

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

FILED

2008 JUL 11 P 3:40

RICHARD W. WIEKING
CLERK
U.S. DISTRICT COURT
NO. DIST. OF CA., S.J.

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING THE)
USE AND MONITORING OF A MOBILE)
TRACKING DEVICE FOR:)

**SEALED BY ORDER
OF THE COURT**

NO.

THE VERIZON WIRELESS BROADBAND)
ACCESS CARD/CELLULAR TELEPHONE)
ASSIGNED TELEPHONE NUMBER)
(415) 264-9596 AND ESN)
NUMBER 005-00717190)
(THE TARGET BROADBAND ACCESS CARD/)
CELLULAR TELEPHONE))

(UNDER SEAL)

RS

CRO8-90330MISC
ORDER

This matter is before the Court pursuant to an Application under Federal Rule of Criminal Procedure 41(b); Title 18, United States Code, Sections 2703 and 3117; and Title 28, United States Code, Section 1651, by Assistant United States Attorney Shawna Yen, an attorney for the Government, which Application requests an Order directing Verizon Wireless to assist agents of the Federal Bureau of Investigation (FBI) by providing all information, facilities, and technical assistance needed to ascertain the physical location of the Verizon Wireless broadband access card/cellular telephone assigned Telephone Number (415) 264-9596 and Electronic Serial Number (ESN) 005-00717190 (the Target Broadband Access Card/Cellular Telephone), through the use and monitoring of a mobile tracking device for the Target Broadband Access Card/Cellular Telephone with service by Verizon Wireless, for a period of thirty (30) days.

228A-PX-8000143

The Court FINDS that there is probable cause to believe that the use and monitoring of a mobile tracking device for the Target Broadband Access Card/Cellular Telephone, will lead to evidence of violations of 18 U.S.C. § 286 – Conspiracy to Defraud the Government; 18 U.S.C. § 287 – False, Fictitious or Fraudulent Claims; 18 U.S.C. § 371 – Conspiracy; 18 U.S.C. § 1028 – Fraud Related to Identity Information; 18 U.S.C. § 1028A – Aggravated Identify Theft; 18 U.S.C. § 1029 – Fraud with Access Devices; 18 U.S.C. § 1030 – Unauthorized Computer Access; 18 U.S.C. § 1341 – Mail Fraud; and 18 U.S.C. § 1343 – Wire Fraud, as well as to the identification of individuals who are engaged in the commission of these offenses. The Court further FINDS that specific and articulable facts establish that there are reasonable grounds to believe that the requested information pertaining to the location of the the Target Broadband Access Card/Cellular Telephone is relevant and material to an ongoing criminal investigation.

The Court therefore ORDERS, pursuant to Federal Rule of Criminal Procedure 41(b); Title 18, United States Code, Sections 2703 and 3117; and Title 28, United States Code, Section 1651, that Verizon Wireless, within ten (10) days of the signing of this Order and for a period not to exceed 30 days, unless extended by the Court, shall provide to agents of the FBI data and information obtained from the monitoring of transmissions related to the location of the Target Broadband Access Card/Cellular Telephone, and shall monitor such transmissions, to extend to any time of the day or night as required, including the monitoring of the Target Broadband Access Card/Cellular Telephone while the agents are stationed in a public location and the Target Broadband Access Card/Cellular Telephone is (a) inside private residences, garages and/or other locations not open to the public or visual surveillance; and (b) anywhere else the Target Broadband Access Card/Cellular Telephone may be present within the United States, pursuant to Title 18, United States

Code, Sections 2703 and 3117; said ORDER being expressly limited to transmissions needed to ascertain the physical location of the Target Broadband Access Card/Cellular Telephone, and expressly excludes any voice communications and data content transmitted by Verizon Wireless to or from the Target Broadband Access Card/Cellular Telephone; and

WHEREAS the return and inventory requirements of Federal Rule of Criminal Procedure 41(f) do not apply to the information sought to be obtained by the instant application, Special Agents of FBI are therefore not required to serve a copy of this Order on any owner of the Target Broadband Access Card/Cellular Telephone, nor to make an inventory of any resulting information to be served on any such owner, except upon further Order of the Court. However, at the conclusion of the tracking mission, the investigating agency shall expunge all of the data obtained by this Court Order;

It is further ORDERED, pursuant to Federal Rule of Criminal Procedure 41(b); Title 18, United States Code, Sections 2703 and 3117; and Title 28, United States Code, Section 1651, that Verizon Wireless shall provide said agents immediately on request with all information, facilities, and technical assistance needed to ascertain the physical location of the Target Broadband Access Card/Cellular Telephone and that FBI shall compensate Verizon Wireless for reasonable expenses incurred in complying with any such request.

