Approved: ______________________________
DAVID M. SIEGAL
Assistant United States Attorney

Before: HONORABLE ANDREW J. PECK
United States Magistrate Judge
Southern District of New York

- -x **FILED UNDER SEAL**

UNITED STATES OF AMERICA : AMENDED COMPLAINT

- v - : Violation of 18 U.S.C. § 371

JASON SMATHERS and SEAN DUNAWAY, :

Defendants. : COUNTY OF OFFENSE: NEW YORK

:
- -x

SOUTHERN DISTRICT OF NEW YORK, ss.:

PETER CAVICCHIA, being duly sworn, deposes and states that he is a Special Agent of the United States Secret Service (the "Secret Service"), and charges as follows:

COUNT ONE

1. From at least in or about April 2003 up to and including in or about April 2004, in the Southern District of New York and elsewhere, JASON SMATHERS, and SEAN DUNAWAY, the defendants, unlawfully, willfully, and knowingly did combine, conspire, confederate and agree together and with each other to violate the laws of the United States, to wit, Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(A), 1037(a)(2), (b)(2)(C) and (b)(2)(E), and 2314.

2. It was a part and an object of the conspiracy that JASON SMATHERS and SEAN DUNAWAY, the defendants, and others known and unknown, unlawfully, willfully and knowingly, in and affecting interstate commerce, used a protected computer to relay and re-transmit multiple commercial electronic mail messages with the intent to deceive and mislead recipients and internet access services as to the origin of such messages, in which the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during a 24-hour period, 25,000 during a 30-day period, and 250,000 during a 1-year period, and as a result of which one and more of the co-conspirators obtained things of value aggregating $5,000 and more during a 1-year period, in violation of Section 1037(a)(2), (b)(2)(C) and (b)(2)(E) of Title 18, United States Code.

3. It was a further part and an object of the conspiracy that JASON SMATHERS and SEAN DUNAWAY, the defendants, and others known and unknown, unlawfully, willfully and knowingly, would and did transport, transmit and transfer, in interstate and foreign commerce, goods, wares, merchandise, securities and money, of the value of $5,000 and more, knowing the same to have been stolen, converted and taken by fraud, and, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false or fraudulent pretenses, representations, and promises, would and did transport in interstate and foreign commerce in the execution and concealment of such scheme and artifice to defraud that person and those persons of money and property having a value of $5,000 and more, in violation of Section 2314 of Title 18, United States Code.

4. It was a further part and an object of the conspiracy that JASON SMATHERS and SEAN DUNAWAY, the defendants, and others known and unknown, unlawfully, willfully and knowingly, accessed a computer without authorization and exceeded authorized access, and thereby obtained information from a protected computer, involving interstate and foreign communications, in violation of Section 1030(a)(2)(C) and (c)(2)(A) of Title 18, United States Code.

OVERT ACTS

5. In furtherance of said conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about May 19 and 20, 2003, JASON SMATHERS, the defendant, obtained unauthorized access to an electronic database of America On Line, and without permission, misappropriated a list of customer accounts for purposes of selling to others.

b. In or about May 2003, JASON SMATHERS, the defendant, sold the misappropriated list of America On Line customers referred to in the previous sub-paragraph to SEAN DUNAWAY, the defendant.

c. In or about May or June 2003, SEAN DUNAWAY, the defendant, sold the misappropriated list of America On Line customers referred to in the previous sub-paragraphs to a co-conspirator not named as a defendant herein.

d. On or about March 1, 2004, SEAN DUNAWAY, the defendant, sold a revised version of the misappropriated list to a co-conspirator not named as a defendant herein for approximately $32,500.

e. In or about early 2004, a co-conspirator not named as a defendant herein used the misappropriated America On Line customer lists to send millions of unsolicited

commercial electronic mail transmissions to America On Line customers in the Southern District of New York and elsewhere.

(Title 18, United States Code, Section 371.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

6. I am a Special Agent with the Secret Service, and I have been involved personally in the investigation of this matter. I am familiar with the facts and circumstances set forth below from my personal participation in the investigation, including interviews I have conducted, my examination of reports and records, and my conversations with other law enforcement officers. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, unless noted otherwise.

