



U. S. Department of Justice

*United States Attorney
Central District of California*

[REDACTED]
Assistant United States Attorney
Cyber and Intellectual Property Crimes Section

United States Courthouse
312 North Spring Street, 12th Floor
Los Angeles, California 90012

June 2, 2009

VIA PDF FILE

[REDACTED] U.S. Postal Inspector
U.S. Department of Justice
Criminal Division (CCIPS)
1301 New York Avenue, N.W. Suite 600
Washington, DC 20530

Re: [REDACTED] Investigation

Dear [REDACTED]

Enclosed please find the Rule 41 Warrant, supporting application and sealing application and order for the tracker warrant, matter no. 09-1145M, issued by Magistrate Judge Patrick Walsh on June 1, 2009. Postal Inspector [REDACTED] was the declarant for the warrant.

Good luck with the investigation and I hope the enclosed warrant leads to further evidence in the case.

Very truly yours,

THOMAS P. O'BRIEN
United States Attorney

[REDACTED]
Assistant United States Attorney
Cyber and Intellectual Property Crimes Section

cc: [REDACTED] CCIPS (w/enclosures also via PDF)

1 THOMAS P. O'BRIEN
United States Attorney

2 [REDACTED]
3 Assistant United States Attorney
Chief, Criminal Division

4 Assistant United States Attorney
Cyber and Intellectual Property Crimes Section
5 1200 United States Courthouse
312 North Spring Street
6 Los Angeles, California 90012
Telephone: [REDACTED]
7 Facsimile: [REDACTED]
8 Email: [REDACTED]

Attorneys for Applicant
9 United States of America

10 UNITED STATES DISTRICT COURT
11 FOR THE CENTRAL DISTRICT OF CALIFORNIA
12

13 IN RE CELLULAR TELEPHONE)
14)

No. **09-1145M**

) [WARRANT]
15)
16)

) (UNDER SEAL)
17)
18)

18 Upon application by the United States of America, supported
19 by the declaration of [REDACTED] Postal Inspector for the
20 U.S. Postal Inspection Service, for a warrant relating to the
21 following cellular telephone:

22 [REDACTED], a cellular telephone issued by Cellco
23 Partnership DBA Verizon Wireless, with ESN [REDACTED]
24 subscribed to in the name of [REDACTED] (a potential victim
25 of identity theft), at [REDACTED]
26 [REDACTED] and believed to be used by
27 suspects [REDACTED]
28

Cell phone signaling (location information)

[REDACTED] and/or others who are as of yet unidentified (hereinafter the "Subject Telephone").

THIS COURT FINDS THAT there is probable cause to believe that cell phone signaling information likely to be obtained concerning the location of the Subject Telephone, currently within, or being monitored or investigated within, the Central District of California, will constitute or yield evidence of violations of Mail Fraud (18 U.S.C. §1341), Wire Fraud (18 U.S.C. §1343), Access Device Fraud (18 U.S.C. §1029), and Conspiracy (18 U.S.C. §371), being committed by [REDACTED]

[REDACTED] and/or others who are as of yet unidentified.

THIS COURT FURTHER FINDS reasonable cause exists to believe that providing immediate notification of this warrant to the user(s) of the Subject Telephone may have an adverse result.

GOOD CAUSE HAVING BEEN SHOWN, THIS COURT HEREBY ISSUES THIS WARRANT AND FURTHER ORDERS THAT:

1. The U.S. Postal Inspection Service ("USPIS"), the Federal Bureau of Investigation ("FBI"), and the Department of Homeland Security, Immigration and Customs Enforcement (DHS/ICE") may obtain signaling information from the Subject Telephone, without obtaining the contents of any communication, to identify the location of the Subject Telephone.

2. As part of the receipt of the requested information, the USPIS/FBI/ICE is prohibited from seizing any tangible property pursuant to this warrant, or any other prohibited wire or electronic information as stated in 18 U.S.C. § 3103a(b)(2).

Cell phone signaling (location information)

1 The USPIS/FBI/ICE is not prohibited from doing so in relation to
2 any other investigation authorized by law.

3 3. The USPIS/FBI/ICE is permitted to delay service of this
4 warrant for signaling information to the subscriber of the
5 **Subject Telephone** for a period of 30 days from the date that the
6 disclosure ends. Any requests for a continuance of this delay
7 should be filed with this Court, unless directed to the duty
8 United States Magistrate Judge by this Court.

9 4. The USPIS/FBI/ICE shall make a return of this warrant
10 for signaling information to this Court (unless directed to the
11 duty United States Magistrate Judge by this Court) within 10
12 calendar days after the collection and/or disclosure of
13 information ceases. The return shall state the date and time the
14 collection and/or disclosure of the signaling information began
15 pursuant to this warrant, and the period during which the
16 information was collected and/or disclosed, including pursuant to
17 any orders permitting continued collection and/or disclosure.

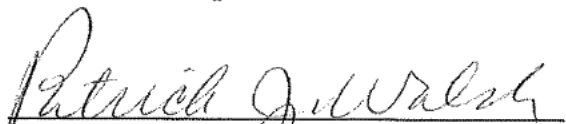
18 5. The collection and/or disclosure of the requested
19 information shall begin during the daytime on the earlier of the
20 day on which law enforcement officers first begin to receive
21 information pursuant to this warrant or ten days after the date
22 of this warrant, and continue for up to 45 days thereafter unless
23 additional orders are made continuing the period of the
24 collection and/or disclosure.