The Court further ORDERS that the government's Application, the attached Affidavit, and the Court's Order be filed under seal, except that copies of the Court's Order in full or redacted form may be served on Special Agents and other investigative and law enforcement officers of FBI, federally-deputized state and local law enforcement officers, and other government and contract personnel acting under the supervision of such investigative or law enforcement officers, and the service providers as necessary to effectuate the Court's Order.

It is further ORDERED that Verizon Wireless, its affiliates, officers, employees, and agents not disclose the Court's Order, the existence of monitoring under the Court's Order, or the underlying investigation to anyone pending further order of the Court.

SO ORDERED this the 11 day of July, 2008.



RICHARD SEEBORG
UNITED STATES MAGISTRATE JUDGE

43. Based on the foregoing, your affiant believes that there is probable cause to believe that the use and monitoring of a mobile tracking device for the Target Broadband Access Card/Cellular Telephone will lead to evidence of violations of the statutes listed above; as well as to the identification of individuals who are engaged in the commission of these offenses.



Special Agent William Ng
Federal Bureau of Investigation

Sworn to before me and subscribed to in my presence, this 11th day of July, 2008



RICHARD SEEBORG
United States Magistrate Judge

ORIGINAL
FILED

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA 08 JUL 11 PM 3:41
SAN JOSE DIVISION

RICHARD W. WIEKING
CLERK
U.S. DISTRICT COURT
NO. DIST OF CA S.J.

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING THE)
USE AND MONITORING OF A MOBILE)
TRACKING DEVICE FOR:)

SEALED BY ORDER
OF THE COURT

NO.

THE VERIZON WIRELESS BROADBAND)
ACCESS CARD/CELLULAR TELEPHONE)
ASSIGNED TELEPHONE NUMBER)
(415) 264-9596 AND ESN)
NUMBER 005-00717190)
(THE TARGET BROADBAND ACCESS CARD/)
CELLULAR TELEPHONE))

(UNDER SEAL)

RS

CRO8-90330MISC

APPLICATION

COMES NOW the United States of America, by and through its counsel, Assistant United States Attorney Shawna Yen, and pursuant to Federal Rule of Criminal Procedure 41(b), Title 18, United States Code, Sections 2703 and 3117, and Title 28; United States Code, Section 1651, submits this Application in support of an Order directing Verizon Wireless to assist agents of the Federal Bureau of Investigation (FBI) by providing all information, facilities, and technical assistance needed to ascertain the physical location of the Verizon Wireless broadband access card/cellular telephone assigned to Telephone Number (415) 264-9596 and Electronic Serial Number (ESN) 005-00717190 (the Target Broadband Access Card/Cellular Telephone), through the use and monitoring of a mobile tracking device for the Target Broadband Access Card/Cellular Telephone with service by Verizon Wireless, for a period of thirty (30) days. The purpose of the installation

of this mobile tracking device is to track the physical location of the target, and it will require the acquisition of real-time cellular information.

The United States submits that, based on the Affidavit in Support of Application for Order Authorizing the Use and Monitoring of a Mobile Tracking Device, by FBI Special Agent William Ng, attached as Exhibit A to this Application, probable cause exists to believe that this information will lead to evidence of violations of 18 U.S.C. § 286 – Conspiracy to Defraud the Government; 18 U.S.C. § 287 – False, Fictitious or Fraudulent Claims; 18 U.S.C. § 371 – Conspiracy; 18 U.S.C. § 1028 – Fraud Related to Identity Information; 18 U.S.C. § 1028A – Aggravated Identify Theft; 18 U.S.C. § 1029 – Fraud with Access Devices; 18 U.S.C. § 1030 – Unauthorized Computer Access; 18 U.S.C. § 1341 – Mail Fraud; and 18 U.S.C. § 1343 – Wire Fraud, as well as to the identification of individuals who are engaged in the commission of these offenses.