Overview of the Scheme

7. As set forth below, there is probable cause to believe that an employee of America On Line ("AOL"), JASON SMATHERS, the defendant, illegally and without authorization, obtained access to protected and confidential computerized business data belonging to AOL, namely, certain identifying data for each of approximately 30 million AOL customers -- i.e., AOL's entire customer base -- misappropriated that information, and sold it for $100,000 and more to other people, including but not limited to SEAN DUNAWAY, the defendant. The purpose for which DUNAWAY purchased this stolen information was, as described herein, so that he and others could use AOL's customer list to send massive amounts of unsolicited commercial e-mails, also known as "SPAM," to AOL's customers.

8. As described more specifically below, my belief that probable cause exists is based on the following, among other things: (1) a confidential source of information (the "Source") informed me that he/she possessed a highly confidential, proprietary list of AOL customers' account information; (2) the Source provided me with a copy of that list, which I observed, by its nature, demonstrably establishes that the information had been stolen from AOL; (3) that list would have been difficult, if not impossible, to steal from AOL absent sophisticated inside access to AOL's secure computer system; (4) the Source was told by the person from whom he/she obtained the list, SEAN DUNAWAY, the defendant, that the list had originally been stolen by an AOL employee insider; (5) JASON SMATHERS, the defendant, was a software engineer employed by AOL at the time the list was stolen; (6) computer records discovered in the AOL work computer assigned to SMATHERS included highly unusual computerized codes and instructions necessary for and capable of stealing the list from AOL's secure database; (7) computer logs of remote network access, as well as records of computer processes conducted against the AOL database that contain the stolen list, show that

SMATHERS conducted those processes using his AOL account, and using the highly unusual computerized codes and instructions found in his computer, at the time the list was stolen; (7) other computer records found in SMATHERS's work computer reflect e-mail dialog between SMATHERS and DUNAWAY, in which SMATHERS discussed with DUNAWAY planning the theft and testing the computer processes to execute the theft, and discussing the profit motive for doing so; and (8) other records found in SMATHERS' computer showed SMATHERS communicating with DUNAWAY utilizing internet communications methods and channels that are designed for secret, encrypted communications.

Background

9. AOL is a commercial Internet Service Provider ("ISP") that offers to its subscribers, among other things, access to the Internet, as well as e-mail services. AOL is one of the world's largest ISPs, and according to AOL investigators with whom I spoke, approximately 30 million customers worldwide subscribe to AOL's service, which includes, among other services, e-mail services and access to the Internet and World Wide Web, and instant messaging. AOL issues each of its subscriber one or more unique User IDs (also referred to as "screen names"), which serve, among other things, as a portion of an e-mail address associated with that customer's AOL account. Each such e-mail address (for example, "user@aol.com") can be used by the AOL customer both to send and receive e-mail to and from that e-mail address, as well as to utilize other services of AOL. In AOL's system, an AOL account holder can be assigned multiple screen names at any given time. Thus, while the total number of screen names in AOL's system changes over time, and the total number of screen names substantially exceeds the total number of AOL's subscriber accounts, in or about May 2003 (when certain of the events described below took place), there were approximately 92 million screen names in AOL's system. Approximately 1 million of those AOL screen names are assigned to AOL subscribers (approximately 350,000 of them) located in zip codes in Manhattan, New York.

10. According to AOL investigators**,** AOL closely guards its customer lists, including the screen names and other client profile information, for several reasons, including that (1) AOL understands that its customers do not, as a general rule, wish to have their names and other personal identification information circulated to anyone who might make use of that information, and (2) AOL's customer list is a proprietary database, derived from years and millions of dollars worth of financial and labor investment, and is one of AOL's most important business assets. AOL's customer list contains a very valuable set of information in the marketplace, especially to marketers and advertisers of products and services of all varieties. A person in possession of contact information for AOL's millions of customers would have the ability to reach, all at once, an enormous potential customer base for whatever he would be seeking to promote. For example, perpetrators of SPAM, in possession of that list in the correct format, would be able to send masses of unsolicited marketing e-mails to millions of people, with the knowledge that there are real recipients of those e-mails, and potential customers, on the receiving end.

