onto the Internet, each customer can utilize the web-based application offered by e-file providers to transmit their tax return information. When the e-file provider transmits a tax return to the IRS, they are required to include the IP information of the customer, consisting of the IP address, IP Date, IP Time and IP Time Zone. The IP information can normally be used to trace back to the individual filing the return.

#### B. Carter Tax and Accounting

14. In May 2007, IRS-CI Phoenix Field Office became aware of questionable activity involving an account in the name of CARTER TAX & ACCOUNTING LLC. Ransom Marion Carter was the authorized signer for the account. Between May 22 and May 25, 2007, 75 U. S. Treasury electronic credits totaling approximately \$129,364.00 labeled "tax refund" were posted to the account. On May 26, 2007, Ransom Carter withdrew \$24,500.00 from the account and purchased two cashier's checks with the funds.

15. On June 5, 2007, EFile Tax Returns, Inc., an authorized IRS e-file provider and member of the Free File Alliance LLC, contacted the ETA, regarding a large volume of returns filed through its website using what appeared to be an automated process. EFile Tax Returns, Inc., identified approximately 200 returns for tax year 2006 and 400 for tax year 2005, which appeared to be related to this automated scheme.

16. The AFDC researched the returns identified by EFile Tax Returns, Inc., and identified Ransom Carters' Compass Bank account as one of the accounts destined to receive refunds claimed on those returns. A search was conducted for all electronically filed returns with refunds destined for the above referenced Compass Bank account. Approximately 209 returns, claiming over \$339,000.00 in refunds, were identified bearing this particular bank account number and routing number.

17. Analysis of the subject returns revealed multiple fraudulent returns filed from single IP addresses within short time periods, indicating the use of some type of computerized bulk filing system. Based on analysis of the IP addresses, it appeared the returns were filed from multiple locations around the United States. However, the real IP address was apparently hidden; possibly by utilizing illicit proxies or intermediary

computers to submit the returns and prevent the identification of the individual filing the returns.

C. CI 1 and CI 2

18. In January 2008, an individual pending unrelated felony fraud charges, in the Superior Court of Arizona, agreed to provide information to IRS-CI and USPIS in order to potentially gain consideration with respect to his/her pending state charges. This individual will hereinafter be referred to as CI 1. To date, based on information provided by IRS-CI, your affiant believes CI 1 to be credible and his/her information has been corroborated and documented through independent investigation, recorded telephone calls, and recorded e-mails. In a debriefing, CI 1 advised that an individual he/she knew only by his/her street name (hereinafter SN 1) and another unknown individual CI 1 referred to as the "Hacker", had been operating an automated system to file fraudulent tax returns using the names and Social Security Numbers of deceased individuals.

19. CI 1 further stated Ransom Carter's receipt of refunds through the Compass Bank account Carter established in 2006, in the name of CARTER'S TAX & ACCOUNTING LLC, represented a successful test run of the scheme. CI 1 said SN 1 and his associates intended to pursue the same scheme for the 2008 filing season (for income earned in 2007). CI 1 also stated he/she believed that during prior years, going back as far as 2005, the fraudulent tax returns had directed refunds be credited to pre-paid debit cards.

20. Based on the information provided by CI 1 and CI 1's agreement to work as a confidential informant on behalf of law enforcement, an undercover operation was initiated by IRS-CI and USPIS to determine the true identity of SN 1, the "Hacker" and their associates, and gather evidence concerning the nature and extent of the bulk filing scheme. Per SN 1's instructions to CI 1, IRS-CI and USPIS, with the assistance of CI 1, established an undercover shell business and a related undercover bank account at Meridian Bank ("Meridian undercover bank account").

21. In the course of the scheme, SN 1 asked CI 1 to open a safe-mail.net e-mail account. The purported purpose of using this e-mail service was to avoid detection. In February 2008, CI 1 e-mailed the account number and routing numbers for the Meridian undercover bank account to SN 1. SN 1 subsequently advised CI 1 the "Hacker" would begin to e-file fraudulent returns which directed refunds to the Meridian undercover bank account.

22. Throughout the initial stages of the undercover operation, CI 1 communicated with SN 1 via telephone and his safe-mail.net account. Incoming e-mails from SN 1 revealed his IP address, which an internet directory service revealed is owned



by Comcast Cable Communications, Inc. In late February 2008, in response to a Grand Jury subpoena, Comcast reported the IP address was leased by SN 1 at SN 1's residential address. It was determined SN 1 was, in fact, the subscriber.

23. In early March 2008, the AFDC identified 72 electronically filed tax returns with refunds, totaling approximately \$117,496.00, destined for the Meridian controlled undercover bank account. Over \$62,000.00 was deposited to the Meridian undercover bank account in mid-March 2008.

24. After the aforementioned deposits, CI 1 contacted SN 1 and informed him money had been deposited in the account. CI 1 told SN 1 he/she would withdraw \$9,000.00 in mid-March 2008 and ship it to SN 1 on March 18, 2008, via FedEx. CI 1 further advised he/she would withdraw money from the account every week and ship \$9,000.00 to SN 1 every other week. The withdrawn money not "shipped" was to be CI 1's cut. SN 1 provided CI 1 with the name and address where the money was to be shipped. SN 1 also told CI 1 to provide the tracking number so he could monitor the shipment of the package.

25. In late March 2008, an IRS-CI agent withdrew \$9,000.00 in currency from the Meridian undercover bank account and on April 1, 2008, the \$9,000.00 was shipped overnight priority mail to SN 1. For the first and second shipments, agents witnessed SN 1 leave his/her personal residence, arrive at the destination of the package delivery, leave the destination with a package appearing to be the undercover package, and return to his/her residence.

26. On April 14, 2008, a third shipment in the amount of \$9,000.00 currency was sent overnight priority mail to SN 1. On April 15, 2008, SN 1 was arrested when leaving the destination location carrying the third and final shipment of \$9,000.00 currency. The second and third of these shipments were in violation of 18 U.S.C. § 1341. All three shipments are proceeds of specified unlawful acts, that is: 18 U.S.C. §§ 1028 and 1343, and subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

27. After his/her arrest on related federal charges, SN 1 agreed to act as a confidential informant and assist law enforcement in identifying and apprehending the "Hacker" and will be hereinafter referred to as CI 2. CI 2 advised he/she has never met the "Hacker" in person and had never spoken to the "Hacker" telephonically or via Voice Over Internet Protocol (VOIP). CI 2 maintained ongoing contact with the "Hacker" via encrypted e-mail using a safe-mail.net e-mail account. Safe-mail.net is located in the country of Israel. CI 2 also indicated the "Hacker" previously operated a website ([www.fakeid.tv](http://www.fakeid.tv)) where the "Hacker" sold fake California driver's licenses.

D. Controlled Delivery of \$68,000.00

28. The "Hacker" was led to believe CI 2 had an associate, "Daniel," who works in the banking industry and was willing to assist CI 2 in moving the "Hacker's" fraudulent tax return proceeds from the Meridian undercover bank account quickly and without detection.

29. On April 17, 2008, CI 2 sent an encrypted e-mail to the "Hacker" explaining he/she had received an additional \$9,000.00 in currency from the Meridian undercover bank account, and was expecting to receive an additional \$75,000.00 by April 22, 2008. CI 2 inquired how the "Hacker" wanted his cut (\$68,000.00) of the money. The "Hacker" provided CI 2 detailed instructions regarding how to physically wash \$68,000.00 in currency with lantern fuel to remove any drug or explosive residues which might cause a detection dog to alert on the package. CI 2 was further instructed to double vacuum seal the currency, to place the sealed currency in the cavity of a toy, gift wrap the toy so it appeared to be a present, attach a birthday card for a dying child, package it for overnight FedEx delivery, and have the package held for pickup at the destination location.

30. Additionally, the "Hacker" informed CI 2 he would send a courier, armed with an AR-15 in a duffle bag, to pick up the package. The "Hacker" added the courier would be prepared to shoot anyone who attempted to arrest him while he was in possession of the package. The "Hacker" informed CI 2 he would send details of the operation in an encrypted format to the media before the pickup date. If law enforcement conducted a sting on the pickup, the "Hacker" would then provide information to the media to decrypt his prior message. The "Hacker" advised this would make law enforcement look bad by proving that law enforcement knew the potential for violence at a public place before conducting the sting.

31. On May 5, 2008, the "Hacker" sent CI 2 an encrypted e-mail with directions to send a package containing \$68,000.00 in currency to Patrick Stout, to a commercial address in Palo Alto, California, and to arrive the morning of May 6, 2008. This location was determined to be a FedEx/Kinko's retail store open 24 hours a day. Prior to the shipment, CI 2 provided the "Hacker" with the undercover package's tracking number via another encrypted e-mail.