In addition, the affidavit of Special Agent Ng sets forth specific and articulable facts establishing that there are reasonable grounds to believe that the requested information pertaining to the location of the Target Broadband Access Card/Cellular Telephone is relevant and material to an ongoing criminal investigation.

Based on a conversation with the FBI, I have learned that the installation of such a mobile tracking device has the potential for temporary interruption of service.

Wherefore, your Applicant respectfully requests that the Court issue an Order directing that:

- 1) Federal Rule of Criminal Procedure 41(b), Title 18, United States Code, Sections 2703 and 3117, and Title 28, United States Code, Section 1651, authorize Special Agents of FBI, for a period not to exceed 30 days unless extended by the Court, to direct Verizon Wireless to assist

the agents in the use and monitoring of a mobile tracking device for the Target Broadband Access Card/Cellular Telephone, and that said authority to monitor transmissions via the Verizon Wireless system shall extend to any time of the day or night as required, including the monitoring of the Target Broadband Access Card/Cellular Telephone while the agents are stationed in a public location and the Target Broadband Access Card/Cellular Telephone is (a) inside private residences, garages and/or other locations not open to the public or visual surveillance; and (b) anywhere else the Target Broadband Access Card/Cellular Telephone may be present within the United States. This authority is expressly limited to transmissions needed to ascertain the physical location of the Target Broadband Access Card/Cellular Telephone and expressly excludes any voice communications and data content transmitted by Verizon Wireless to or from the Target Broadband Access Card/Cellular Telephone;

2) Pursuant to Federal Rule of Criminal Procedure 41(b), Title 18, United States Code, Sections 2703 and 3117, and Title 28, United States Code, Section 1651, Verizon Wireless shall provide said agents immediately on request with all information needed to ascertain the physical location of the Target Broadband Access Card/Cellular and FBI shall compensate Verizon Wireless for reasonable expenses incurred in complying with any such request;

3) The return and inventory requirements of Federal Rule of Criminal Procedure 41(f) do not apply to the information sought to be obtained by the instant application, and FBI therefore is not required to serve a copy of this Order on any owner of the Target Broadband Access Device, nor to make an inventory of any resulting information to be served on any such owner, except upon further Order of the Court. However, at the conclusion of the tracking mission, the investigating agency will expunge all data obtained by the Court's Order;

4) Because disclosure of this Application and the attached Affidavit could jeopardize the ongoing investigation, Applicant further requests that this Application, the attached Affidavit, and the Court's Order be filed under seal, except that copies of the Court's Order in full or redacted form may be served on Special Agents and other investigative and law enforcement officers of FBI, federally-deputized state and local law enforcement officers, and other government and contract personnel acting under the supervision of such investigative or law enforcement officers, and the service providers as necessary to effectuate the Court's Order; and


5) Verizon Wireless, its affiliates, officers, employees, and agents shall not disclose the existence of the requested Order, the existence of monitoring under the requested Order, or the underlying investigation to anyone until further order of the Court.

I declare under penalty of perjury that, I have discussed the foregoing application with FBI Special Agents, and that the foregoing is true and correct to the best of my knowledge and belief.

EXECUTED on this the 11th day of July, 2008.

Respectfully submitted,

JOSPEH P. RUSSONIELLO
United States Attorney



SHAWNA YEN
Assistant United States Attorney

EXHIBIT A

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR ORDER AUTHORIZING THE
USE AND MONITORING OF A MOBILE TRACKING DEVICE**

I, William Ng, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn and deposed, state the following:

1. I am submitting this Affidavit in connection with an application for an Order authorizing the use and monitoring of a mobile tracking device to ascertain the physical location of the Verizon Wireless broadband access card/cellular telephone assigned to Telephone Number (415) 264-9596 and Electronic Serial Number (ESN) 005-00717190 (the Target Broadband Access Card/Cellular Telephone). The following information has been provided to me by fellow FBI Special Agent Richard Murray. Special Agent Murray is assigned to the FBI Field Office located in Phoenix, Arizona.