11. JASON SMATHERS, the defendant, resides in Harpers Ferry, West Virginia.

12. JASON SMATHERS, the defendant, has been an employee of AOL since 1999, and during the relevant time period (including between in or about April 2003 and the present), SMATHERS has been employed as a software engineer, working at AOL's Dulles, Virginia, offices.

13. According to AOL investigators, as a perquisite of employment at AOL, every employee is issued an AOL account free of charge. The AOL account issued to JASON SMATHERS, the defendant, in connection with his employment at AOL, was "JasonS2e." Among other things, this enabled SMATHERS to send and receive e-mail communications by using the e-mail address "JasonS2e@aol.com."[1]

14. SEAN DUNAWAY, the defendant, resides in Las Vegas, Nevada. According to the Source, DUNAWAY is in the internet gambling business, and has been engaged in the practice of bulk e-mail messaging – SPAM – primarily for purposes of marketing that gambling business over the Internet for some time, including the relevant time periods described below.

Definitions

15. "E-mail" is a mechanism by which individuals can transmit messages and images over electronic communications networks. Sent messages are stored in electronic mailboxes. An e-mail address is a name that identifies an electronic mailbox on a network where e-mail can be sent.

16. "AOL Instant Message" ("AIM") is a proprietary computer messaging service provided by AOL. According to AOL investigators, AOL has two separate but inter-related Instant Message products, AIM and Instant Message in the AOL service. Both computer messaging services enable individuals to engage in "real time," one-to-one text messaging between two computers or other electronic devices, such as cell phones. Through the two interrelated services, AOL subscribers and those who obtain the free AIM service can communicate, both from within and from outside of the AOL service. While instant message communications are not routinely stored or retained in the computers on which they occur, it is nevertheless possible to capture the contents of an instant message through logging functions built into the software, in order to preserve the correspondence as a text file on the computer. In the absence of the operation of those logging functions, instant messages are typically lost when the communication is terminated.

---

[1] For e-mail communications between AOL accounts, the "@aol.com" suffix is not required.

17. "Query" refers to a formal computer-coded question that is formulated to be "asked" to a computer or a computer database (akin to a "search"), to produce a resulting subset of data from that computer or database.

18. As described below, there is probable cause to believe that, as part of the conspiracy charged herein, the conspirators sent and intended to send certain e-mail by use of "open proxy" computer systems. An open proxy is a computer that has been configured to retransmit (re-route) computerized information (including e-mails) sent from an originating computer on to a destination computer system. Open proxies operate in much the same way as third-party re-mailing services do for postal mail, with the key exception that the owner or operator of the computer system used as the proxy often does not realize that his computer is being used for this purpose. (Indeed, computer viruses and other forms of malicious computer code have been released specifically for purposes of causing computer systems to serve as open proxies.) Typically, an open proxy receives computer data sent over the Internet, and then alters certain information that would otherwise identify for the ultimate recipient the identity of the sender. Open proxy computers are used by SPAMmers in part because they hide the true source or origin of the bulk e-mail, making it appear as if it was sent from the Internet address of the proxy computer, and in part to defeat certain Internet e-mail filters that might otherwise be set to "block" (i.e, refuse to receive) e-mail identified as being generated by a particular source. In this way, the sender of the SPAM can distribute it with greater degree of certainty that the e-mail will circumvent filters, and without concern that individual recipients will be able to trace the e-mail to its true source.