32. The package containing \$68,000.00 in currency was delivered to the FedEx/Kinko's store on May 6, 2008. On May 7, 2008, at approximately 5:00 am, an unknown white male, average build, wearing a dark jacket with a hood, who appears to be in his twenties and presented identification in the name "Patrick Stout," was observed entering the back entrance of the Fed Ex/Kinko's on foot and retrieving the package. The male carried the box to a nearby corner where he ripped open the box, removed the contents containing the currency and discarded the packaging in a nearby dumpster. The unknown male proceeded toward a nearby train station. Agents

conducting surveillance were unsuccessful in efforts to identify the unknown male or follow the unknown male to his final destination. During the execution of the search warrants for the "Hacker's" apartment and storage unit, a fake California driver's license bearing the "Hacker's" photograph and the name Patrick Stout was found along with clothing that appeared to be the clothing worn by the person who picked up the package on May 7, 2008.

33. On or about May 8, 2008, the "Hacker" e-mailed CI 2 and confirmed receipt of the money. The "Hacker" indicated in his e-mail the money was picked up by a third party. The "Hacker" advised CI 2 that the courier who retrieved the package believed that he was being followed by police. According to the "Hacker", the courier advised he noticed a "car circling around the area after he left with the driver acting like he was looking for someone. There were also some suspect characters walking around on foot 'trying to follow him' so he said he did a 180 and 'came right at them' but they did not do anything about it. The "Hacker" then advised that the courier was "likely just really paranoid."

34. Investigation of the name "Patrick Stout" led the investigation team to a Post Office Box located in Sacramento, California, that was opened under the name "Patrick Stout" on November 21, 2007 and was closed on May 31, 2008. Investigation of the information provided to open the Post Office Box has determined that the California Driver's License number used to open the Post Office Box was actually assigned to a female with a different name in California.

a. In addition, approximately two weeks after the "Hacker's" receipt of the \$68,000 controlled delivery at the FedEx/Kinkos located in Palo Alto, California, an account was opened with Bullion Direct in the name of "Patrick Stout". According to its website, Bullion Direct holds itself out to be an online source to buy and sell precious metals, including gold, silver, platinum and palladium coins and bars. Bullion Direct ships precious metals to customers via UPS/FedEx or United States Postal Service registered mail. The investigation has further revealed an unknown individual used a debit card, which was linked to fraudulent tax refunds, to purchase United States Postal Money Orders. The postal money orders were then used to purchase gold through Bullion Direct for the "Patrick Stout" account. Two separate shipments of gold, totaling approximately \$18,000, were mailed via FedEx to "Patrick Stout", to the same FedEx/Kinkos location as the \$68,000 controlled delivery.

35. CI 2 and the "Hacker" soon thereafter agreed "Daniel" would withdraw all of the money from the Meridian undercover bank account and deposit the money in an account controlled by "Daniel." CI 2 informed the "Hacker", "Daniel" was able to make very large one-time withdrawals only at the end of each quarter, the next quarter ending June 30, 2008.

36. On May 16, 2008, CI 2 informed the "Hacker" that "Daniel" had moved \$364,260 (the remaining cut for CI 2 and the "Hacker") from the Meridian undercover bank account into another bank account believed to be controlled by "Daniel." CI 2 provided a Bank of America routing number and undercover account number to the "Hacker" where future tax refunds could be deposited. Per the "Hacker"'s request, the funds in the Bank of America account would be swept weekly into another account controlled by "Daniel."

37. On May, 27, 2008, the "Hacker" informed CI 2 he had filed approximately 200 additional fraudulent tax returns seeking refunds destined for the new undercover account located at Bank of America. As of June 26, 2008, the AFDC identified 249 fraudulent tax returns claiming approximately \$404,382 destined for this account. The returns were filed from multiple IP addresses.

E. Travis Rupard

38. On March 1, 2008, a fraudulent tax return for James A. Johnson (xxx-xx-3549) was filed with the Internal Revenue Service using IP address 75.208.105.186, with a refund amount of \$2,099.00 destined for a debit card issued by Galileo Processing (See paragraph 88). This debit card account was linked by the investigation team to the Meridian undercover bank account through analysis of connected IP addresses and bank accounts. The account holder is listed as James Johnson (xxx-xx-8024) with an address in Alameda, California. The AFDC identified additional tax returns electronically filed claiming refunds destined for same account as follows:

Date	Name	Social Sec #	City, State	Refund	IP Address
01/19/08	James L. Johnson	xxx-xx-5366	Culver City, CA	\$2,397	24.205.80.123
02/07/08	James Johnson	xxx-xx-4889	Bentonville, AR	\$2,437	76.195.145.182
02/29/08	James B. Johnson	xxx-xx-1692	Rocky Ridge, MD	\$717	67.82.193.84
02/29/08	James B. Johnson	xxx-xx-8023	Culver City, CA	\$1,384	76.250.136.120
03/01/08	James D. Johnson	xxx-xx-7537	North Wilkesboro, NC	\$2,249	68.36.156.35

03/01/08	James C. Johnson	xxx-xx-4542	Chicago, IL	\$1,061	68.36.156.35
----------	------------------	-------------	-------------	---------	--------------

39. On March 1, 2008, a fraudulent tax return for Michael S. Deshields (xxx-xx-8782) was filed with the Internal Revenue Service using IP address 75.208.105.186, with a refund amount of \$1,988.00 destined for a debit card issued by NetSpend (See paragraph 87). This debit card account was linked by the investigation team to the Meridian undercover bank account through analysis of connected IP addresses and bank accounts. The account holder is listed as Barbara L. Piper (xxx-xx-8344) with an address in Detroit, Michigan. The AFDC identified three additional tax returns electronically filed claiming refunds destined for the same debit card account as follows:

Date	Name	Social Sec #	City, State	Refund	IP Address
01/22/08	Barbara Piper	xxx-xx-8344	Marion, IN	\$5,514	24.251.75.193
02/29/08	Arjuna Desilva	xxx-xx-6629	Phoenix, AZ	\$1,463	208.97.32.251
02/29/08	Banhdasack Detsadachanh	xxx-xx-5124	Lake Havasu City, AZ	\$1,861	68.36.156.35

40. On March 5, 2008, a tax return for Robert W. Galletly (xxx-xx-7628) was filed with the Internal Revenue Service using IP address 75.209.41.104, with a refund amount of \$1,093.00 destined for a debit card issued by Account Now (See paragraph 86). This debit card account was linked by the investigation team to the Meridian undercover bank account through analysis of connected IP addresses and bank accounts. The account holder is listed as Margaret Murray (xxx-xx-0901) with an address in Petersburg, Virginia. The AFDC identified three additional tax returns electronically filed claiming refunds destined for the same debit account number as follows:

Date	Name	Social Sec #	City, State	Refund	IP Address
01/17/08	Margaret Murray	xxx-xx-0901	Millville, NJ	\$3,907	68.44.96.153

03/05/08	Beth A. Gallamore	xxx-xx-5092	Phoenix, AZ	\$1,490	99.130.28.126
03/25/08	Justin P Hopper	xxx-xx-9313	West Chester, PA	\$980	24.61.51.52

41. On March 26, 2008, a tax return for Kevin Furman (xxx-xx-8975) from Eugene, Oregon, was filed with the Internal Revenue Service using IP address 75.209.101.132, with a refund amount of \$1,282.00 destined for the Meridian undercover bank account. Furman died on August 30, 1989.

42. Investigation revealed the IP addresses associated with the James Johnson, Michael Deshields, Robert Galletly, and Kevin Furman tax returns, are registered to Verizon Wireless. In response to a Federal Grand Jury subpoena, Verizon Wireless reported that IP addresses 75.208.105.186, 75.209.41.104, and 75.209.101.132 were utilized by a person who opened the account in the name of Travis Rupard, with Post Office Box 730031, San Jose, California, and telephone number (206) 666-3620. The above mentioned IP addresses were linked via the following mobile device number (MDN): (415) 264-9596. Verizon Wireless issued the Travis Rupard Broadband Access Card, with ESN 005-00717190, assigned telephone number (415) 264-9596 and Verizon Wireless account number 270691733, to the customer claiming to be "Travis Rupard" on May 23, 2006. This device will hereinafter be referred to as the "Travis Rupard Broadband Access Card." This device was also found during the recent search of the "Hacker's" apartment and was attached to a laptop computer.