25 6. This authorization for the requested information shall
26 occur whether the **Subject Telephone** is located within this
27 District, outside of the District, or both.

28
Cell phone signaling (location information)

7. The collection and/or disclosure of the requested information shall not only be with respect to the **Subject Telephone**, but also with respect to any changed telephone number(s) assigned to an instrument bearing the same ESN as the **Subject Telephone**, or any changed ESN subsequently assigned to the same telephone number as the **Subject Telephone**, or any additional changed telephone number(s) and/or ESN, whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the **Subject Telephone** within the period of disclosure authorized by the warrant.

8. To avoid prejudice to this criminal investigation, the applicable cellular telephone service providers and their agents and employees shall not disclose to or cause a disclosure of this Court's warrant and orders, or the request for information by the USPIS/FBI/ICE or other law enforcement agencies involved in the investigation, or the existence of this investigation, except as necessary to accomplish the assistance hereby ordered. In particular, the cellular telephone service providers and their agents and employees are ordered not to make any disclosure to the lessees of the telephone or telephone subscribers.


THE HONORABLE PATRICK J. WALSH
UNITED STATES MAGISTRATE JUDGE

DATE/ TIME OF ISSUE: 6/1/09 4:30 p.m.

DECLARANT NAME/ AGENCY: [REDACTED] /USPS

Cell phone signaling (location information)

1 THOMAS P. O'BRIEN
United States Attorney

2 [REDACTED]
3 Assistant United States Attorney
Chief Criminal Division

4 Assistant United States Attorney
Cyber and Intellectual Property Crimes Section
5 1200 United States Courthouse
312 North Spring Street
6 Los Angeles, California 90012
Telephone: [REDACTED]
7 Facsimile: [REDACTED]
Email: [REDACTED]

8 Attorneys for Applicant
9 United States of America

10 UNITED STATES DISTRICT COURT
11 FOR THE CENTRAL DISTRICT OF CALIFORNIA
12

13 IN RE CELLULAR TELEPHONE)

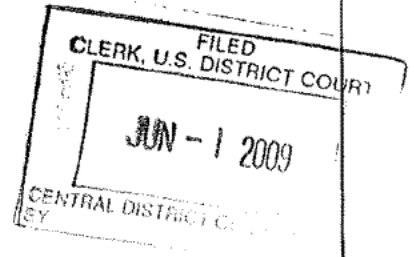
No. 09-1145M

) GOVERNMENT'S EX PARTE APPLICATION
) FOR A RULE 41 WARRANT AUTHORIZING
) THE COLLECTION AND/OR DISCLOSURE
) OF CELL PHONE SIGNALING
) INFORMATION TO LOCATE A CELLULAR
) PHONE; DECLARATION OF [REDACTED]
) [REDACTED]
)

) (UNDER SEAL)
18
19

20 The United States of America, by and through its counsel of
21 record, the United States Attorney for the Central District of
22 California, hereby applies for a warrant pursuant to Fed. R.
23 Crim. P. 41 authorizing the collection and/or disclosure of non-
24 content cell phone signaling information to assist in locating a
25 telephone. This process may occur with or without the assistance
26 of a service provider, and seeks information to establish the
27

28 Cell phone signaling (location information)



1 location of the following cellular telephone for a period of 45
2 days:

3 [REDACTED] a cellular telephone issued by Cellco
4 Partnership DBA Verizon Wireless, with Electronic
5 Serial Number ("ESN") [REDACTED] subscribed to in the
6 name of [REDACTED] (a potential victim of identity theft),¹
7 at [REDACTED]

8 [REDACTED] " and believed to be used by suspects [REDACTED]
9 [REDACTED]

10 [REDACTED] and/or others who are as of yet unidentified
11 (hereinafter the "Subject Telephone").

12 This application also seeks authorization under 18 U.S.C.
13 § 3103a(b), for reasonable cause shown, to delay notification of
14 the above Warrant to the subscriber and users of the Subject
15 Telephone for a period of 30 days from the date that the
16 collection and/or disclosure ends.²

17 //

18 //

19 //

21 ¹ Initials are being substituted in place of the full name
22 because this individual is believed to potentially be a victim of
23 identity theft. Thus, throughout this application, initials will
24 be used in place of full names when in doubt of the individual's
complicity in the crimes alleged.

25 ² The government wishes to alert the Court that the present
26 application and proposed order have been drafted to the specific
27 facts and circumstances of this case and are not a standard form
used in the U.S. Attorney's Office and have not been previously
submitted to the Magistrate Bench.

28 Cell phone signaling (location information)

1 This application is based on the attached memorandum of
2 points and authorities, and the attached Declaration of [REDACTED]
3 [REDACTED]

4 DATED: June 1, 2009

Respectfully submitted,

5 THOMAS P. O'BRIEN
6 United States Attorney

7 [REDACTED]
8 Assistant United States Attorney
9 Chief, Criminal Division
10 [REDACTED]

11 Assistant United States Attorney
12 Cyber and Intellectual Property
13 Crimes Section

14 Attorneys for Applicant
15 United States of America
16
17
18
19
20
21
22
23
24
25
26
27

28 Cell phone signaling (location information)

MEMORANDUM OF POINTS AND AUTHORITIES

I

INTRODUCTION

By this application, the government seeks a warrant under Rule 41 to obtain signaling information generated by a cellular phone (whether in use or not) in order to help locate the phone. As set forth in the attached affidavit, the **Subject Telephone** is being used by the subject(s) of a federal investigation being conducted by the U.S. Postal Inspection Service ("USPIS"), the Federal Bureau of Investigation ("FBI"), and the Department of Homeland Security, Immigration and Customs Enforcement ("DHS/ICE"), under circumstances where there is probable cause to believe that federal crimes are being committed, and that the information likely to be received concerning the location of the **Subject Telephone**, currently within, or being monitored or investigated within, the Central District of California, will constitute or yield evidence of those crimes.

The information under this warrant will allow agents to obtain the location of the **Subject Telephone** apart from the content of any communication, whether or not a call is in progress. The investigative agency may or may not require the assistance of a service provider to obtain the requested information. This information is sought based on the authority in Federal Rule of Criminal Procedure 41(b) and 28 U.S.C. § 1651 (the All Writs Act), and will be obtained in conformity with the procedures of Federal Rule of Criminal Procedure 41.

Also, this application seeks authorization under 18 U.S.C.

Cell phone signaling (location information)

1 § 3103a(b), for reasonable cause shown, to delay notification of
2 the above Warrant to the subscriber and users of the **Subject**
3 **Telephone** for a period of 30 days from the date that the
4 collection and/or disclosure ends. As discussed in the attached
5 declaration of United States Postal Inspector [REDACTED]
6 immediate notification of this order to the user of the **Subject**
7 **Telephone** may have an adverse result.

8 This application further seeks an order that: (1) authorizes
9 the collection and/or disclosure of the requested information
10 whether the **Subject Telephone** is located within this District,
11 outside of the District, or both; and (2) authorizes the
12 collection and/or disclosure of not only information with respect
13 to the **Subject Telephone**, but also with respect to any changed
14 telephone number(s) assigned to an instrument bearing the same
15 ESN as the **Subject Telephone**, or any changed ESN subsequently
16 assigned to the same telephone number as the **Subject Telephone**,
17 or any additional changed telephone number(s) and/or ESN, whether
18 the changes occur consecutively or simultaneously, listed to the
19 same subscriber and wireless telephone account number as the
20 **Subject Telephone** within the period authorized by the order.

21 The application is made in connection with an investigation
22 of offenses committed by suspects [REDACTED]
23 [REDACTED] and/or others who are
24 as of yet unidentified, for violations of mail fraud (18 U.S.C. §
25 1341), wire fraud (18 U.S.C. § 1343), access device fraud (18
26 U.S.C. § 1029), and conspiracy (18 U.S.C. § 371), and is based
27

28 Cell phone signaling (location information)

1 upon the certification by the attorney for the government as well
 2 as the attached declaration of [REDACTED].

3 II

4 DISCUSSION

5 A. Federal Rule of Criminal Procedure Rule 41 and the All Writs 6 Act

7 Federal Rules of Criminal Procedure 41(b) and (c) authorize
 8 the court to order the provision of information upon a showing of
 9 probable cause to believe that the information sought will lead
 10 to the discovery of evidence of identified criminal activity.³
 11 Because the cell phone location and signaling information is
 12 being sought under this authority, and because as discussed
 13 below, the procedures of Rule 41(e)(2)(B) and (f)(2) are being
 14 followed, the information may be obtained regardless of whether a
 15 call is in progress.

16 In addition, the All Writs Act permits courts to "issue all
 17 writs necessary or appropriate in aid of their respective
 18 jurisdictions and agreeable to the usages and principles of law."
 19 28 U.S.C. § 1651(a); see also Adams v. United States ex rel.
 20 McCann, 317 U.S. 269, 273 (1942) ("unless appropriately confined
 21 by Congress, a federal court may avail itself of all auxiliary
 22 writs as aids in the performance of its duties, when the use of
 23 such historic aids is calculated in its sound judgment to achieve
 24 the ends of justice entrusted to it.").

25
 26 ³ As set forth herein, the government does not concede that
 27 probable cause must be shown in order to collect the signaling
 28 information, but nonetheless provides probable cause in this
 case.

Cell phone signaling (location information)

1 The proposed warrant establishes a procedure that is in
2 conformity with Rule 41(e)(2)(B) and (f)(2). These procedures
3 include obtaining a court warrant for the information that states
4 (1) the **Subject Telephone** whose location is to be identified; (2)
5 that the information to be collected and/or disclosed shall be
6 for no longer than 45 days, unless extensions are obtained; (3)
7 that the collection and/or disclosure shall begin within 10 days;
8 (4) that a return will be provided to the court; and (5) that
9 notice will be provided after the collection and/or disclosure
10 has ended, unless an order allowing delayed notice is obtained.

11 B. Although Seeking A Warrant Under Rule 41, The Government
12 Does Not Concede That The Information Requested Implicates
13 the Fourth Amendment

14 The government does not concede that the Fourth Amendment
15 requires that a warrant be used to determine the location of the
16 **Subject Telephone** under the facts of this case. However, in an
17 abundance of caution, the government is complying with Rule 41,
18 and is providing to the Court an affidavit establishing probable
19 cause to believe that the **Subject Telephone** is being used in the
20 commission of crimes and/or that the location of the **Subject**
21 **Telephone** is evidence of such crimes.

22 As a general proposition, a cellular telephone emits signals
23 at various times, including when receiving or responding to a
24 Network page, when powering up/down, or when changing major
25 market areas. As part of that signaling, the telephone transmits
26 its unique network identifying number to the cell site in the
27 service provider's network to identify the particular telephone
28 for billing, routing, and other purposes. Even when not in

Cell phone signaling (location information)

1 active use, however, electronic processes or system commands may
2 be initiated by a provider and/or the government to
3 electronically derive the **Subject Telephone's** location. In either
4 scenario, the signaling information that the government seeks to
5 obtain does not contain the contents of any communication. By
6 obtaining that signaling information, the government can identify
7 the location of the **Subject Telephone**.

8 Given that this signaling information contains no content
9 information, and is routinely shared with a third-party (the
10 service provider) as part of the normal operation of the phone,
11 it is at best uncertain whether the user of the **Subject Telephone**
12 has a Fourth Amendment privacy interest in the signaling
13 information. See Smith v. Maryland, 442 U.S. 735, 744-45
14 (1979) (use of a conventional telephone pen register does not
15 constitute a search under the Fourth Amendment); id. at 743-44
16 id. at 742 (no reasonable expectation of privacy in information
17 such as phone numbers that a person "voluntarily turns over to
18 third parties"); United States v. Forrester, 512 F.3d 500, 511
19 (9th Cir. 2008) (no expectation of privacy for the computer or
20 e-mail addressing information shared with service provider as
21 part of normal operation of device). On the other hand, in some
22 circumstances, where the signaling information is used to
23 determine the exact location of a phone within a private
24 residence, or similar location, a Fourth Amendment interest may
25 arguably exist. Cf. United States v. Forest, 255 F.3d 942, 951-
26 952 (6th Cir. 2004) (in dicta suggesting without deciding, that a
27 person "might" have a legitimate expectation of privacy in cell-

28 Cell phone signaling (location information)

1 site data when used to track location). Thus, while reserving
2 its rights with respect to its position on this issue, based on
3 the specific facts of this case, the government has decided to
4 seek a warrant under Rule 41.

5 C. Delayed Notice

6 18 U.S.C. § 3103a(b) states that any notice required
7 following the issuance of a warrant may be delayed if, *inter*
8 *alia*, the court finds reasonable cause to believe that providing
9 immediate notification of the execution of the warrant may have
10 an adverse result. An adverse result is defined in 18 U.S.C.
11 § 2705(a)(2) as including endangering the life or physical safety
12 of a person, flight from prosecution, destruction of or tampering
13 with evidence, intimidation of potential witnesses, and serious
14 jeopardy of an investigation. Moreover, the Advisory Committee
15 Notes for Fed. R. Crim. P. 41(f)(3) (2006 Amendments) state that
16 delay of notice may be appropriate where "the officer establishes
17 that the investigation is ongoing and that disclosure of the
18 warrant will compromise that investigation." The attached
19 declaration of [REDACTED] provides reasonable cause to believe
20 that immediate notification of the execution of the warrant may
21 have an adverse result, and the proposed warrant both provides
22 for the giving of such notice within 30 days after the date that
23 the collection and/or disclosure ends and prohibits, as part of
24 the receipt of the requested information, the seizure of any
25 tangible property or any other prohibited wire or electronic
26 information as stated in 18 U.S.C. § 3103a(b)(2).

27
28 Cell phone signaling (location information)

III

CONCLUSION

Applicant respectfully requests that the Court issue the
warrant in the form presented herewith.

DATED: June 1, 2009

Assistant United States Attorney
Cyber and Intellectual Property Crimes
Section

Cell phone signaling (location information)

DECLARATION OF [REDACTED]

I, [REDACTED] do hereby declare and affirm:

1. I am a Postal Inspector ("PI") with the United States Postal Inspection Service ("USPIS"), and have been so employed for approximately 17 years. I am currently assigned to the Global Security and Investigations Division, in Long Beach, California, in which I investigate mail theft, identification theft, mail fraud and other postal-related crimes. For the past 17 years, I have worked assignments including internal and external mail theft, workers' compensation fraud, assaults, drugs in the mails, and child pornography in the mails. I have conducted hundreds of postal-related criminal investigations. I have also attended training, classes and seminars concerning mail fraud and other postal-related crimes. I have a four-year Bachelor of Arts Degree in Criminal Justice from California State University, Fullerton.

PURPOSE OF DECLARATION

2. This declaration is made in support of an application for a warrant authorizing the collection and/or disclosure of cell phone signaling information, as defined within the application, at such intervals and times as requested and/or determined by the government, which will establish the location of the following cellular telephone for a period of 45 days:

[REDACTED] a cellular telephone issued by Cellco Partnership DBA Verizon Wireless (hereinafter "Verizon"), with ESN [REDACTED] subscribed to in the

Cell phone signaling (location information)

1 name of [REDACTED] (a potential victim of identity theft),⁴
2 at [REDACTED]

3 [REDACTED] " and believed to be used by suspects [REDACTED]
4 [REDACTED]

5 [REDACTED] and/or others who are as of yet unidentified
6 (hereinafter the "Subject Telephone").

7 I also seek authorization under 18 U.S.C. § 3103a(b), for
8 reasonable cause shown below, to delay notification of the
9 proposed warrant for a period of 30 days from the date that the
10 disclosure ends.

11 3. The facts set forth in this declaration are based upon
12 my own personal observations, my training and experience, and
13 information obtained during this investigation from other law
14 enforcement officers and sources. This declaration is intended
15 to show that there is cause to obtain the information herein
16 sought, and does not purport to set forth all my knowledge of, or
17 investigation into, this matter.

18 PROBABLE CAUSE

19 4. On or about July 30, 2008, e*Trade Financial
20 Corporation, 4005 Windward Plaza Drive, Alpharetta, Georgia 30005
21 ("e*Trade"), reported a financial loss in excess of \$434,000
22 involving two e*Trade accounts. The first account was
23 established on March 20, 2008, using the name [REDACTED], with a date
24 _____

25 ⁴ Initials are being substituted in place of the full name
26 because this individual is believed to potentially be a victim of
27 identity theft. Thus, throughout this application, initials will
be used in place of full names when in doubt of the individual's
complicity in the crimes alleged.

28 Cell phone signaling (location information)

1 of birth of [REDACTED] social security number [REDACTED] and
2 listing [REDACTED] (i.e., the Subject Telephone) as the home
3 telephone number ("e*Trade Account #1"). e*Trade Account #1
4 involved a financial loss of approximately \$300,808.58 to
5 e*Trade. The second account was established on May 27, 2008,
6 using the name [REDACTED] with a date of birth of [REDACTED] and a
7 social security number of [REDACTED] ("e*Trade Account #2").
8 e*Trade Account #2 involved a financial loss of approximately
9 \$134,888.38 to e*Trade. Both e*Trade accounts listed the mailing
10 address of [REDACTED]
11 [REDACTED]

12 5. Investigation revealed that unknown suspects
13 transferred, via online automated clearinghouse ("ACH")
14 transactions, over \$600,000 into the two e*Trade accounts from
15 accounts at Wachovia Bank [REDACTED], Citibank [REDACTED]
16 and Washington Mutual Bank [REDACTED]. Approximately \$465,000
17 was then transferred from the e*Trade accounts, via ACH transfer
18 and wire transfer, to a Citibank account [REDACTED] and a Wells
19 Fargo account [REDACTED]. Of the \$465,000 transferred,
20 approximately \$287,500 was sent, via wire transfer, from the Well
21 Fargo account to an account at the Central Bank in the United
22 Arab Emirates. The originating ACH transactions from Wachovia
23 Bank, Citibank and Washington Mutual Bank, used to fund the
24 e*Trade accounts, were all returned as unauthorized transactions,
25 resulting in significant financial losses in excess of \$400,000
26 to e*Trade.

27 6. On December 4, 2008, [REDACTED], an
28

Cell phone signaling (location information)

1 employee of RBS Lynk Inc., advised that RBS Lynk, Inc. also known
 2 as RBS World Pay (hereinafter "RBS Lynk"),⁵ sustained financial
 3 losses involving an account using the same Subject Telephone used
 4 on e*Trade Account #1.

5 7. Specifically, [REDACTED] stated that on or about April 15,
 6 2008, RBS received a completed application in the name [REDACTED]
 7 [REDACTED]

8 [REDACTED] Social Security Number [REDACTED] The
 9 application requested credit card processing capabilities for
 10 Visa, MasterCard, Discover, JCB Consumer Credit and Commercial
 11 Cards and Signature Debit Cards, as well as American Express
 12 processing services. [REDACTED] stated that the applicant provided
 13 California driver's license number [REDACTED] in the name [REDACTED] as a
 14 method of identification, along with a blank check from Bank of
 15 America, account [REDACTED]; the top center of the check was
 16 printed with the name [REDACTED]

17 [REDACTED] " [REDACTED] explained to me
 18 that when an applicant applies for a credit card processing
 19 terminal through RBS Lynk, the applicant must provide a copy of a
 20 blank check from their account.⁶

21 8. [REDACTED] further advised that on April 16, 2008, after
 22

23 ⁵ A company that provides merchants with credit card
 24 processing terminals, and is located at 600 Morgan Falls Road,
 25 Suite 260, Atlanta, Georgia 30350.

26 ⁶ I later obtained Bank of America bank statements for
 27 account [REDACTED], which revealed that the account is not in
 28 the name [REDACTED] as printed on the checks, but rather,
 is actually in the name of [REDACTED], [REDACTED] at an
 address in North Hollywood, California.

1 an account was opened, RBS Lynk shipped a credit card processing
2 terminal, via FedEx, addressed to [REDACTED]
3 [REDACTED] [REDACTED]

4 [REDACTED] further stated that in May of 2008, this RBS Lynk terminal
5 was used to process three unauthorized credit card charges
6 totaling \$9,136.00, resulting in an estimated financial loss to
7 RBS Lynk of \$4,920.00. When cross-checking the telephone
8 numbers, it was determined that the telephone number provided to
9 RBS Lynk as a contact number for the manager of [REDACTED]
10 was the same telephone number used on e*Trade Account #1, i.e.
11 the Subject Telephone.

12 9. According to [REDACTED] RBS Lynk risk analysts researched
13 the information listed on the initial account application and
14 determined that the date of birth [REDACTED] provided on the
15 application did not match the records received from Equifax,
16 which listed [REDACTED] date of birth as [REDACTED] RBS Lynk risk
17 analysts also researched [REDACTED] on the Internet and
18 determined that there was "no information documented on the
19 business through internet searches."

20 10. According to [REDACTED] RBS Lynk either limited or froze
21 the funds for the already processed credit card transactions.
22 This resulted in RBS Lynk receiving several telephone calls from
23 a male, who identified himself as [REDACTED] and claimed to be the
24 Manager of [REDACTED] During a call from [REDACTED] on May
25 14, 2008, [REDACTED] provided RBS Lynk with telephone number
26 [REDACTED] (i.e., the Subject Telephone) as an alternate
27
28

Cell phone signaling (location information)

1 contact telephone number. As noted above, this is the same
2 telephone number provided on e*Trade Account #1.

3 11. Verizon telephone subscriber records were obtained for
4 the Subject Telephone. The records revealed that the Subject
5 Telephone is registered to [REDACTED], at [REDACTED]
6 [REDACTED] which is the same name and
7 address previously provided to RBS Lynk, and which eventually led
8 to the above-described loss by RBS Lynk.

9 12. An analysis of the telephone toll records for the
10 Subject Telephone for the period of May 1, 2008 to October 2,
11 2008 indicates that it made several telephone calls to RBS
12 Lynk/RBS World. The toll records also show that the Subject
13 Telephone was used to make a number of calls to Bank of America,
14 which is the bank designated to facilitate the processing of the
15 [REDACTED] credit card charges through the RBS terminal.
16 The toll records further show that the Subject Telephone called
17 other financial institutions involved in the e*Trade
18 transactions, including e*Trade itself, Citibank, Washington
19 Mutual Bank, and others. In addition to RBS Lynk, the Subject
20 Telephone also made telephone calls to other credit card
21 companies and credit card processing terminal providers.

22 13. According to Verizon records, the Subject Telephone is
23 registered in the name of [REDACTED], a person believed to be a victim
24 of identity theft who, according to Experian Inc., filed an
25 identity theft claim on or about November 14, 2008.

26
27
28 Cell phone signaling (location information)

1 14. Pursuant to court orders⁷, the U.S. Postal Inspection
2 Service began receiving cell site data from Verizon on April 15,
3 2009 relative to the **Subject Telephone**. Between April 15, 2009
4 through May 17, 2009, approximately 650 telephone calls were made
5 and/or received involving the **Subject Telephone**.

6 15. In performing an analysis of the data gathered about
7 the **Subject Telephone**, it was discovered that the **Subject**
8 **Telephone** had called [REDACTED] on May 8, 2009. This is
9 significant because telephone number [REDACTED] has previously
10 been listed by suspects as the contact number for the e*Trade
11 account opened using the identity of [REDACTED], which resulted in the
12 financial loss of \$300,808.58 to victim e*Trade.

13 16. Telephone number [REDACTED] was also provided to
14 Verizon as an alternate contact number for the **Subject Telephone**
15 subscribed to under the name of [REDACTED]

16 17. Additionally, telephone number [REDACTED] was
17 provided to victim RBS Lynk by someone purporting to be [REDACTED] DBA
18 [REDACTED]

19 18. Data gathered about the **Subject Telephone** also reveals
20 that it received a call from telephone number [REDACTED] on
21 _____

22 ⁷ On March 31, 2009, an order was issued by Magistrate
23 Judge Jeffrey W. Johnson of the Central District of California
24 for a pen register and trap and trace on the **Subject Telephone**.
25 That order was for a period of sixty days expiring on May 31,
26 2009. On May 21, 2009, Magistrate Judge Frederick Mumm of the
27 Central District of California signed an order extending the pen
28 register and trap and trace on the **Subject Telephone** for an
additional 60 days. On April 8, 2009, an order was issued by
Magistrate Judge Carla Woehrle of the Central District of
California for cell site information for the **Subject Telephone**;
that order is for a period of sixty days expiring on June 8,
2009.

Cell phone signaling (location information)

1 April 13, 2009. Telephone number [REDACTED] is the same phone
2 number listed on an e*Trade account in the name of [REDACTED]
3 [REDACTED] which was opened on or about June 18, 2008. Of
4 significance to this investigation, some of the same Internet
5 Protocol ("IP") addresses used to log into the [REDACTED]
6 e*Trade account were also used to log into e*Trade accounts under
7 the identities of [REDACTED] and [REDACTED]; two accounts that resulted in
8 the financial loss to victim e*trade of at least \$435,696.96.
9 Likewise of interest, two telephone calls were made by the
10 Subject Telephone to victim e*Trade on April 8, 2009 and May 15,
11 2009.

12 19. Based upon the foregoing, there is probable cause to
13 believe that the Subject Telephone is being used in the
14 commission of crimes, including, but not limited to Mail Fraud
15 (18 U.S.C. §1341), Wire Fraud (18 U.S.C. §1343), Access Device
16 Fraud (18 U.S.C. §1029), and Conspiracy (18 U.S.C. §371), that
17 the individual(s) using the Subject Telephone is/are complicit in
18 these crimes, and that there is evidence of such crimes located
19 on the Subject Telephone.

20 20. The cell site information collected for the Subject
21 Telephone over the preceding weeks reveals that communications
22 to/from the Subject Telephone have occurred utilizing a small
23 handful of towers located in, or adjacent to, North Hollywood,
24 California, and within this judicial district. For example, a
25 review of the cell site data provided by Verizon reveals that
26 between April 15, 2009 and May 17, 2009, approximately 240
27 telephone calls were made and/or received by the Subject

28 Cell phone signaling (location information)

1 **Telephone** using Verizon Cell Site Tower 36 in Quadrant Y.
2 According to Verizon, Cell Site Tower 36 is located in North
3 Hollywood, California at 34.153618 Latitude and -118.368412
4 Longitude. Unfortunately, however, each Quadrant encompasses a
5 large number of streets/blocks, and thus the known cell tower
6 locations (that is, the physical addresses of the towers and
7 their service coverage areas) are too imprecise to physically
8 locate the **Subject Telephone** or its user(s).

9 21. Your Declarant understands, however, that the **Subject**
10 **Telephone** emits signals at various times, including when in use
11 (for example, when receiving or responding to a Network page,
12 when powering up/down, or when changing major market areas), and
13 that even when not in use, electronic processes may be initiated
14 by Verizon or USFIS and/or the Federal Bureau of Investigation
15 ("FBI"), and the Department of Homeland Security, Immigration and
16 Customs Enforcement (DHS/ICE") to obtain available location
17 information from the **Subject Telephone**. Verizon and/or the
18 USFIS/FBI/DHS/ICE, working either alone or, at times, in
19 conjunction with one another, may be able to electronically
20 derive the **Subject Telephone's** location from this network or
21 signaling information, thereby physically locating the **Subject**
22 **Telephone** and its user(s). As such, we respectfully request
23 authorization to deploy, operate or issue any network
24 infrastructure signaling or system commands necessary to isolate
25 and physically locate the **Subject Telephone**, regardless of
26 whether the **Subject Telephone** is inside a non-public structure or
27 private dwelling.

28 Cell phone signaling (location information)

G R O U N D S F O R D E L A Y I N G N O T I C E

22. Based on my training and experience and my investigation of this matter, I believe that reasonable cause exists to delay the service of the warrant, as normally required, for a period of 30 days beyond the end of the collection and/or disclosure period because I believe that providing immediate notification of the warrant is likely to have the adverse result of placing the investigation in serious jeopardy. The investigation is ongoing, and disclosure of the warrant will compromise that investigation. Additionally, based upon the known modus operandi of the suspects, I believe there is a real risk that providing immediate notification will risk potential destruction of or tampering with evidence, coordination of false exculpatories, and/or flight from prosecution.


23. Specifically, the suspects in this investigation use multiple compromised identities to facilitate the frauds. They have access to other person's identifiers and means with which to utilize these identities, such as fraudulent identification documents. Some of the suspects of this investigation are believed to be foreign nationals and/or residing in the United States without legal immigration documentation. In addition, the **Subject Telephone** has engaged in, and continues to engage in, numerous telephone calls with unknown entities in Moldova, Russia, Sweden and Armenia indicating an international network where suspects may seek refuge from United States prosecution. Likewise, a significant portion of the known stolen funds in this investigation were transferred, by suspects, to accounts in the

Cell phone signaling (location information)

1 United Emirates, Latvia and Slovakia, again indicating resources
2 in foreign countries that could facilitate a departure from the
3 United States if they became aware of this ongoing investigation.

4 I declare and affirm under penalty of perjury that the
5 foregoing is true and correct to the best of my knowledge.

6 Executed on June 1, 2009, at Los Angeles, California.

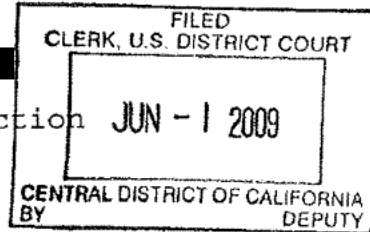
7 
8 _____
9 Postal Inspector,
10 U.S. Postal Inspection Service
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Cell phone signaling (location information)

THOMAS P. O'BRIEN
 United States Attorney
 Assistant United States Attorney

Chief, Criminal Division

Assistant United States Attorney
 Cyber and Intellectual Property Crimes Section
 1200 United States Courthouse
 312 North Spring Street
 Los Angeles, California 90012
 Telephone: [REDACTED]
 Facsimile: [REDACTED]
 E-mail: [REDACTED]



Attorneys for Plaintiff
 UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT
 FOR THE CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

No. **09-1145M**
 IN RE CELLULAR TELEPHONE)
)
) GOVERNMENT'S EX PARTE APPLICATION
) FOR ORDER SEALING DOCUMENTS;
) DECLARATION OF [REDACTED]
)
) [UNDER SEAL]

The government hereby applies ex parte for an order directing that the application, order, and supporting affidavit in the above-titled case, together with this ex parte application, the memorandum of points and authorities, the declaration of [REDACTED] and this court's sealing order, be kept under seal until such time as the government informs the Clerk's Office that it is appropriate to unseal these documents.

1 This ex parte application is based on the attached
2 memorandum of points and authorities, and the attached
3 declaration of [REDACTED]

4 DATED: June 1, 2009

5 Respectfully submitted,

6 THOMAS P. O'BRIEN
7 United States Attorney

8 [REDACTED]
9 Chief, Criminal Division

10 [REDACTED]
11 Assistant United States Attorney
12 Cyber and Intellectual Property Crimes
13 Section

14 Attorneys for Plaintiff
15 UNITED STATES OF AMERICA
16
17
18
19
20
21
22
23
24
25
26
27
28

MEMORANDUM OF POINTS AND AUTHORITIES

The government requests that this court seal the application, warrant for location information regarding the subject telephone, and supporting affidavits in this case in order to maintain the integrity of this investigation. Approval from this court to seal these documents is required under Local Rule 79-5.1. The Court of Appeals for the Ninth Circuit has held that district courts have the inherent power to seal affidavits in support of warrants. In re Sealed Affidavit (Agosto), 600 F.2d 1256 (9th Cir. 1979) (per curiam); see also Offices of Lakeside Non-Ferrous Metals, Inc., 679 F.2d 778 (9th Cir. 1982) (citing Agosto).

The Court of Appeals for the Seventh Circuit has rejected the proposition that pre-indictment disclosure of a search warrant affidavit is required under either constitutional principles or Federal Rule of Criminal Procedure 41(g). In re EyeCare Physicians of America, 100 F.3d 514 (7th Cir. 1996). In doing so, the Seventh Circuit held:

By the very nature of a secret criminal investigation of this type, the target of an investigation more often than not remains unaware of the specific grounds upon which a warrant was issued. If preindictment disclosure of sealed warrant affidavits was required to satisfy due process (assuming there has been a predicate deprivation of life, liberty or property), the hands of law enforcement would be needlessly tied and investigations of criminal activity would be made unduly difficult if not impossible.

Id. at 517. Accord In re Grand Jury Proceedings, 115 F.3d 1240,

1 1247 (5th Cir. 1997).

2 Here, for the reasons described in the attached declaration,
3 sealing is necessary to maintain the integrity of the
4 government's investigation. The government accordingly requests
5 that the documents described in the attached declaration be
6 maintained under seal until the government notifies the Court
7 that it is appropriate to unseal them.

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

DECLARATION OF [REDACTED]

I, [REDACTED], declare as follows:

1. I am an Assistant United States Attorney in the United States Attorney's Office for the Central District of California (USAO). I am assigned to the Cyber and Intellectual Property Crimes Section of the USAO. As part of my responsibilities in that section, I have become responsible for assisting U.S. Postal Inspector [REDACTED] in obtaining the cell phone location information search warrant for the **Subject Telephone** in the investigation of various fraud crimes described in the application being concurrently filed herewith.

2. The cellular phone warrant above is part of a long, on-going fraud investigation. A significant part of the investigation has been conducted through pen registers, trap and trace devices, and an order for cell site information, the existence of which remains unknown to the suspects. Due to the nature of this investigation, and the fact that the pen/trap and cell site applications and orders remain under seal, this investigation might be jeopardized if the order requested today, or the affidavit in support thereof were made publicly available.

3. Based upon the known modus operandi of the suspects, there is a real risk that premature disclosure of the cell phone location information search warrant and affidavit in this case will, among other things: (1) jeopardize the success of the cell phone location information sought, (2) cause the targets of this investigation to flee, and/or (3) lead to the destruction of evidence. In particular, as set forth in the declaration of [REDACTED] some of the suspects of this investigation are

1 believed to be foreign nationals and/or residing in the United
2 States without legal immigration documentation. In addition, the
3 **Subject Telephone** has engaged in, and continues to engage in,
4 numerous telephone calls with unknown entities in Moldova,
5 Russia, Sweden and Armenia indicating an international network
6 where suspects may seek refuge from United States prosecution.
7 Likewise, a significant portion of the known stolen funds in this
8 investigation were transferred, by suspects, to accounts in the
9 United Emirates, Latvia and Slovakia, again indicating resources
10 in foreign countries that could facilitate a departure from the
11 United States if they became aware of this ongoing investigation.

12 4. Accordingly, the government requests that the search
13 warrant and supporting affidavit in the above-titled case,
14 together with this ex parte application, the memorandum of points
15 and authorities, and the declaration of [REDACTED] and this
16 court's sealing order, be kept under seal until such time as the
17 government notifies the Court that it is appropriate to unseal
18 the documents. The government requests that the court's order
19 not limit its ability to provide copies of the search warrant at
20 the time the warrant is executed as required by Federal Rule of
21 Criminal Procedure 41(d).

22 I declare under penalty of perjury that the foregoing is
23 true and correct to the best of my knowledge and belief.

24 DATED: June 1, 2009
25 [REDACTED]
26
27
28

THOMAS P. O'BRIEN
United States Attorney
Assistant United States Attorney

Chief, Criminal Division

Assistant United States Attorney
Cyber and Intellectual Property Crimes Section
1200 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: [REDACTED]
Facsimile: [REDACTED]
E-mail: [REDACTED]

Attorneys for Plaintiff
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
WESTERN DIVISION

No. **09-1145M**
IN RE CELLULAR TELEPHONES)
[Proposed] ORDER SEALING)
DOCUMENTS; DECLARATION OF [REDACTED])
[REDACTED])
[UNDER SEAL])

For good cause shown, IT IS HEREBY ORDERED THAT:

The search warrant, application and supporting affidavits in the above-titled case, together with this ex parte application, the memorandum of points and authorities, and the declaration of [REDACTED] and this Court's sealing order, be kept under seal until such time as the government notifies the Court that it is appropriate to unseal the documents. The executing agents or

officers are permitted to provide a copy of the search warrant as required by Federal Rule of Criminal Procedure 41(d) and/or in compliance with the Court's order granting the warrant.

DATED: 6/1/09

DAVEICK J. WALSH

UNITED STATES MAGISTRATE JUDGE

IN CASE OF DENIAL:

The government's application for sealed filing is DENIED. The underlying document(s) and the sealing application shall be returned to the government, without filing of the documents or reflection of the name or nature of the documents on the clerk's public docket.

DATED: _____

UNITED STATES MAGISTRATE JUDGE