2. Special Agent Murray is a Special Agent with the FBI and has been so employed since 1999. Since 2005, Special Agent Murray has been assigned to the Phoenix FBI Cyber Squad. He has participated in investigations relating to computer crimes including computer intrusions and frauds committed using computers and has been responsible for conducting criminal investigations regarding violations of law committed against the United States of America. Special Agent 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. Based upon his personal observations, consultation with other agents and law enforcement officers, and a review of records, Special Agent Murray has learned the following facts relating to an ongoing joint

criminal investigation being conducted by the Federal Bureau of Investigation (FBI), Internal Revenue Service - Criminal Investigation (IRS-CI), and United States Postal Inspection Service (USPIS). The investigation pertains to an unidentified individual (investigation moniker "the Hacker") presumably located within Northern California, who has assumed the identity of Travis Rupard, a resident of the State of Texas, who has masterminded a wide ranging scheme possibly in violation of 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 Identify Theft;
- f. 18 U.S.C. § 1029 – Fraud with Access Devices;
- g. 18 U.S.C. § 1030 – Unauthorized Computer Access;
- h. 18 U.S.C. § 1341 – Mail Fraud; and
- I. 18 U.S.C. § 1343 – Wire Fraud.

3. 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, who operates in the United States, is 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 through the use of identities of innocent third parties and deceased individuals, and directing the deposit of the proceeds of those fraudulent tax returns to bank accounts and debit cards where the funds can be accessed by the subject and co-conspirators.

A. Electronic Filing of Income Tax Returns

4. 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.

5. 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.

6. 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 a 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).

7. 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

8. In May 2007, IRS-CI became aware of questionable activity involving an account at Compass Bank, 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, and 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.

9. 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.

10. The IRS Fraud Detection Center in Austin, Texas (AFDC), researched the returns identified by EFile Tax Returns, Inc., and identified Ransom Carter's 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.

11. 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.

12. 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 AFDC identified approximately 1,272 returns, 175 IP addresses, and 73 bank accounts that 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.

C. CI 1 and CI 2

13. 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, the investigation team has found 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 as "JP" and another unknown individual CI 1 referred to as "The Hacker," hereinafter referred to as the "Target Subject," had been operating an automated system to file fraudulent tax returns using the names and Social Security Numbers of deceased individuals. CI 1 also advised that Ransom Carter had worked with CI 1 and JP in the past in order to promote various fraudulent schemes.

14. 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 "JP" 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.

15. 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 "JP," the Target Subject and their associates, and gather evidence concerning the nature and extent of the bulk filing scheme. Per "JP'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 (the "Meridian undercover bank account").

16. In the course of the scheme, "JP" asked CI 1 to open a safe-mail.net e-mail account. Safe-mail holds itself out as a highly secure communication, storage, sharing and distribution system for the internet and offers a variety of services including secure e-mail. The purported purpose of using this e-mail service, therefore, was to avoid detection. In February 2008, CI 1 e-mailed the account number and routing numbers for the Meridian undercover bank account to "JP." "JP" subsequently advised CI 1 that the Target Subject would begin to e-file fraudulent returns which directed refunds to be sent to the Meridian undercover bank account. Per CI 1, "JP" generally acted as the middleman between street-level individuals such as himself/herself and the Target Subject.

17. Throughout the initial stages of the undercover operation, CI 1 communicated with "JP" via telephone and his safe-mail.net account. Incoming e-mails from "JP" revealed his IP address as 76.27.37.158. Investigation of this IP address ultimately determined that IP address 76.27.37.158 was owned by Comcast Cable Communications, Inc. In late February 2008, in response to a subpoena, Comcast reported that IP address 76.27.37.158 was leased by "JP" at "JP's" residential address. It was determined that "JP" was, in fact, the subscriber.

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

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

20. 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 "JP." On April 14, 2008, a third shipment in the amount of \$9,000 in currency was sent overnight priority mail to "JP." On April 15, 2008, "JP" was arrested when leaving the destination location carrying the third and final delivery of \$9,000 in currency. The second and third shipments were in violation of 18 U.S.C. § 1341.

21. After his/her arrest on related federal charges, "JP" agreed to act as a confidential

informant and assist law enforcement in identifying and apprehending the Target Subject and will be hereinafter referred to as CI 2. CI 2 has advised he/she has never met the Target Subject in person and has never spoken to the Target Subject telephonically or via Voice Over Internet Protocol, i.e., the transmission of voice over the internet (VOIP). CI 2 maintains ongoing contact with the Target Subject via encrypted e-mail using a safe-mail.net e-mail account. Safe-Mail is owned and operated by Secure Information Technologies Limited, which is a privately owned company, registered in Israel and with offices in Israel the United Kingdom and Japan.

D. CONTROLLED DELIVERY OF \$68,000

22. The Target Subject has been led to believe that CI 2 has an associate, "Daniel," who works in the banking industry and is willing to assist CI 2 in moving the Target Subject's fraudulent tax return proceeds from the Meridian undercover bank account quickly and without detection.

23. On April 17, 2008, CI 2 sent an encrypted e-mail to the Target Subject explaining that he/she had received an additional \$9,000 in currency from the Meridian undercover bank account, and was expecting to receive an additional \$75,000 by April 22, 2008. CI 2 inquired how the Target Subject wanted his cut (\$68,000) of the money. The Target Subject provided CI 2 detailed instructions regarding how to physically wash \$68,000 in currency in 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.

24. Additionally, the Target Subject informed CI 2 he would send a courier, armed with an AR-15 in a duffle bag, to pick up the package. The Target Subject added the courier would be prepared to shoot anyone who attempted to arrest him while he was in possession of the package. The Target Subject informed CI 2 that 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 Target Subject would then provide information to the media to decrypt his prior message. The Target Subject advised that 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.

25. On May 5, 2008, the Target Subject sent CI 2 an encrypted e-mail with directions to send a package containing \$68,000 in currency to Patrick Stout, using an address of 249 South California Avenue, Palo Alto, California, to arrive on 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 Target Subject with the undercover package's tracking number via another encrypted e-mail.

26. The package containing \$68,000 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 male, wearing a

dark jacket with a hood, 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 on foot were unsuccessful in efforts to identify the unknown male or follow the unknown male to his final destination due to the fact that the area was practically deserted at that early hour.

27. On or about May 8, 2008, the Target Subject e-mailed CI 2 and confirmed receipt of the money. The Target Subject indicated in his e-mail that the money was picked up by a third party. The Target Subject advised CI 2 that the courier who retrieved the package believed that he was being followed by police. According to the Target Subject, the courier advised that 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. He said they looked like UK (United Kingdom) government agents by the way they were dressed." The Target Subject then advised that the courier was "likely just really paranoid."

28. CI 2 and the Target Subject 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 Target Subject, "Daniel" is able to make very

large one-time withdrawals only at the end of each quarter, the next quarter ending June 30, 2008.

29. On May 16, 2008, CI 2 informed the Target Subject that "Daniel" had moved \$364,260 (the remaining cut for CI 2 and the Subject) 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 Target Subject where future tax refunds could be deposited. Per the Target Subject's request, the funds in the Bank of America account would be swept weekly into another account controlled by "Daniel."

30. On May, 27, 2008, the Target Subject informed CI 2 that 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

31. On March 1, 2008, a fraudulent tax return for James Johnson was filed with the IRS using IP address 75.208.105.186, claiming a refund amount of \$2,099.00 and also a fraudulent tax return for Michael Deshields claiming a refund amount of \$1,988.00. Both refunds were destined for debit card accounts at MetaBank. The debit card accounts were linked by the investigation team to the Meridian undercover bank account through connected

IP addresses and bank accounts.

32. On March 5, 2008, a tax return for Robert Galletly was filed with the IRS using IP address 75.209.41.104, with a refund amount of \$1,093.00 destined for a debit card account at MetaBank. 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.

33. On March 26, 2008, 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.

34. Investigation revealed the IP addresses associated with the James Johnson return, Robert Galletly return, Michael Deshields returns and the Kevin Furman return, 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 an account in the name of Travis Rupard, customer account ID number 270691733, mobile device number (MDN) (415) 264-9596, subscriber SSN 455-89-7884, contact address Post Office Box 730031 in San Jose, California, telephone number (206) 666-3620.

35. USPS conducted an investigation of Post Office Box 730031 in San Jose, California and determined that this PO Box was opened on March 31, 2006 and was closed on August 31, 2006. The application indicated that 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 that 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.

36. Further investigation has revealed a PayPal account in the name of Travis Rupard, San Jose, California, to possibly be involved with identity theft. The Travis Rupard account had multiple bank accounts on the corresponding PayPal account from which funds were received and then either sent for an attempted purchase of gold coins or withdrawn into a secondary bank account. The original source of the funds was identified as being fraudulent tax returns. PayPal attempted to contact Travis Rupard but found the provided telephone number was not correct. The money funding the Travis Rupard PayPal account was from US Bank Account xxxxxx6706. The Travis Rupard account listed the following: Post Office Box 730031, San Jose, California, telephone number (408) 368-3479, e-mail Travis Rupard@safe-mail.net. Travis Rupard's related bank accounts included accounts at US Bank, Centennial Bank and a Visa Credit Card.

37. CI 2 has advised that he/she has been involved with the Target Subject in a number of fraudulent schemes over a period of several years and in the past he/she had sent money to the Target Subject by sending it to e-gold account number 3501337. 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 Target Subject \$7,640.00 on August 17, 2006. Records further indicate that 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, 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 additional fraudulent tax refunds related to the overall scheme. The Target Subject recently asked CI 2 to inquire about the Southwest Bank Account with "Daniel" to determine if the Target Subject could obtain proceeds in the account. The Target Subject has advised CI 2 that he has been unable to withdraw the proceeds from the scheme out of this account.

J. E-Mail Communications Between the Target Subject and CI 2

38. In an e-mail sent on unknown date and recently recovered from CI 2's records, the Target Subject advised CI 2 that he uses a different IP address for each tax return and has filed returns with many different efilers. The Target Subject believes that filing the returns in this manner would prevent "them," (i.e., the IRS), to link them all. The Target Subject advised that an e-filer "took some heat" from the IRS because of his automated filing scheme. The Target Subject stated that 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.

39. On or about May 14, 2008, the Target Subject sent an e-mail to CI 2 stating that he needed a web based account which had a list of proxies that the Target Subject could search by geographic location and then utilize the proxy IP address and port number of his choice. The Target Subject explained that these proxies could come from home personal computers that have proxy Trojans, (i.e., a malicious program which allows unauthorized activity unbeknownst to the computer's lawful owner/user) or from scanning computers which results in identifying open proxies. The Target Subject advised CI 2 that CI 2 should be willing to pay any amount to identify proxies in order to continue funding accounts. The Target Subject stated that he could scan for his own proxies but that he would need to use a T1 line (a dedicated high speed Internet line) to obtain the needed bandwidth and sit all day while the computer conducted the vulnerability scanning.

40. On or about June 10, 2008, the Target Subject sent an e-mail to CI 2 stating that "I funded other bank accounts at the same time from the same proxies and they all work out..." The investigation team believes that the Target Subject is referencing fraudulent tax returns sent to other accounts in addition to the Bank of America undercover bank account.

41. On or about June 11, 2008, the Target Subject sent an e-mail to CI 2 asking for personal identifying information of third parties. The Target Subject 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 Target Subject 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....” The reference to the film “Mad Max” appears to refer to the post-apocalyptic world depicted in that film.

42. Special Agent Murray has confirmed with a representative of Verizon Wireless that the Target Broadband Access Card/Cellular Telephone may be capable of being monitored by a mobile tracking device. In addition, the representative of Verizon Wireless believes that a telephone call to the Target Broadband Access Card/Cellular Telephone may generate a transmission between the card and one or more cell sites. The cell sites provide a link between the Target Broadband Access Card/Cellular Telephone and Verizon Wireless facilities, where the Verizon Wireless and then determine the general location of the Target Broadband Access Card/Cellular Telephone. The mobile tracking equipment ultimately generate a signal that fixes the geographic position of the Target Broadband Access Card/Cellular Telephone.

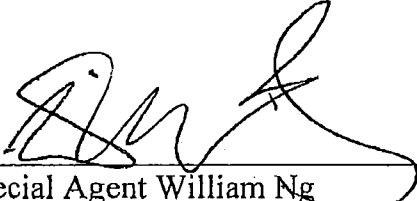
/

/

/

/

43. Based on the foregoing, your affiant believes that there is probable cause to believe that the use and monitoring of a mobile tracking device for the Target Broadband Access Card/Cellular Telephone will lead to evidence of violations of the statutes listed above; as well as to the identification of individuals who are engaged in the commission of these offenses.



Special Agent William Ng
Federal Bureau of Investigation

Sworn to before me and subscribed to in my presence, this 11th day of July, 2008



RICHARD SEEBORG
United States Magistrate Judge