43. USPS conducted an investigation of Post Office Box 730031 in San Jose, California and determined this PO Box was opened on March 31, 2006 and was closed on August 31, 2006. The application indicated an individual purporting to be Travis Rupard presented a California Driver's License, number D2740168 and a Student ID Card, and provided a physical address of 1780 Oakland Road, #17, San Jose, California, 95131. Further investigation showed the California Driver's License number is assigned to a female with a Bakersfield, California address. Based on information provided by the San Jose, California, Post Office, the address 1780 Oakland Road is a physical street address for the Leasing Offices of an apartment complex in San Jose. There are no apartment numbers or suite numbers associated with 1780 Oakland Road, San Jose, California.

44. CI 2 advised he/she had been involved with the "Hacker" in a number of fraudulent schemes over a period of several years and in the past he/she had had sent

money to the "Hacker" by sending it to e-gold account XXXX337. A Federal Grand Jury subpoena was issued for documents related to this account. Records show that this account was created on August 16, 2006, in the name of Sam Blat and Benjamin Cohan. Records corroborate that CI 2 sent the "Hacker" \$7,640 on August 17, 2006. The Sam Blat account sent money to an account in the name of Aaron Johnson on five occasions beginning on November 19, 2006 through December 22, 2006. On July 31, 2006, an account in the name of Travis Rupard, 6447 Ivy Lane, San Jose, California, 95129, e-mail address [travisrupard@safe-mail.net](mailto:travisrupard@safe-mail.net), telephone number (408) 252-1678, sent \$9.50 to the Aaron Johnson account. The name Aaron Johnson is listed as the account holder of a Southwest Bank Account used to receive fraudulent tax refunds. The "Hacker" recently asked CI 2 to inquire about the Southwest Bank Account with "Daniel" to determine if the "Hacker" could obtain proceeds in the account. The "Hacker" later advised CI 2 that he has been unable to withdraw the proceeds from the scheme out of this account.

#### F. Time Zones

45. On or about June 25, 2008, in response to an Order issued pursuant to 18 U.S.C. § 2703(d), Verizon Wireless provided IP transaction information related to the IP addresses utilized by the Travis Rupard account, and identified in Section E. Verizon Wireless reports connection times in Greenwich Mean Time (GMT). GMT was researched on [www.greenwichmeantime.com](http://www.greenwichmeantime.com). The website indicated that during Daylight Saving Time (DST), which began on Sunday, March 9, 2008, that Pacific Daylight Saving Time (PDST) for California, the suspected location of the "Hacker", is GMT - 7 hours. During DST, Arizona is on the same time as California.

#### G. IP transaction records for "Hacker" - CI 2 e-mails

46. On May 15, 2008, the "Hacker" sent CI 2 an e-mail from IP address 67.187.132.91 at 07:37:13 a.m. GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to the same IP address on the same date as early as 01:29:34 a.m. GMT and as late as 08:40:23 a.m. GMT, including multiple connections at 07:35 a.m. GMT, two connections at 07:36 a.m. and multiple connections at 07:37 a.m. GMT.

47. On May 16, 2008, the "Hacker" sent CI 2 an e-mail from IP address 212.62.97.23 at 05:38:25 a.m. GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to IP same address on the same date as early as 5:29:40 a.m. GMT and as late as 11:29:05 a.m. GMT, including multiple connections at 5:31 a.m. GMT and one connection at 5:32:07 a.m. GMT.

48. On May 17, 2008, the "Hacker" sent CI 2 an e-mail from IP address 81.27.4.177 at 02:32:23 a.m. GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to the same IP address on the same date as early as 12:20:10 a.m. GMT and as late as 06:06:10 a.m. GMT, including multiple connections at 2:23 a.m. GMT, a connection at 02:24:00 a.m. GMT and a connection at 02:32:28 a.m. GMT.

49. On May 18, 2008, the "Hacker" sent CI 2 an e-mail from IP address 80.73.48.232 at 17:00:28 GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to the same IP address on the same date as early as 12:39:12 p.m. GMT and as late as 5:07:37 p.m. GMT including multiple connections at 4:58 p.m. GMT and one connection at 5:00:30 p.m. GMT.

50. On May 19, 2008, the "Hacker" sent CI 2 an e-mail using e-mail address from IP address 67.187.132.91 at 4:00:38 a.m. GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to the same IP address as early as 3:28:45 a.m. GMT and as late as 5:58:36 p.m. GMT, including a connection at 3:50:10 a.m. GMT and a connection at 04:00:43 a.m. GMT.

51. On May 21, 2008, the "Hacker" sent CI 2 an e-mail from IP address 66.177.227.9 at 17:56:40 p.m. GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to the same IP address as early as 5:48:45 p.m. GMT and as late as 11:53:08 p.m. GMT, including one connection that lasted from 5:52:07 p.m. to 11:53:08 p.m. GMT.

52. On May 22, 2008, the "Hacker" sent CI 2 an e-mail using IP address 24.3.79.57 at 9:14:05 a.m. GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to the same IP address on the same date as early as 8:31:33 a.m. GMT and as late as 4:39:40 p.m. GMT, including one connection beginning at 9:13:47 a.m. GMT.

53. On May 23, 2008, the "Hacker" sent CI 2 an e-mail using IP address 24.3.79.57 at 01:00:29 a.m. GMT and at 03:05:11 a.m. GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to the same IP address on the same date as early as 12:29:43 a.m. and as late as 7:00:41 p.m. GMT, including two connections at 12:59 a.m. GMT, one connection at 1:00:36 a.m. GMT and multiple connections at 3:05 a.m. GMT.

54. On May 27, 2008, the "Hacker" sent CI 2 an e-mail using IP address 67.187.132.91 at 03:40:53 a.m. GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to the same IP address on the same date as early as 02:54:47 a.m. GMT and as late as 03:58:26 a.m., including multiple connections at 03:40 a.m. GMT.



55. On May 28, 2008, the "Hacker" sent CI 2 an e-mail using IP address 80.73.48.232 at 18:47:04 p.m. GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to the same address on the same date as early as 06:05:40 p.m. and as late as 07:34:21 p.m. GMT, including two connections at 06:45 p.m. GMT and one connection at 06:47:07 p.m. GMT.

56. On May 29, 2008, the "Hacker" sent CI 2 an e-mail using IP address 200.51.41.29 at 18:37:42 p.m. GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to the same IP address on the same date as early as 06:20:55 a.m. and as late as 09:53:54 p.m. GMT, including a connection at 06:37:41 p.m. GMT.

57. On May 30, 2008, the "Hacker" sent CI 2 an e-mail using IP address 85.181.29.196 at 22:44:30 p.m. GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to the same IP address on the same date as early as 10:41:36 p.m. GMT and as late as 10:57:42 p.m. GMT, including multiple connections at 10:44 p.m. GMT.

58. On June 1, 2008, the "Hacker" sent CI 2 an e-mail using IP address 98.194.41.225 at 02:02:20 a.m. GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to the same IP address on the same date as early as 01:39:17 a.m. and as late as 05:45:02 p.m. GMT, including multiple connections at 2:01 a.m. GMT and one connection at 02:02:27 a.m. GMT.

#### H. Undercover Meridian Bank Account Access and Gmail Access

59. CI 2 provided logon credentials to access the Meridian undercover bank account to the "Hacker". In order to access account information online, the "Hacker" utilized the username "Mike1," which is reserved for his exclusive use. Meridian Bank's online banking service requires a user to authenticate his or her identity when logging into an account from a computer not recognized by the bank. When this occurs, the user is challenged and must enter a one time security code. The "Hacker" received the one-time security code at Gmail account andersonsats@gmail.com.

60. On May 16, 2008, the "Hacker" attempted to logon to the Meridian undercover bank account from IP address 81.27.4.177. At 05:42:36 a.m., Arizona Time, the bank rejected the logon because the computer was not recognized and challenged the user. At 05:44:45 Arizona Time, after entering the one time security code and enrolling the computer, the "Hacker"'s login was authenticated. The "Hacker" accessed Account Summary and Account History."

55. On May 28, 2008, the "Hacker" sent CI 2 an e-mail using IP address 80.73.48.232 at 18:47:04 p.m. GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to the same address on the same date as early as 06:05:40 p.m. and as late as 07:34:21 p.m. GMT, including two connections at 06:45 p.m. GMT and one connection at 06:47:07 p.m. GMT.

56. On May 29, 2008, the "Hacker" sent CI 2 an e-mail using IP address 200.51.41.29 at 18:37:42 p.m. GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to the same IP address on the same date as early as 06:20:55 a.m. and as late as 09:53:54 p.m. GMT, including a connection at 06:37:41 p.m. GMT.