Discovery of the Theft and Sale of AOL's Customer List

19. I have spoken with the Source,[2] who is not an employee of AOL. The Source told me, among other things, the following:

a. The Source twice purchased from SEAN DUNAWAY, the defendant, large computerized lists of AOL customer information. Specifically, with respect to the first such purchase, which occurred in or about May or June 2003, the Source stated that DUNAWAY told the Source that he (DUNAWAY) had obtained a list of 92 million AOL screen names from an AOL employee, and that DUNAWAY described that AOL employee as an "engineer" who had very powerful access to AOL's internal information. DUNAWAY also told the Source that the database was extracted directly from AOL's computer servers. DUNAWAY sold the Source (and the Sources' then-business associate) the original 92 million AOL screen name list (hereinafter, the "Full List") in 26 separate blocks (each block corresponding with a particular letter of the alphabet, containing all screen names beginning with that letter), and that

[2] The Source has provided information and assistance to the Government in the hope of receiving leniency concerning his/her participation in the conspiracy described herein. The information provided by the Source has been reliable, and has been corroborated by independent information, as described more fully herein.

DUNAWAY charged the Source $2,000 per letter, for a total of $52,000, for the complete package. The Source purchased the second list from DUNAWAY, in or about February or March 2004, for approximately $32,500.

b. With respect to the second purchase, in early 2004, the Source sought to purchase from SEAN DUNAWAY, the defendant, an updated list, comparable to the Full List. Ultimately, the Source purchased a second list from DUNAWAY for approximately $32,500. (I have reviewed a record of a wire transmission of funds sent by the Source to DUNAWAY's bank account on or about March 1, 2004, confirming that the payment did occur.) Upon receiving the second list, the Source observed that it was smaller than the Full List, in that it contained approximately 18 million AOL screen names, not 92 million. DUNAWAY told the Source that this second list (the "Short List") was more up to date, and had been a more risky proposition for his AOL insider contact to obtain, because this list had more information concerning the subscriber for each AOL screen name, and DUNAWAY stated that he had paid $100,000 for the Short List. The Source observed that the Short List, while containing fewer screen names than the Full List, did contain additional information concerning those screen names, including more specific subscriber name and address information than in the Full List, but the Source also observed that certain of that additional information appeared to have come from publicly available internet databases, such as internet "white pages," and that the Short List thus appeared to have been the result of a merging of data, some from AOL and some from public information. The Source explained to DUNAWAY that he/she would be more interested in purchasing from DUNAWAY another complete list, akin to the Full List, because he/she (the Source) wanted to use it to send SPAM to as many screen names as possible, and so the more screen names in the list, the better. DUNAWAY explained that the 18 million screen name list was the best list he (DUNAWAY) had available to sell at that time. DUNAWAY told the Source that he could obtain for the Source a longer list, but that he was unable to do so at that time, because DUNAWAY stated that it would take some time, and DUNAWAY's AOL insider contact was traveling overseas on vacation, which DUNAWAY asserted happened frequently, whenever DUNAWAY purchased new material from that AOL insider.

c. During the Source's communications between the Source and DUNAWAY, the Source informed DUNAWAY of the nature of the Source's SPAMming business, which is primarily the sending out of masses of unsolicited e-mail marketing herbal penile enlargement pills. The Source also informed DUNAWAY that he/she (the Source) employed the use of open proxies to perpetrate these mass e-mailings. Also during their communications in 2004, DUNAWAY asked the Source to assist DUNAWAY in marketing his own (DUNAWAY's) internet gambling business, by having the Source send out for DUNAWAY mass e-mails with advertisements for DUNAWAY's business. DUNAWAY told the Source, at one point during their communications, that DUNAWAY's business of SPAMming for his internet gambling operation was earning him approximately $10,000 to $20,000 per day.

d The Source said that he/she had communicated with DUNAWAY through DUNAWAY's email address "seand@dunklabs.com," in connection with obtaining these lists. During

e. The Source used both lists he/she purchased from DUNAWAY on multiple occasions, including in or about early 2004, to send SPAM, through open proxies, to the AOL e-mail addresses in those lists.

20. AOL investigators informed me that in or about late April 2004, the Source provided to AOL three (3) CD-ROMs containing databases of information, organized into "fields" of types of information, relating to approximately 18 million AOL subscribers, as further proof of the assertions described above. I have reviewed these CD-ROMs, and observed that among the fields of information contained in these databases are screen names, account numbers, zip codes, credit card types (but no actual credit card numbers), telephone numbers, and a series of information fields relating to internal AOL processes. As explained to me by the Source, the CD-ROMs contain a copy of the Short List, which according to the Source, resembles, but is not identical to, the Full List.