57. On May 30, 2008, the "Hacker" sent CI 2 an e-mail using IP address 85.181.29.196 at 22:44:30 p.m. GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to the same IP address on the same date as early as 10:41:36 p.m. GMT and as late as 10:57:42 p.m. GMT, including multiple connections at 10:44 p.m. GMT.

58. On June 1, 2008, the "Hacker" sent CI 2 an e-mail using IP address 98.194.41.225 at 02:02:20 a.m. GMT. Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to the same IP address on the same date as early as 01:39:17 a.m. and as late as 05:45:02 p.m. GMT, including multiple connections at 2:01 a.m. GMT and one connection at 02:02:27 a.m. GMT.

#### H. Undercover Meridian Bank Account Access and Gmail Access

59. CI 2 provided logon credentials to access the Meridian undercover bank account to the "Hacker". In order to access account information online, the "Hacker" utilized the username "Mike1," which is reserved for his exclusive use. Meridian Bank's online banking service requires a user to authenticate his or her identity when logging into an account from a computer not recognized by the bank. When this occurs, the user is challenged and must enter a one time security code. The "Hacker" received the one-time security code at Gmail account andersonsats@gmail.com.

60. On May 16, 2008, the "Hacker" attempted to logon to the Meridian undercover bank account from IP address 81.27.4.177. At 05:42:36 a.m., Arizona Time, the bank rejected the logon because the computer was not recognized and challenged the user. At 05:44:45 Arizona Time, after entering the one time security code and enrolling the computer, the "Hacker"'s login was authenticated. The "Hacker" accessed Account Summary and Account History."

61. On May 16, 2008, at 12:43:34 p.m. GMT, IP address 81.27.4.177 accessed the e-mail account andersonsats@gmail.com. This e-mail access is after the logon rejection yet before the successful logon to the Meridian undercover bank account by IP address 81.27.4.177. Verizon Wireless broadband access card connection records reported the Travis Rupard Account connected to IP address 81.27.4.177 multiple times on May 16, 2008 including connections during 12:42 p.m. 12:43 p.m. and 12:44 p.m. GMT.

62. On May 24, 2008, the "Hacker" attempted to logon to the Meridian undercover bank account from IP address 68.199.62.250. At 11:00:02 Arizona time, the bank rejected the logon because the computer was not recognized and challenged the user. At 11:01:34, Arizona Time, after entering the one time security code and enrolling the computer, the "Hacker"'s login was authenticated. The "Hacker" accessed Account Summary, Account History and a Check Image.

63. On May 24, 2008, at 06:00:36 p.m. GMT, IP address 68.199.62.250 accessed the e-mail account andersonsats@gmail.com. This e-mail access was after the logon rejection yet before the successful logon to the Meridian undercover bank account by IP address 68.199.62.250.

64. Verizon Wireless broadband access card connection records reported the Travis Rupard Account connected to IP address 68.199.62.250 multiple times on May 24, 2008, including connections during 6:00 p.m., 6:01 p.m. and 6:02 p.m. GMT.

I. Analysis of IP addresses used to file fraudulent tax returns

65. The IP Addresses logged for the 395 tax returns filed using the undercover bank account located at Meridian Bank were researched on an internet reference directory. A sampling of the IP addresses and ISP information is set forth below:

<b>IP Address</b>	<b>Internet Service Provider</b>	<b>No. of Returns</b>	<b>Subscriber</b>	<b>City &amp; State</b>
12.216.17.121	Media Com Communications	10	Janet Martin	Des Moines, IA
24.26.218.97	Time Warner Cable	21	Bruce Hicks	Belton, TX
24.17.47.176	Comcast Cable Communications Inc.	9	Gayle Johnston	Willow Springs, IL

67.168.17.7	Comcast Cable Communications Inc.	18	Derek Smith	Federal Way, WA
67.175.211.144	Comcast Cable Communications Inc.	2	Valerie Wachholz	Mundelein, IL
75.209.101.132	Verizon Wireless	1	Travis Rupard	San Jose, CA

66. Based on the analysis of the IP Addresses, it appears as if the returns were filed from multiple locations throughout the United States. However, due to the nature of the information contained in the returns, and the manner in which they were filed, it appears the real IP Address, or IP Addresses, were hidden, possibly by use of IP spoofing, IP anonymizer services, or utilizing a botnet to submit the returns. In order to gain additional information regarding these types of activities, your affiant consulted IRS-CI Special Agent Tracy Daun and FBI Special Agent Richard Murray. Special Agent Daun has been a special agent with IRS-CI since February 2001. She has participated in numerous criminal investigations relating to financial crimes, including but not limited to, income tax related crimes, money laundering, wire fraud, telemarketing fraud and mail fraud. Special Agent Daun expanded her expertise to include computer forensics, and computer crime scene investigations in January 2006, when she received training as a Computer Investigative Specialist (CIS) at the Federal Law Enforcement Training Center. She is trained in the execution of search warrants involving computers and related equipment, electronic data preservation, and the recovery, documentation and authentication of evidence. Special Agent Daun has taken computer related courses covering databases, spreadsheets, word processors, and other specialized software developed to assist with forensic analysis of digital data, digital evidence recovery, password detection, etc.

67. Special Agent Murray has been an FBI Special Agent since 1999 and has been assigned to the Phoenix FBI Cyber Squad since 2005. SA Murray has participated in investigations relating to computer crime including computer intrusions and fraud committed using computers. SA Murray has received over 350 hours of computer crime

training including, but not limited to topics on Internet investigations, networking, computer intrusion investigations, computer security and wireless technology.

68. Special Agents Daun and Murray have advised your affiant that using a proxy or intermediary computer can allow individuals to mask their true IP address and true identity and appear to be another computer. By using a proxy computer, an attacker makes it appear that his transmittal has come from another machine by sending and receiving communications through the proxy computer.

69. Special Agents Daun and Murray have advised your affiant that IP anonymizer services are internet based anonymization tools available to hide an individual's real identity. An Internet user may visit an anonymizer tool's website and complete all of their web browsing/actions through the site. Special Agent Daun is aware of multiple free anonymizing websites on the internet including Anonymouse, iphide.com, and Proxify.

70. Special Agents Daun and Murray have advised your affiant that the term botnet is generally used to refer to a collection of compromised computers (called zombie computers) running programs, under a common command and control infrastructure. A botnet's originator can control the group remotely. A botnet typically runs hidden. While most owners are oblivious to the infection, the networks of botnets are frequently used to launch spam e-mail campaigns, denial-of-service attacks or on-line fraud schemes.

J. Tax Return Filing Activity by the Travis Rupard Broadband Access Card

71. The AFDC reported the following fraudulent returns were filed on May 22, 2008, using IP address 24.3.79.57, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
19:38:01	JESSLYN ACERET	\$560.00
19:41:36	RICHARD R. AGUILERA	\$929.00
19:48:28	GINA M. ABAGNARO	\$1,538.00

19:57:27	MIGUEL A. ALARCON	\$1,566.00
20:00:12	DONALD M. ADAMS	\$1,756.00
20:11:55	KATRYNKA N. ADACHI	\$912.00
20:17:58	CHRISTOPHER B. AKIN	\$2,211.00

Verizon Wireless broadband access card connection records for the Travis Rupard account show connections to IP address 24.3.79.57 on May 23, 2008, as early as 12:29:43 a.m. GMT and as late as 7:00:41 p.m. GMT. Therefore, your affiant has concluded that the subject wireless broadband access card was used to file each of these fraudulent returns.

72. The AFDC reported the following fraudulent returns were filed on May 24, 2008, using IP address 24.47.154.61, with refunds destined for the undercover Bank of America account:

IP Time (PSDT)	Name	Refund Amount
13:28:07	STEVEN A. ABBOTT	\$2,150.00
13:30:56	MICHAEL Y. AHN	\$1,136.00
13:31:06	KEITH T. ALLEN	\$1,596.00
13:33:00	JOSEPH C. AIREY	\$1,006.00
13:42:12	ARTHUR A. ADOLPHSON	\$1,159.00
13:43:00	MICHAEL L. ADELMAN	\$479.00
13:44:07	DAVID C. ACKERMAN	\$1,303.00
13:44:55	ANA C. ALFARO	\$1,436.00
13:53:41	ELIZABETH ALLEN	\$1,857.00
13:58:03	CARLOS O. ALVARADO	\$507.00
14:00:25	RYAN D. ALVARADO	\$635.00

14:03:07	JAMES P. ACOSTA	\$2,179.00
14:05:51	CAROL S. AKINS	\$2,085.00
14:08:54	MIGUEL D. ADAME	\$1,034.00
14:09:52	MEMORIE P. AGUERRE	\$779.00
14:11:57	LARRY A. ACEVEZ	\$428.00
14:19:26	DAVID L. ALCANTAR	\$1,152.00
14:20:14	JOHN D. ADAMSON	\$1,930.00
14:21:17	MARIO C. ALONSO	\$602.00
14:25:35	DANIEL A. ACETO	\$953.00
14:30:45	DAVID R. ACUNA	\$655.00

Verizon Wireless broadband access card connection records for the Travis Rupard account show the Travis Rupard account with multiple connections to IP address 24.47.154.61 on May 24, 2008, as early as 8:23:51 p.m. GMT and as late as 9:30:59 p.m. GMT. Therefore, your affiant has concluded that the subject wireless broadband access card was used to file each of these fraudulent returns.