21. The AOL investigators explained to me that AOL maintains its customer information in a number of different business databases. One of AOL's principal proprietary data repositories, which is located in Virginia and which is referred to within AOL as the "Data Warehouse," is used for the storage and analysis of customer-related data. The Data Warehouse contains a number of "data tables," each of which consists of a particular set of data fields, usually including a customer name or account number, among other information. AOL computer specialists have analyzed the databases contained on the CD-ROMs provided by the Source, and confirmed that, with the exception of certain external information that was likely obtained from publicly available "white pages," the database on the CD-ROMs was formatted in a manner identical to the way the data is maintained in the Data Warehouse.

22. According to AOL investigators, between March 11 and 21, 2004, SMATHERS was on vacation from work. I have reviewed records of the United States Customs Service that reflect that SMATHERS traveled from Dulles Airport in Virginia to Scandinavia on March 12, 2004, and returned to the United States on March 21, 2004.

Evidence of SMATHERS' Plan to Steal AOL's Customer List,
And to Distribute it to DUNAWAY for Use for SPAM

23. AOL computer specialists advised me that, in or about late May 2004, they obtained and analyzed the AOL laptop computer issued to and used by JASON SMATHERS, the defendant, at work (the "Smathers Laptop"). Among other things, the computer specialists discovered the following:

a. In the Smathers Laptop, one of the files in which those computer specialists looked was a designated file where sent and received AOL e-mail can be permanently

stored (beyond the typical 28-day e-mail retention period). There, the specialists found an e-mail dated April 14, 2003, sent from "JasonS2e" to "JasonS2e" with the subject line "spam/the brews."[3] The e-mail contained the text of a lengthy set of AOL Instant Message correspondence between the screen name "JasonS2e" and an individual identified only by the AOL Instant Message screen name "The Brews." I have reviewed a printout of the file, and the text reflects a discussion concerning ways in which unsolicited multiple e-mails to AOL subscribers could profitably be sent – i.e., SPAM. In that discussion, the person identified in the communications as "JasonS2e" (i.e., JASON SMATHERS, the defendant) initially states that SPAMming AOL members is illegal. SMATHERS and "The Brews" then go on to discuss various techniques by which to SPAM AOL, as well as the large profits to be made from such activity. At one point, "The Brews" wrote

> Well . . . it would be different if you mailed current AOL members But the lists I use, and others have used, are just collected lists where people have to enter their emails and all there is thousands and thousands of fake emails If you have a database of REAL emails, that were fresh, the ratio of sign ups would be sooo much greater If you have any ideas on bulk mailing with AOL lol let me know and I can get you a program set up in a heart beat heh"

To this suggestion, SMATHERS replied:

> well I'll check it out . . . It isn't going to be easy I think I found the member database . . . Just need to figure out how to get the SNs [screen names] it is spread over like 30 computers . . . You can't talk about this.

SMATHERS also asserted, during the exchange:

> OK, I got it figured out . . . there are going to be millions of them so, will take time to extract I will do them a chunk at a time . . . because 37 million accounts have up to 7 screen names per account I'd expect there to be around 100 million active screen names[4] maybe more.

For the remainder of this set of correspondence, SMATHERS and "The Brews" discussed detailed plans for the theft and use of the AOL subscriber database.

---

[3] Based on my training and experience, I know that, to avoid losing data or files kept in e-mail "boxes" that are subject to periodic automatic deletion, e-mail users frequently send themselves their own e-mail as a way of preserving those files or data for later retrieval.

[4] As described below, this estimate is fairly close to the correct number of subscribers as represented to me by AOL officials – 92 million.

b. Another file contained an e-mail sent from JasonS2e to JasonS2e (i.e., sent by JASON SMATHERS, the defendant to himself, apparently for purposes of maintaining access to the information later), with the subject line "member_sub," dated April 25, 2003. That e-mail contained the user name and password for the AOL employee user account "AMS_READ." (As described more fully below, this AOL account was used to perpetrate the theft of the Full List).

c. Another file in the Smathers Laptop was an email sent by JasonS2e to JasonS2e (i.e., sent by JASON SMATHERS, the defendant, to himself), with the subject line "query," dated May 19, 2003, at 5:46:21 p.m. Eastern Standard Time. That e-mail contained the exact query that was used to obtain the AOL subscriber database corresponding to the letter "a" from the Data Warehouse. According to the AOL computer specialists, this query, if run against the AOL Data Warehouse, would have produced a list of all AOL subscriber screen names beginning with the letter "a" (the "Letter A Query").

d. The Smathers Laptop also contained an additional set of correspondence, between JASON SMATHERS, the defendant, and SEAN DUNAWAY, the defendant, using e-mail software known as "Hushmail." From my experience and training, I know that "Hushmail" is a program that encrypts the contents of e-mails, and it is commonly used by people who wish to conceal the nature of their communications. Such communications can be deciphered only by those who have access to the computerized decoder "key." Nevertheless, the e-mail address and subject line of the e-mails are, by necessity, rendered in plain text, and with respect to one such e-mail, the e-mail address used by the recipient was "seand@dunklab.com" -- DUNAWAY's e-mail address. Specifically, on or about June 1, 2003, Smathers sent Dunaway an encrypted e-mail with the subject line: "My NEW PGP Public Key." I also know, based on my training and experience, that "PGP" refers to a Public Key/Private Key encryption program that allows individuals to exchange information in a high level of encryption, so that it can not be rendered into human readable text.

The Time, Place and Method of the Theft

24. The AOL computer specialists advised me of the following:

a. AOL computer specialists attempted to identify the source of the illicitly obtained copy of its Data Warehouse data by examining the CD-ROM databases provided by the Source. Among other things, they attempted to pinpoint the approximate date upon which the theft took place. The CD-ROM databases include a data "field" reflecting the date upon which each account was created, and the analysis revealed that the latest date of creation for any of the screen names on the CD-ROM was May 19, 2003, thus indicating that the copying of data from the Data Warehouse most likely took place on or about May 19, 2003.

b. AOL computer specialists then sought to determine who accessed the Data Warehouse in or about May 2003. AOL's internal computer system is configured so that computer activity logs record on a regular basis all computer "queries" (attempts to obtain

information from a database) run against the Data Warehouse. Those logging functions were in operation in May 2003, and the logs provide a "snapshot" of the processes being run in the computer system at any given time. These records (which I have reviewed) reveal that several queries were run against the Data Warehouse on or about May 19 and 20, 2003. Analysis of the query snapshot determined that when those queries were run on the Data Warehouse database, they would return the exact type of data which was found on the CD-ROMs -- AOL internal account number, screen-name, billing name, address, phone number, and type of credit card (but not credit card number). Accordingly, the AOL computer specialists concluded that those queries most likely produced the databases contained on the Source's CD-ROMs. Specifically, the records show that a series of queries were run against the Data Warehouse of AOL on or about May 19 and 20, 2003, and those queries (hereinafter referred to as the "Intrusion Queries") produced in response an alphabetical list of all AOL subscribers, sorted by the initial letter of the screen name for each account. That list would have contained a complete list of all AOL screen names, including account-holders' zip codes, credit card types (but no actual credit card numbers)[5] and telephone numbers, as well as a series of information fields pertaining to AOL's own internal processes.

c. Specifically, the activity logs show that the Letter A Query (which, as described above in paragraph 23(c), was the query saved by JASON SMATHERS, the defendant, in the Smathers Laptop, in an e-mail dated May 19, 2003, at 5:46:21 p.m. Eastern Standard Time), was run against the Data Warehouse on May 19, 2003, at 5:36 p.m. Eastern Standard Time. The activity logs further show that the Intrusion Queries, which were a series of queries run against the AOL Data Warehouse on May 19, and 20, 2003, were exactly the same as the Letter A Query, with the exception that each separate query substituted one letter of the alphabet -- "b," "c," etc. -- for the letter "a." The Intrusion Queries were, thus, apparently designed to draw from the Data Warehouse the entirety of AOL's subscriber list, one letter of the alphabet at a time, in an apparent attempt to make the search results for each individual query to be of a manageable size.