73. The AFDC reported the following fraudulent returns were filed on May 25, 2008, using IP address 74.73.116.37, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
12:11:53	DON A. ABELLA	\$1,945.00
12:17:18	ROGER L. ADAMS	\$1,329.00
12:23:41	REUBEN ALICEA	\$1,036.00
12:25:26	LUIS J. ALATRISTE	\$1,238.00
12:27:00	MICHAEL ACOSTA	\$673.00

12:31:01	CAROLYN M. ADAMS	\$1,120.00
12:34:12	MARY R. AKINS	\$1,815.00
12:39:06	MATTHEW S. ALVAREZ	\$1,668.00
12:45:42	MARTIN M. AGUAYO	\$418.00
12:51:29	BRIAN W. ALBOHER	\$1,452.00

Verizon Wireless broadband access card connection records for the Travis Rupard account show multiple connections to IP address 74.73.116.37 on May 25, 2008, as early as 7:10:14 p.m. GMT and as late as 7:59:36 p.m. GMT. Therefore, your affiant has concluded that the subject wireless broadband access card was used to file each of these fraudulent returns.

74. The AFDC reported the following fraudulent returns were filed on May 26, 2008, using IP address 67.187.132.91, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
20:05:49	LOREN L. AISENBREY	\$1,572.00
20:07:03	WALTER F. ALEXANDER	\$1,747.00
20:08:05	DAVID ALVAREZ	\$575.00
20:09:18	SHARON M. ADAMS	\$1,447.00
20:15:03	BART AGUIRRE	\$425.00
20:23:03	PATRICK ALDERETE	\$652.00
20:24:20	GLORIA A. AGANZA	\$1,939.00
20:27:57	EUGENE A. ALCANTER	\$1,246.00
20:29:15	MANUEL M. ADVIENTO	\$1,457.00



Verizon Wireless broadband access card connection records for the Travis Rupard account show multiple connections to IP address 67.187.132.91 on May 27, 2008, as early as 2:54:47 a.m. GMT and as late as 3:58:26 a.m. GMT. Therefore, your affiant has concluded that the subject wireless broadband access card was used to file each of these fraudulent returns.

75. The AFDC reported the following fraudulent returns were filed on May 27, 2008, using IP address 67.64.43.108, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
11:21:03	MICHAEL ALDERSON	\$1,436.00
11:23:20	ROBERT M. AASE	\$1,470.00
11:27:31	AHMAD R. ALFRED	\$924.00
11:35:15	ROBERT J. ADAME	\$2,130.00
11:39:59	JAMES E. ADAMS	\$1,763.00
11:42:03	DELAWARENCE L. ADKINS	\$1,981.00
11:47:23	LEONARD S. ABEYTA	\$1,420.00
11:48:58	LIZABETH A. AGUILAR	\$655.00
11:50:52	WAYNE A. ABEL	\$725.00
11:56:09	DANIEL E. ALBRIGHT	\$1,200.00
11:59:40	BRENT C. ALLRED	\$987.00

Verizon Wireless broadband access card connection records for the Travis Rupard account show the Travis Rupard account connecting with multiple connections to IP address 67.64.43.108 on May 27, 2008, as early as 6:18:31 p.m. GMT and as late as 7:04:01 p.m. GMT. Therefore, your affiant has concluded that the subject wireless broadband access card was used to file each of these fraudulent returns.

76. The AFDC reported the following fraudulent returns were filed on May 28, 2008, using IP address 66.42.152.107, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
13:14:46	MARCIA ADKINS	\$1,056.00
13:16:07	BETTY A. ABRIL	\$981.00
13:20:02	DARLENE ALARCON	\$1,302.00
13:21:27	SERGIO R. AGUILAR	\$1,103.00
13:22:54	GERALD D. AKERS	\$1,188.00
13:25:47	BRYAN M. ACOSTA	\$1,326.00
13:27:15	GARY L. ALDINGER	\$1,865.00
13:28:40	DANIEL E. ADAMS	\$2,045.00
13:30:04	MARIO N. AGUIRRE	\$593.00
13:40:18	MICHAEL G. ALLEN	\$1,238.00
14:09:54	MARK S. ADLER	\$1,166.00
14:11:48	JULIA L. AKMAN	\$1,413.00
14:14:40	RAYMOND ALVAREZ	\$2,081.00
14:17:18	CHARLES O. ALIANO	\$1,079.00

Verizon Wireless broadband access card connection records for the Travis Rupard account show the Travis Rupard account with multiple connections to IP address 66.42.152.107 on May 28, 2008, as early as 8:13:27 p.m. GMT and as late as 9:17:22 p.m. GMT. Therefore, your affiant has concluded that the subject wireless broadband access card was used to file each of these fraudulent returns.

77. The AFDC reported the following fraudulent returns were filed on June 1, 2008, using IP address 68.198.200.5, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
11:43:48	THOMAS G. ANDRADE	\$1,525.00
11:50:06	ARTHUR R. ALVAREZ	\$1,651.00
11:51:28	GLORIA J. ARMIJO	\$1,910.00
11:53:14	DALE W. AMBLER	\$2,592.00
11:55:27	DALE B. ALFORD	\$950.00
12:14:59	ROBERT G. AMMONS	\$2,854.00
12:38:03	DAVID A. ALFATHER	\$888.00
12:39:37	MICHELLE L. ANDREWS	\$2,562.00
12:41:08	ROBERTO A. ALVAREZ	\$1,935.00

Verizon Wireless broadband access card connection records for the Travis Rupard account show the Travis Rupard account with multiple connections to IP address 68.198.200.5 on June 1, 2008 as early as 6:42:21pm GMT and as late as 7:42:48pm GMT. Therefore, your affiant has concluded that the subject wireless broadband access card was used to file each of these fraudulent returns.

78. The AFDC reported the following fraudulent returns were filed on June 3, 2008, using IP address 67.64.43.108, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
13:16:53	DAVID C. ALBERTSON	\$2,443.00
13:27:16	JESUS E. ALVARADO	\$2,349.00

Verizon Wireless broadband access card connection records for the Travis Rupard account show the Travis Rupard account with multiple connections to IP address 67.64.43.108 on June 3, 2008, as early as 8:13:09 p.m. GMT and as late as 8:47:38 p.m.

GMT. Therefore, your affiant has concluded that the subject wireless broadband access card was used to file each of these fraudulent returns. Therefore, your affiant has concluded that the subject wireless broadband access card was used to file each of these fraudulent returns.

79. The AFDC reported the following fraudulent returns were filed on June 3, 2008, using IP address 76.229.232.193, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
13:50:37	KIM W. ALLEN	\$2,736.00
13:52:39	MICHAEL A. AMATUCCI	\$2,211.00
13:55:17	JENNIFER L. BARNUM	\$2,774.00
14:04:01	PATRICIA E. ALLEN	\$2,842.00
14:06:49	JAMES D. ALTUM	\$2,741.00
14:23:29	MARIA D. BARRAZA	\$2,842.00
14:25:08	JOSE A. ALVARENGA	\$2,481.00
14:26:36	AMBER D. BARFIELD	\$2,964.00
14:28:25	KAREN D. ALEXANDER	\$2,335.00
14:39:03	JAMES B. ALEXANDER	\$2,113.00
14:40:36	SCOTT A. ANDERSON	\$2,722.00
14:45:11	TRISHA L. BARTLETT	\$2,353.00
14:49:01	LEO L. ALBERT	\$2,241.00

Verizon Wireless broadband access card connection records for the Travis Rupard account show the Travis Rupard account with multiple connections to IP address 76.229.232.193 on June 3, 2008, as early as 8:48:23 p.m. GMT and as late as 10:07:17 p.m. GMT on June 3, 2008. Therefore, your affiant has concluded that the subject wireless broadband access card was used to file each of these fraudulent returns.

80. The AFDC reported the following fraudulent returns were filed on June 4, 2008, using IP address 67.172.220.94, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
23:16:11	RICK I. ALLISON	\$984.00
23:32:26	DANIEL L. ALLEN	\$2,556.00
23:33:56	RAYMOND J. ALVAREZ	\$1,557.00
23:37:44	ROSARIO V. ALTURA	\$2,966.00
23:48:40	SALLY M. BANDA	\$1,549.00
23:52:18	JAMES L. ALSUP	\$2,260.00
23:57:18	MANUEL S. ALLEN	\$2,928.00

Verizon Wireless broadband access card connection records for the Travis Rupard account show the Travis Rupard account with multiple connections to IP address 67.172.220.94, on June 5, 2008 as early as 6:06:42 a.m. GMT and as late as 7:06:36 a.m. GMT. Therefore, your affiant has concluded that the subject wireless broadband access card was used to file each of these fraudulent returns.

81. The AFDC reported the following fraudulent returns were filed on June 5, 2008, using IP address 67.187.119.170, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
00:13:58	MELVIN G ARNOLD	\$1,629.00
00:16:25	CHRISTINE A ARENA	\$934.00
00:18:11	ANDREW L ALLISON	\$2,886.00
00:28:37	RACHELLE M BARROWS	\$1,405.00

00:32:58	CORLAINE R ALTO	\$1,955.00
----------	-----------------	------------

Verizon Wireless broadband access card connection records for the Travis Rupard account show the Travis Rupard account with multiple connections to IP address 67.187.119.170 on June 5, 2008, as early as 7:08:22 a.m. GMT and as late as 7:40:29 a.m. GMT. Therefore, your affiant has concluded that the subject wireless broadband access card was used to file each of these fraudulent returns.

**K. Analysis of Bank Accounts**

82. The AFDC has identified refunds destined for the undercover bank accounts and continues to monitor the accounts for additional fraudulent returns. In addition, the AFDC uses the information from the electronically filed returns to identify any additional fraudulent tax returns, IP addresses and/or accounts being used to facilitate the scheme. As of June 26, 2008, the following banks have been identified as being linked to this bulk filing scheme:

<b>Bank</b>	<b>No. of Accounts</b>	<b>No. of Returns</b>
Meridian Bank (Undercover Account)	1	395
Columbus Bank & Trust	1	73
Centennial Bank	23	200
GE Money Bank	3	134
Bancorp Bank	9	53
MetaBank	30	156
Arkansas State Bank	3	10
Bank of America (Undercover Account)	1	249
International Bank	2	2

83. Centennial Bank has identified the Centennial Bank accounts noted in Paragraph 82 as being related to a debit card program that was issued by Galileo Processing, an intermediary processor as further discussed in Paragraph 88 below.

84. Bancorp Bank identified the Bancorp accounts noted in Paragraph 82 as being related to prepaid debit cards where the funds are loaded to the card at authorized third party locations, or electronically by direct deposit. A representative of the bank advised Special Agent Medrano that the tax refunds deposited into the account are listed in the names of people other than the account holder.

85. A representative of MetaBank has informed Special Agent Medrano that the MetaBank accounts noted in Paragraph 82 were related to debit cards. The representative further explained that cards with account numbers starting with a 5 were from Account Now, the account numbers starting with a 7 were from NetSpend, and the accounts beginning with 065 were from Galileo Processing Inc.

86. According to Account Now Inc's website, [www.accountnow.net](http://www.accountnow.net), they are a premier provider of financial solutions for the millions of consumers in the United States who do not have established credit or traditional banking relationships. Account Now offers prepaid Master Cards. Account Now states their prepaid Master Cards are issued by MetaBank. Deposits can be made to the account by paycheck, direct deposit or MoneyGram Express Payment.

87. According to NetSpend Corporation's website, [www.netspend.com](http://www.netspend.com), this company offers all-access prepaid Visa and Master Card debit cards. The company's website states that the cards work like debit cards, without the hassle of a bank account and are accepted at millions of places worldwide. The website states that a person can obtain a card without a credit check. Funds are loaded on the card via direct deposit, by visiting a reload center or online with PayPal. Cards can be purchased at certain reload centers or through the website. NetSpend states on their website they are an authorized Independent Sales Organization of Inter National Bank and MetaBank and the cards are issued through these two banks.

88. According to Galileo Processing, Inc.'s website, [www.galileoprocessing.com](http://www.galileoprocessing.com), the company offers partners, clients, and consumers solutions and support for financial payment processing. According to the company's website, Galileo Processing, Inc., is an advanced processor for credit, debit, and prepaid

card programs. The company offers multi-purse technology, a proprietary bill payment service, integrated ACD and IVR, world-class customer service, and real-time connectivity to over 100,000 retail locations that accept cash loads to prepaid cards.

#### L. California Death Index Information

89. The social security numbers listed on the 395 tax returns identified with refunds destined for the IRS controlled undercover bank account at Meridian Bank and the 249 tax returns identified with refunds destined for the IRS controlled undercover account at Bank of America were researched on the California Death Index. The California Death Index contains millions of records with information for birth years 1940 through 1997. All 654 corresponding social security numbers were located using this data base. Research revealed that all of the individuals listed on these returns were deceased well before 2007, and therefore, did not receive taxable income in the form of wages in 2007.

#### M. E-Mail Communications between the "Hacker" and CI 2

90. In the course of the execution of a Search Warrant on April 15, 2008, of a computer used by CI 2, e-mails records were recovered which had been sent on or before April 15, 2008, by the "Hacker".

91. In an e-mail sent on unknown date prior to April 15, 2008, the "Hacker" advised CI 2 he produces fraudulent identification documents and that he has sold identification documents for many years without any problems. The "Hacker" stated if he is raided by law enforcement, he will use his keystroke kill switch to shut down the computer and then physically hold down the power button to turn off the computer in case the kill switch fails. When the computer is shut down, all saved encryption keys are deleted from the computer memory. Moreover, the "Hacker's" entire hard drive is always encrypted.

92. In an e-mail sent on unknown date prior to April 15, 2008, the "Hacker" advised CI 2 he uses a different IP address for each tax return and has filed returns with many different efilers. The "Hacker" believes filing the returns in this manner would prevent "them," (i.e., the IRS), to link them all. The "Hacker" advised an e-filer "took some heat" from the IRS because of his automated filing scheme. The "Hacker" stated the e-filer tried to stop him by use of a captcha, i.e. a box that appears on a webpage requiring the user to personally view a screen and then enter in a series of characters. The purpose of a captcha is to prevent automated entry of data on a webpage.



93. In an e-mail sent on unknown date prior to April 15, 2008, the "Hacker" advised CI 2 he knows "everything there is to know about creating new identities in the USA and I know a lot about assumed identities." The "Hacker" advised CI 2 he is an encryption expert and a privacy expert. Further, during a debriefing of CI 2 after April 15, 2008, he/she advised that the "Hacker" had obtained proceeds from the subject bulk filing scheme in the past through the receipt of encrypted electronic information regarding debit cards. CI 2 also stated that he/she has sent related account information to the "Hacker" which he could then use to create his own debit cards using an electronic debit card reader/writer and then withdraw the funds from automatic teller machines. In the course of follow-up investigation with respect to this information, an unknown white male or males, average build, appearing to between the age of 20 and 29, have been observed making withdrawals, or attempting to make withdrawals, with multiple debit cards from automatic teller machines on security camera photos obtained via Grand Jury subpoenas. In each case in March and April of 2008, the subject debit card accounts had previously received fraudulent tax refunds that had been obtained as part of the scheme. During the recent search of the "Hacker's" apartment and storage unit, materials and equipment were found that could be used to create the debit cards CI 2 spoke of.

94. On or about April 23, 2008, the "Hacker" advised CI 2 in an e-mail he had burned his identification document and his birth certificate. The "Hacker" stated to CI 2, "I am probably the single biggest threat to the US government currently living and they don't even know it. I can do things to the government that will make all these terrorist organizations look like sewing circles." In this same e-mail, the "Hacker" claims to have a contact with an individual who was previously a United States Intelligence Agent who assists the "Hacker" primarily with information on identities. The "Hacker" claims he trades computer information with this former Intelligence Agent in exchange for information known to the former Intelligence Agent. The "Hacker" claims this individual fears being accused of treason even though the former Intelligence Agent has not worked in the government for ten years.

95. On or about May 12, 2008, the "Hacker" e-mailed CI 2 and stated "I was thinking of starting with robotic aerial assassins that can be controlled from a computer over the internet. It would be essentially a flying handgun that no one would likely see. Perfect for taking out politicians. The controls would be military grade but designed by me. I was also thinking about making 50 mile range missiles without the warheads...I would only want to arm militias planning on standing up against the feds when the winner take all war takes place in the US...I am also trying to convince some old friends to help out with chemical and biological weapons as well. There will be no rules in this war. The government has already set the stage...". The "Hacker" added, "I have always wanted a small automatic weapon with a silencer similar to the one Bruce Willis used in

Pulp Fiction to kill the Scientologist..." The "Hacker" advised CI 2, "If you can help me expand my arsenal then I would appreciate it" (The weapon used in the movie appears to be a handheld machine gun with a silencer.)

96. On or about May 14, 2008, the "Hacker" e-mailed CI 2 a list of numerous weapons to follow up on. In numerous subsequent e-mails, the "Hacker" engaged in discussions regarding purchasing an unregistered MAC-10 with a silencer with CI 2 serving as a broker. On or about June 2, 2008, the "Hacker" e-mailed CI 2 that, "I have a lot of money to spend on guns (100k+) but if this is what it is like to deal with illegal gun dealers then I will stick to making AR15s, AK47s and M4s in my garage." The "Hacker" decided not to purchase the weapon at the present time but advised he will consider purchasing a weapon in the future through CI 2. During the recent search of the "Hacker's" apartment and storage unit, no firearms or ammunition was found.

97. On or about May 23, 2008, the "Hacker" sent an e-mail to CI 2 asking for access to the Social Security Administration internal "death master file". The "Hacker" believes this death index contains information on deaths of persons for whom the Social Security Administration has not been able to verify the deaths and therefore cannot treat these persons as deceased for tax purposes. The "Hacker" asked CI 2 for other personal identifying information in database format and access to information in a state death database for persons who died in the year 2008. Your affiant believes the "Hacker" has sought personal identifying information on individuals that he could utilize to file fraudulent tax returns. After CI 2 successfully provided the "Hacker" with \$68,000.00 in cash, the "Hacker's" opinion of CI 2's capabilities as a middleman were greatly enhanced.

98. On or about June 10, 2008, the "Hacker" sent an e-mail to CI 2 stating, "I funded other bank accounts at the same time from the same proxies and they all work out..." Your affiant has probable cause to believe the "Hacker" is referencing fraudulent tax returns sent to other accounts in addition to the Bank of America undercover bank account. During the recent search of the "Hacker's" apartment and storage unit, computer records relating to other accounts, including numerous prepaid debit cards, were found along with records relating to the "Daniel" account.

99. On or about June 11, 2008, the "Hacker" sent an e-mail to CI 2 asking for personal identifying information of third parties. The "Hacker" again sought information on the Social Security Administration "internal death master file," the previous Choicepoint data compromise, and personal identifying information on Bank of America customers. The "Hacker" further advised that, "I can and will bring this country into a "Mad Max" state if the government continues down their path. I just hope there are enough people with enough guns spread through out the country to fight off the feds

and split the country into new countries....” Your affiant believes that the reference to Mad Max refers to the post-apocalyptic world depicted in the film “Mad Max.”

100. On or about June 26, 2008, the “Hacker” warned CI 2 about the countermeasures he would use to take possession of a bulk currency delivery he is owed after June 30, 2008, representing his percentage of the proceeds derived from fraudulent tax returns. The “Hacker” advised the courier who retrieves the package containing the bulk currency from the mailing center will be armed with a concealed M4 assault rifle. The “Hacker” stated the courier will scan the package for both analog and digital radio signals and with an ultraviolet black light. The “Hacker” advised CI 2 if the package is transmitting a radio frequency signal or the tape on the package has been replaced, the courier will run away and shoot anyone who tries to grab him. According to the “Hacker”, a team will be in place to provide cover fire so all members of the pickup team can escape. The “Hacker” advised if anything happens in the FedEx center, “everyone who works there will be dead.” The “Hacker” advised if anything happens outside the Fedex store, then anyone the pickup team sees will be dead and any cops will be dead. The “Hacker” stated the pickup team will “make a point” by killing innocent people just to teach law enforcement a lesson. On the chance that CI 2 is a CI, the “Hacker” plans on e-mailing unidentified reporters, in encrypted fashion, the exact details of the package pickup and the countermeasures in place to prove that CI 2 knew beforehand that people would die if law enforcement intervened. If a law enforcement sting ensues at the Fedex store, the “Hacker” will then e-mail the passwords to the encrypted messages previously sent to the reporters so that the news will be, “Law Enforcement and CI knew about murderous rampage but did nothing to prevent it!”

#### N. Historical Cell Tower Information and Other Investigative Techniques

101. Historical cell tower information for the Travis Rupard Broadband Access Card and the records relating to the use of particular IP Addresses used by the card as described above, lead your affiant to conclude the “Hacker” has used the Travis Rupard Broadband Access Card to commit offenses in violation of the statutes set forth in Paragraph 3 above.

102. Historical cell tower information and other investigative techniques have led the investigation team to the location of the Travis Rupard Broadband Access Card within the “domicilio” apartment complex; 431 El Camino Real; Apartment 1122; Santa Clara, California, 95050; and, as stated above, the subject device was found in the apartment on August 3, 2008.

103. On July 17, 2008, a Grand Jury subpoena was issued to domicilio for the file information related to 431 El Camino Real, Apartment 1122, Santa Clara, California, 95050. The subpoena revealed the apartment was being rented by an individual claiming to be Steven Travis Brawner. The rental application indicated that Brawner was a software engineer.

104. The rental applicant provided a California driver's license in the name of Steven Travis Brawner, license number D6870214. Further investigation revealed the California driver's license number is assigned to a female with a Chino Hills, California address.

105. In order to rent the apartment, the applicant was required by the rental company to provide a copy of the first page of what he claimed to be this 2006 tax return. The return purports to show an adjusted gross income (AGI) of \$110,314. The social security number on the return is 559-87-4167. Internal records for the Internal Revenue Service were researched and revealed no tax return for 2006 was filed for Steven Travis Brawner. Additionally, Social Security Administration records for social security number 559-87-4167 indicate that Steven Brawner died in 1997.

106. On July 21, 2008, Forensic Document Examiner William J. Flynn conducted a handwriting analysis of the original application documents for 431 El Camino Real, Apartment 1122 and the original application documents for the Sacramento Post Office Box. After conducting the analysis of the documents, Mr. Flynn has advised that forensic evidence indicates common authorship among the documents.

#### SUMMARY OF ITEMS FOUND AT SEARCH LOCATIONS

107. Pursuant to the above described search warrants the following locations were searched.

- a. 431 El Camino Real; Apartment 1122; Santa Clara, California, 95050
- b. Storage Unit No. A-047, located at CBD Indoor Mini, 570 Cinnabar Street  
San Jose, California 95110

108. With respect to the subject residence, the probable cause was based upon the information set forth throughout this affidavit, including the following information:

- a. On March 26, a fraudulent tax return for Kevin Furman was filed with the IRS using IP address 75.209.101.132, claiming a refund amount of \$1,282.00 destined for the Meridian undercover bank account.
- b. In response to an Order issued pursuant to 18 U.S.C. § 2703(d), Verizon Wireless reported that IP addresses 75.208.105.186, 75.209.41.104, and 75.209.101.132 were utilized by the Travis Rupard Broadband Access Card.
- c. Historical cell tower information and other investigative techniques have led the investigation team to the location of the Travis Rupard Broadband Access Card within the "domicilio" apartment complex; 431 El Camino Real; Apartment 1122; Santa Clara, California, 95050.
- d. On July 17, 2008, a Grand Jury subpoena was issued to domicilio for the file information related to 431 El Camino Real, Apartment 1122, Santa Clara, California, 95050. The subpoena revealed the apartment was being rented by an individual claiming to be Steven Travis Brawner.
- e. In the course of the subject apartment rental application, the applicant provided a California driver's license bearing number D6870214. Further investigation revealed the California driver's license number is assigned to a female with a Chino Hills, California, address.
- f. In order to rent the apartment, applicant was required by the rental company to provide a copy of the first page of what he claimed to be this 2006 tax return. The return purports to show an adjusted gross income (AGI) of \$110,314. The social security number on the return is 559-87-4167. Internal records for the Internal Revenue Service were researched and revealed no tax return for 2006 was filed for Steven Travis Brawner. Additionally, Social Security Administration records for social security number 559-87-4167 indicate that Steven Brawner died in 1997.
- g. CI 2 indicated the "Hacker" previously operated a website ([www.fakeid.tv](http://www.fakeid.tv)) where the "Hacker" sold fake California driver's licenses.
- h. On July 21, 2008, Forensic Document Examiner William J. Flynn conducted a preliminary handwriting analysis of the original rental application documents for 431 El Camino Real, Apartment 1122 and the original application documents for the Sacramento Post Office Box. A preliminary review of the documents by

Mr. Flynn has indicated it appears that both applications were completed by the same individual.

i. On August 3, 2008, a person matching the description of Steven Travis Brawner was observed near the subject apartment by law enforcement officers. As he was followed, he began to seek to evade them. Local police in marked units then assisted federal agents in following the subject. The subject attempted to flee on foot. During a search incident to arrest nearby, a key to the subject apartment was found in the arrestee's pocket.

j. On August 3, 2008, during the execution of the second warrant relating to the subject apartment, numerous items were located including the subject wireless broadband access card, false California drivers' licenses in names of Steven Travis Brawner, Patrick Stout and numerous others all bearing the arrestee's photographic image, and U.S. currency.

k. On August 3 and 4, 2008, during the execution of the second warrant relating to the subject apartment, numerous additional items were found which are evidence of conduct in furtherance of the subject scheme or occupancy of the subject apartment, including surveillance equipment, items possibly bearing DNA, keys, clothing and baggage, "to-do" lists, silver coins; files and correspondence related to the creating of false identification documents, resisting the United States Government, survival, fleeing the United States, and moving money out of the United States undetected.

109. With respect to the storage unit, the probable cause was based upon the information set forth throughout this affidavit, including the following information:

a. On August 4, 2008, during the ongoing execution of the second warrant relating to the subject apartment, a review of the computers, as listed in the second Attachment B – Items to be seized was conducted by Special Agent Daun. In the process of the review of the computers, computer records relating to a storage unit were identified. The storage unit, Unit A-47 is located within the CBD Indoor Mini self-storage facility; located at 570 Cinnabar Street; San Jose, California 95110. The unit was rented under the name Daniel Clifton Aldrich. Per the computer records, the rent was paid on March 13, 2008 in the amount of \$399.00. The rent was paid for a period of six months up to October 1, 2008.

b. On August 4, 2008, Special Agent Medrano spoke with the facility manager for CBD Indoor Mini. The facility manager confirmed that Daniel Clifton Aldrich y rented Unit A-47 at that time. The facility's rental records for the unit include a photo copy of a drivers' license in the name of Daniel Clifton Aldrich. The image in the drivers' license is similar to the image in the Steven Travis Brawner and Patrick Stout drivers' licenses as listed in Paragraph 108(j), and appears to be arrestee.

c. The facility manager specifically identified Unit A-47 to Special Agent Medrano.

d. On August 4, 2008, during the execution of the warrant relating to the storage unit, numerous additional items were found which are evidence of conduct in furtherance of the subject scheme, including false California drivers' licenses in various names, U.S. currency; gold coins, a passport in the name of Andrew Johnson, three (3) birth certificates for Steven Brawner, death certificates for Andrew Johnson and Steven Brawner, rental documents for the "domicilio" apartment complex, and numerous debit cards.

111. A total of approximately \$117,000 in U.S. Currency was found during the searches at both locations. At least one (1) \$100 bill from the \$68,000 controlled delivery described in this affidavit was observed in the collection of currency. All of the serial numbers for the bills comprising the \$68,000 were recorded. The one bill observed was visible through a clear plastic bag which contained some of the seized currency and was sealed after the searches for evidence and accounting purposes. Therefore, no effort to identify additional bills has been undertaken at this time.

112. A total of approximately 230 ounces of gold coins were also discovered during the searches. At the time of the seizure of the coins, gold was trading for approximately \$880.00 per ounce. Therefore the gold was valued at approximately \$202,400.

113. A total of approximately 588 1 ounce silver coins were discovered during the searches. At the time of the seizure of the coins, silver was trading for approximately \$17 per ounce. Therefore the silver coins are valued at approximately \$10,000.00.

114. Also found during the searches was U.S. passport, previously issued by the State Department in the name of Andrew Glenn Johnson, bearing a photo of Brawner/Rigmaiden. On the computer located within the subject apartment, the images of the birth and death certificates for Andrew Glenn Johnson were found.

115. Also found in the "Hacker's" computer was a list of Prepaid Card Accounts which set forth in respective Attachments A1-A6, incorporated by herein. Your affiant has probable cause to believe these are the debit cards and related accounts which were created by or on behalf of Brawner/Rigmaiden to receive fraudulent IRS tax refunds.

116. Your affiant cannot determine how many co-conspirators might have the necessary information to remove funds from these accounts. Although these accounts are in the control and custody of Brawner/Rigmaiden, it will take some time to determine the actual names associated with each account.

117. Due to the complexities involved with the amount of funds; the unknown number of co-conspirators, including yet to be identified individuals who played roles similar to C1 1 and C1 2, as well as persons who have acted as mail-drops in order to receive the original debit cards mailed by the card providers; the identity of parties who may have access to these funds and the total number of accounts, it is unrealistic to believe a restraining order would be sufficient to insure the funds are made available to this Court. Unless the funds contained in or on the prepaid debit cards associated with the respective account numbers, it is likely that some of the funds will be removed or dissipated prior to the conclusion of the related criminal case. Moreover, the search of the "Hacker's" seized computer records and physical evidence, to date, has revealed no means of generating income other than the subject bulk filing tax scheme.

#### ADDITIONAL INFORMATION DETERMINED SINCE ARREST

##### O. Criminal History of Daniel David Rigmaiden

118. Fingerprint analysis was conducted on the fingerprints that were taken after arrest of the "Hacker". The fingerprint analysis determined the "Hacker" has a previous criminal history. Based on the fingerprint analysis, the "hacker's" real identity has determined to be Daniel David Rigmaiden. Rigmaiden's criminal history is as follows:

- a. 1999, Monterey, California - Rigmaiden was convicted of three felony counts of grand theft access cards and was sentenced to 120 days in jail and 3 years probation.
- b. 2000, San Luis Obispo, California - Rigmaiden was charged with attempting to manufacture PCP and driving without a license. Rigmaiden has an outstanding arrest warrant for Failure to Appear, dated November 7, 2000.
- c. 2000, Santa Cruz County, California - Rigmaiden has an outstanding arrest warrant regarding a pending fraud charge.



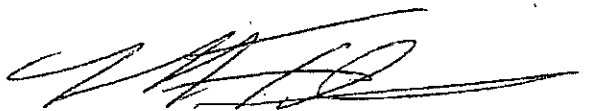
P. Items Found on the "Hacker's" Computer

119. The following items were found on the "Hacker's" computer which was found at his apartment:

- a. Birth and death certificates of Steven Brawner; the name used to rent the apartment. Brawner's birth certificate was issued from the State of Michigan; Brawner's death certificate was issued from the State of Idaho; date of death is May 27, 1997.
- b. Birth and death certificates of Andrew Glenn Johnson. A passport in the name of Andrew Glenn Johnson was found at the storage unit; bearing a picture similar to arrestee.
- c. Indications the subject has been filing fraudulent tax returns since 2004.
- d. A folder for Travis Rupard (the broadband card was issued under the name of Travis Rupard), which contained information on an e-gold account.
- e. Emails regarding leaving the United States for the country of Dominica. The first of these emails occurred in October/November of 2006. The subject stated he wanted to have \$250,000 before he left the United States and that it would take him 12-18 months to have that much money. The emails, which were sent to an unidentified individual, also asked the unidentified individual to find a bank that would accept United States currency, with the intention of the subject to have his friend send him \$5,000 in cash each week.
- f. Documents regarding obtaining citizenship in other countries; emails regarding paying off Dominican officials to get Dominican birth certificates and passports; and a Belize residency guide.

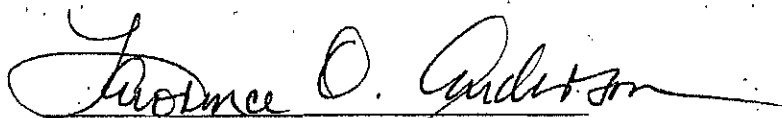
CONCLUSION

120. Based on your affiant's, and his fellow agents', education, training and experience, and the facts set forth in this affidavit, your affiant has probable cause to believe the debit cards and related accounts, also referred to as Prepaid Card Accounts, further described in Attachment A, are property, real or personal, which constitutes or is derived from proceeds traceable to any specified unlawful activity as defined in 18 U.S.C. §§ 1956(c)(7) and 1961(1) and a conspiracy to commit such offenses, and are subject to seizure pursuant to 18 U.S.C. §§ 981(a)(1)(C) and 982, and 28 U.S.C. §2461.



Michael P. Fleischmann  
Special Agent  
Internal Revenue Service – Criminal Investigation

Sworn to and subscribed  
in my presence this 22<sup>ND</sup> day of August, 2008



Hon. Lawrence O. Anderson  
United States Magistrate Judge  
District of Arizona