---

[5] According to the AOL investigators, when new suscribers open accounts at AOL, they are required to provide a method of payment, such as credit card type and card number, which AOL will bill each month for the costs of AOL's services. While the information concerning the type of credit card used by each subscriber is kept in the Data Warehouse, linked to other basic accountholder information, the credit card account number -- i.e., the number required for billing purposes -- is kept in a separate highly secured data location, apart from the Data Warehouse. While, as noted, the number of AOL employees permitted access to the Data Warehouse is strictly limited by AOL, the number of people with access to credit card account number information is even more restricted. JASON SMATHERS, the defendant, was not authorized to access that information either, but there is no evidence he has gained access to that information, and the AOL investigators informed me that the databases obtained by the Source did not include subscribers' credit card numbers.

d. The activity logs further reflect that each of the Intrusion Queries was generated by an AOL employee computer account identified as "AMS_READ." According to the AOL investigators, only a small number of AOL employees are given computer access "rights" that include the ability to run queries against the Data Warehouse of the nature of the Intrusion Queries. The AOL investigators further informed me that JASON SMATHERS, the defendant, is not the AOL employee assigned the account "AMS_READ," but that the employee who is assigned that account does have such access rights.

e. The activity logs also show that, prior to the Intrusion Queries, the "AMS_READ" account was used, unsuccessfully, to run a series of queries against the Data Warehouse in attempts to obtain the AOL subscriber database as early as late April 2003. Several of those queries failed because the data attempted to be captured thereby was simply too much information to be processed in the way those queries were posed. However, one such query (the "Test Query"), run on or about May 4, 2003 (in an apparent attempt to obtain the information in smaller, more readily processed pieces), requested the subscriber information for a single AOL account -- the account issued to JASON SMATHERS, the defendant in connection with his employment -- i.e., "JasonS2e."

f. At the time the Intrusion Queries and the Test Query were run, JASON SMATHERS, the defendant, did not have those access rights to run queries of this nature against the Data Warehouse -- i.e., SMATHERS was not authorized by AOL to access the Data Warehouse in this way during the time period when the Intrusion Queries and the Test Query were run.

g. In connection with his employment at AOL, AOL issued SMATHERS a remote secure connection, known as a virtual private network ("VPN") to permit him to gain access to AOL's internal networks from outside the office, such as from home, or from hotels or other locations when he was traveling and away from the office. The VPN enables employees to perform necessary computer operations remotely (i.e., when physically outside the office). The remote access to AOL internal networks would allow an individual to perform tasks as if he were physically present in the AOL office facility, including the ability to run queries against the Data Warehouse. AOL computer specialists then reviewed certain computer generated logs reflecting remote access to the AOL internal network through the VPN, to determine who was using the AMS_READ account to run the Intrusion Queries and the Test Query.[6] These logs (which I, too, have reviewed) show that JASON SMATHERS, the defendant, remotely accessed the internal AOL network through the VPN numerous times during May 2003, including on May 19, 2003 and May 20, 2003, at or about the times at which the

---

[6] AOL security attendance records reflect that the AOL employee assigned the AMS_READ account (who works for AOL in an office building in Tucson, AZ), show that that employee was not present in any AOL premises at the time the Intrusion Queries or the Test Query were run. In addition, the logs of the VPN activity do not show that employee accessing AOL's computer system by remote access at that time either.

Intrusion Queries and the Test Query were being run. Those logs also reflect that the computer connection from which SMATHERS was logging into AOL's system through the VPN during May 19, 2003 and May 20, 2003, was located at SMATHERS' residence in West Virginia.

WHEREFORE, deponent prays that an arrest warrant be issued for JASON SMATHERS and SEAN DUNAWAY, the defendants, and that they be imprisoned or bailed as the case may be.

PETER CAVICCHIA
SPECIAL AGENT
UNITED STATES SECRET SERVICE

Sworn to before me this
__th day of June, 2004

UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK