

1 messages. I have personally reviewed a number of these complaints, including the
2 following:

3 30. I have reviewed the complaint of EO, residing in Floresville, TX. On
4 July 6, 2004, EO received an unsolicited e-mail from NIM advertising a broadcast e-
5 mail software package for \$149.00. The advertisement represented that use of the
6 software to send out e-mail advertisements would result in a minimum 400% increase
7 in sales, and that the user would receive a minimum of 750,000 website hits within 90
8 days or receive a full 100% refund. The advertisement further represented that the
9 broadcast e-mail software would automatically create 10 super-fast mail servers on the
10 user's computer that would provide the ability to send out unlimited, personalized and
11 targeted broadcast e-mail advertisements to over 500,000,000 people on the internet at
12 the rate of up to 1,000,000 daily, automatically and for free. The advertisement further
13 represented that the software would provide millions of the newest and freshest general
14 interest and regionally targeted e-mail addresses; that a purchaser would be guided
15 through the entire process of installing and utilizing the entire broadcast e-mail
16 package; and that a purchaser would receive unlimited lifetime customer and technical
17 support.

18 31. EO has provided copies of credit card statements showing he purchased
19 the broadcast e-mail software from NIM on July 6, 2004. EO has provided a copy of a
20 FedEx label that shows the broadcast e-mail package was shipped to him in Floresville,
21 Texas on July 6, 2004. EO has provided copies of e-mails to NIM requesting
22 information and assistance on the use of the software and complaining that the software
23 did not work. EO has provided a copy of an additional FedEx label and tracking
24 records that show a second broadcast e-mail package was shipped to him in Floresville,
25 Texas on July 16, 2004, that originated from Seattle, Washington even though the
26 shipping label shows NIM to be located at PO Box 1736, Phoenix, OR 97535. EO has

1 provided copies of additional e-mails to NIM requesting information and assistance on
2 the use of the software and requesting a refund because the software did not produce
3 the results represented in NIM's advertisement. EO has provided information that his
4 credit card was charged three times by NIM for \$149.00 on July 6, July 8, and July 11,
5 2004; that he has not received a refund of any monies; and that NIM has threatened to
6 send him to a collection agency if he tries to reverse the charges by NIM on his credit
7 card account.

8 32. I have reviewed the complaint of A.H. residing in Cedarburg, WI. A.H.
9 reported that she ordered the broadcast e-mail software from NIM on August 29, 2005,
10 and received the shipped package on August 31, 2005. A.H. reports that she was
11 immediately dissatisfied with the software due to the difficult process that NIM
12 required to register and activate the product. From that point forward A.H. was
13 concerned about the quality of the product and wanted to return it, but NIM required
14 they evaluate the product for 90 days before returning it.

15 33. A.H. sent an e-mail requesting instructions to return the software and
16 referencing a charge back to their credit card for the purchase price. A.H. received the
17 following response from NIM via e-mail explaining their guarantee, "If You Do Not
18 Receive At Least a 400% Increase in Sales After Using Our Broadcast Email Package
19 for 90 Days, Simply Return it to us for a Full 100% Refund, No Questions Asked.
20 Any Dispute of this Charge with Your CC Will Automatically be Forwarded to Our
21 Collection Agency With Their Additional \$250 Service Charge for a Total of \$399 to
22 be Owed." A.H. received another e-mail stating "If you dispute the charge your debt
23 will be forwarded to our collection agency with an additional \$250 service charge by
24 them, which if not paid will be forwarded to the 3 US Credit Agencies, in turn
25 negatively affecting your credit rating for the next 7 years not paying said debt owed,
26

1 and will appear on your credit report indicating you refused to pay a \$399 debt that you
2 own. We do not stand for theft at our corporation.”

3 34. A.H. reported that after waiting the required 90 days she sent daily e-
4 mails to NIM over a two week period trying to obtain an address for use in returning
5 the broadcast e-mail software. It was only after posing as a new customer, and using a
6 new e-mail address that A.H. was able to obtain the address of PO Box 1259, Seattle,
7 Washington 98111 as an address for NIM Corporation. The BBB records associated
8 with A.H.’s complaint indicate that NIM advised BBB that it was refusing to refund the
9 purchase price because, “[t]his customer is not entitled to a refund for opened software.
10 We have over 10,000 customers currently using our software and it works
11 PERFECTLY. This is customer to email customer service at nim@cyberservices.com and
12 we will assist them with any questions or concerns they may have.”

13 35. A.H. stated that NIM told her that they refused to pay the refund because
14 A.H. did not return the broadcast e-mail software. A.H., however, reported that she
15 did return the product and that she had a PS Form 3811, Domestic Return Receipt,
16 signed by what appears to be Robin or Robert Soloway, indicating receipt.

17 36. As part of my investigation in this case, I learned that the Washington
18 State Attorney General’s Office has also received dozens of complaints about spamming
19 and fraudulent activities related to Robert Soloway, Newport Internet Marketing
20 Corporation, and/or Newport IM Corporation during the period from 2004 through and
21 until the present. Like the complaints to the FTC and BBE, these included complaints
22 from individuals who had received spam e-mails from NIM; people who had purchased
23 internet mailing software from NIM that failed to function as advertised but who were
24 nevertheless denied a full refund as promised; and people whose e-mail addresses or
25 domain names had been used without their permission and fraudulently inserted into
26 forged “From:” headers in spammed e-mail messages.

1 37. The complaints made to the Washington Attorney General's Office
2 included a complaint made by J.N., who is a Senior Computer Systems Specialist with
3 the Santa Barbara Department of Social Services, in Santa Maria, California. On April
4 9, 2007, I contacted J.N. by telephone, and he reported the following to me:

5 a) Employees of the Santa Barbara Department of Social Services (DSS)
6 began receiving unsolicited e-mail addressed to their individual work e-mail addresses
7 in around February of 2007. The e-mail was fraudulent because it listed the same e-
8 mail address in both the "To:" and "From:" fields in the header. The e-mail address
9 that was used included the name of an individual DSS employee, and the domain name
10 of DSS, ("kt@sdcsocialserv.org"). The employee had not sent this e-mail to himself.
11 J.N. reported that four other employees were receiving the same e-mails, also with
12 forged "From" headers that contained their own names in both the "From:" and "To:"
13 fields.

14 b) The message sent with the forged headers stated that: "we email
15 advertise your charity web site to 7,500,000 people. free", and contained a link to a
16 website at domain: "emailmarketingassociates.com". J.N. researched the website on
17 the Internet and discovered that the mass e-mail marketing business belonged to Robert
18 Soloway, and was purportedly located at 1001 4th Ave., #1259, Seattle, Washington,
19 98111. (As noted above, I have investigated that address, which has repeatedly been
20 identified on Soloway's websites as the address for his company, and have determined
21 that it is not a valid address.)

22 c) J.N. further reported that the spamming of DDS employees had
23 continued for about eight weeks at the time I spoke with him, and that the cost to Santa
24 Barbara County DDS to deal with this spam that contained forged e-mail addresses of
25 DDS employees was about \$1,000.00 per week, based on the hours of IT employees
26 that had been spent trying to put a stop to it.

1 38. Other complaints filed with the Washington Attorney General's Office
2 from individuals who have had their own, or their company's e-mail address or domain
3 name effectively stolen, and used fraudulently in a forged "From" header in spam
4 include H.D., from Minnesota, J.A. from California, and M.H. of California. These
5 complainants note that because their own e-mail addresses are being forged and inserted
6 fraudulently into the "From" headers of spam, they are unable to stop the spam by any
7 filter. M.H. reported that his company is losing revenue due to complaints that it is
8 sending spam, because Broadcast Email Services is sending spam with his company's e-
9 mail addresses and domain name in forged "From" headers.

10 **B. Technical and Other Evidence Corroborating Victim Claims**

11 39. In January, 2007, an Internet Service Provider (ISP) provided three
12 servers to the FBI. The ISP turned the servers over to the FBI because the customer
13 who had leased them had violated the ISP's terms of service agreement by using them
14 to transmit spam. An Agent from the Seattle FBI Cyber Squad, as well as an Agent
15 from the FBI's Computer Analysis Response Team (CART) forensically examined the
16 three servers. Based on that examination, they made the following findings:

17 a) A software program called Dark Mailer had been installed on all three
18 servers. Dark Mailer, (as defined by the online encyclopedia wikipedia), is a software
19 program that has been under attack from anti-spam groups since its inception. The
20 software taps into a network of zombie proxy computers and is able to send 50,000
21 pieces of e-mail per hour, from a regular cable modem connection. It affords near-total
22 anonymity because of the zombie proxy network feature. Dark Mail proponents claim
23 it can be used for legitimate "bulk-emailing" to opt-in subscribers, but the fact that it
24 relies on zombie proxy computers to transmit the "bulk e-mails" is inconsistent with
25 claims of legitimacy. It is widely believed within the Internet security industry that
26 Dark Mailer is often used by spammers, who are able to conceal their connection to

1 spamming activity because of the anonymity provided by Dark Mailer's zombie proxy
2 network system. Dark Mailer does not currently does not have an official website for
3 downloading; copies, however, can still be found.

4 b) The Dark Mailer program installed on the three servers was
5 configured to copy e-mail addresses from text files to a template, send the e-mail out
6 using the template, and record the e-mail address of the sent e-mail in a file called
7 C:\SENT\SENT.TXT. A review of the SENT.TXT files on two of the servers
8 revealed that e-mail had been sent from server1 to 57 million e-mail addresses, and sent
9 from server2 to 37 million e-mail addresses, in a three month period. The Dark Mailer
10 software was also configured on all three servers to use a list of 2,023 proxy computers
11 to resend the e-mail. This configuration, as noted above, would effectively disguise the
12 the originating source of the e-mail.

13 c) The body of the e-mail template configured on the Dark Mailer
14 software included the following text:

15 "email advertise like this to 8,000,000 people... free.."

16 "http://www.advertisingemailcorporation.com"

17 "advertise now for christmas... 15 days left ..."

18 d) A copy of the website that had been viewed by one of the spam
19 complainants at "http://www.advertisingemailcorporation.com" was available, and was
20 compared to the content of websites that had been copied from
21 "www.emailadvertisinginc.com", "www.newportcorp.cn", and
22 "www.colidsilver.com". All of these websites had identical content, and all listed PO
23 Box 1259, Seattle, WA (the PO Box registered by Soloway), as an address for receipt
24 of orders and payments for the "broadcast e-mail" services and software that were
25 offered for sale on each website.

1 40. The ISP that turned over the servers to the FBI identified the person who
2 had leased them as "Rob Solowa," 1200 Western Avenue, Seattle, WA, 98101,
3 telephone number 206-226-9558. The servers were leased by "Solowa" beginning in
4 September, 2006 until the ISP took them offline on approximately December 15, 2006.

5 41. In April of 2007 I learned that spam potentially connected to Soloway was
6 being transmitted from IP addresses 209.160.33.45, 209.160.41.77, and
7 209.160.41.78. Through WHOIS lookups, I learned that these IP addresses belonged
8 to an ISP named Hopone Internet Corporation. On April 19, 2007, I contacted
9 Hopone, and was referred to the abuse department. The head of the department
10 reported that the servers with those IP addresses had been taken offline due to a
11 violation of Hopone's terms of use policy. He stated that Hopone had learned about
12 this when it was contacted by another ISP, which had informed Hopone that the three
13 IP addresses were sending out spam. He further advised that the three servers
14 containing the hard drives using the above IP addresses had not been touched after they
15 were powered off. Because the contract had been violated by the customer, the abuse
16 manager for Hopone Internet Corporation agreed to provide the hard drives to the FBI.
17 After a "Consent to Search" document was signed by management officials at Hopone
18 Internet Corporation, I took possession of the hard drives on April 20, 2007.

19 42. An Agent from the Seattle FBI Cyber squad, as well as an Agent from the
20 FBI's CART team analyzed these three servers. Based on that examination, they made
21 the following findings:

22 a) The Dark Mailer program was installed on all three servers. Dark
23 Mailer was configured to copy sent e-mail messages in text files beginning with the
24 letters "em", in a directory called "sent." A review of the "em" text files on the hard
25 drives revealed that 120,000,000 e-mails had been sent to 79,610,868 unique e-mail
26 addresses.

1 b) The hard drives all contained text files beginning with "list", followed
2 by a number. For example, on one server the first "list" file started with "list0001.txt"
3 and ended with "list0136.txt." Together these files contained 135,579,118 unique e-
4 mail addresses. The majority of the e-mail addresses used the names "accounting",
5 "admin", "billing", "contact", "feedback", "help", "info", "mail", "sales",
6 "service", "support", and "webmaster", with different domain names.

7 c) A file named "doms" was present that contained 3,177,034 unique
8 domain names.

9 d) Dark Mailer was configured to use proxy IP addresses to resend the e-
10 mail to the ultimate recipient. A review of the proxy text files revealed that 3,148 unique
11 IP addresses were included in this proxy network.

12 43. According to Hopone records, the person paying for the three servers
13 with the IP addresses of 209.160.33.45, 209.160.41.77, and 209.160.41.78. was
14 identified as "Robert Solowa," 1200 Western Avenue - 17E, Seattle, Washington,
15 98101, telephone number 206-226-9558, e-mail address:
16 powerseller2003@mailshack.com. "Robert Solowa" had begun paying for these
17 servers on December 29, 2006, and continued to do so until they were taken offline in
18 mid-April of 2007. Hopone records also indicated that these servers had been managed
19 on April 3, 2007 and April 4, 2007 by someone who was originating their
20 communication from an IP address of 24.143.67.229.

21 44. I did a WHOIS look up on IP address 24.143.67.229, and learned that it
22 belonged to an ISP named Millennium Digital Media Systems. Millennium Digital
23 subsequently provided records that identified the subscriber to whom IP address
24 24.143.67.229 was assigned from March 8, 2007 to April 6, 2007 as Robert Soloway,
25 1200 Western Avenue, Apt. 17E, Seattle, Washington, 98101-2964, telephone number
26 206-226-9558.

1 45. During the course of this investigation, I have received and reviewed
2 information and records that show a connection to, and indicate that Robert Soloway
3 has used as many as 50 different domain names, over a two year period, as the hosting
4 address for the website to advertise his spamming services and software. Many of
5 these were used prior to the start of my investigation, and I have not been able to obtain
6 records with respect to the registrations for them. Three of the domain names that
7 were utilized in 2004 were reportedly registered to "Robert Alan" or "Bob Alan."
8 Since approximately March of 2006, the domains connected to the scheme have
9 typically been registered through an ISP in China.

10 46. One of the domain names that has been used in Soloway's scheme -
11 colidsilver.com, was registered and paid for with the stolen identity of C.W., from
12 Texas. I interviewed C.W. in December, 2006, and he reported to me as follows:

13 a) In mid-September of 2006, C.W. noted four odd charges on his credit
14 card statement. One of these was for the registration of the www.colidsilver.com
15 domain. C.W. had never registered a domain, or given any one else permission to do
16 so. C.W. contacted his bank, which reversed the charge.

17 b) C.W. also accessed the website www.colidsilver.com to see what it
18 was. C.W. observed that it was a website for "Broadcast Email Corporation." C.W.
19 looked through the website and noted that the "owner" was listed as "Bob Soloway."
20 C.W. does not know Bob Soloway and did not authorize him to use his credit card
21 information to register the domain www.colidsilver.com.

22 **C. Money Laundering Activity**

23 47. As part of this investigation, SA Sylvia Reyes, IRS-CI, has obtained and
24 reviewed numerous banking, credit card, and on-line financial account records for
25 Soloway and NIM. SA Reyes has shared her findings with me.
26

1 48. SA Reyes has determined from the records she has reviewed that Soloway
2 is the sole shareholder of NIM, and he alone holds ownership, financial interests, and
3 control of the corporate assets. She also found that Soloway routinely commingles
4 personal and corporate assets and liabilities.

5 49. SA Reyes has identified multiple banking, credit card, and on-line
6 financial accounts that have been used by Soloway and NIM as accounts for deposits of
7 proceeds from the mail and wire fraud and spam scheme activities. Specific accounts
8 used for this purpose by Soloway and NIM are further specifically identified in the
9 Affidavit of SA Silvia Reyes in Support of Seizure Warrants that is attached hereto and
10 fully incorporated by reference herein.

11 50. SA Reyes has also identified numerous payments made by Soloway and
12 NIM from accounts containing proceeds of the scheme, that have been made to
13 continue and promote the carrying on of the scheme. These include payments, for
14 example, to rent servers, to pay for hosting servers, to pay for ISP services, to pay for
15 money transmitting services, to pay for package delivery services, and to pay the rent
16 on Soloway's apartment, which is also his place of business.

17 51. Consistent with, and based on the findings of SA Reyes as more fully set
18 forth in her Affidavit in Support of Seizure Warrants, attached hereto and fully
19 incorporated by reference herein, there is probable cause to believe that any and all
20 business records of NIM corporation and any and all financial records of either
21 Soloway or NIM are, or contain, fruits, instrumentalities and evidence of violations of
22 Title 18 U.S.C. Sections 1037(a)(2) and(a)(3) (Fraud in Electronic Mail), Title 18
23 U.S.C. Section 1341 (Mail Fraud), Title 18 U.S.C. Section 1343 (Wire Fraud), Title
24 18 U.S.C. Section 1028(A) (Aggravated ID Theft), and Title 18 U.S.C. Section
25 1956(a)(1) (Money Laundering).

1 **D. Other Investigative Information**

2 52. As part of this investigation, I learned that Robert Soloway and Newport
3 Internet Marketing were named as defendants in a civil action filed by the Microsoft
4 Corporation, in King County Superior Court, in December, 2003. (Case No. 03-2-
5 12648-9 SEA). Plaintiff alleged violations of Washington State, and federal law based
6 on Soloway's spamming activities. During the course of that litigation, Soloway
7 responded to questions, under oath, in a proceeding on October 26, 2005. I have
8 reviewed portions of the transcript from that proceeding. Included within the
9 information Soloway provided under oath was the following:

10 a) Soloway "established residency for tax purposes" in Washington State
11 in January of 2004, although he had come to the state and "set things up" in his
12 apartment prior to that time.

13 b) Soloway started the Newport Internet Marketing company in 1996,
14 and he is the sole employee and the sole company officer. Soloway's employment with
15 NIM has been the "only employment [he's] had in [his] life."

16 c) Soloway works and runs his company from his one bedroom apartment
17 in Seattle, Washington, at 1200 Western Avenue, Apartment 17E, Seattle, Washington
18 98101.

19 d) Soloway has and uses a computer and related supporting equipment at
20 his apartment at 1200 Western Avenue to run his business.

21 e) Soloway rents a storage facility at a Public Storage facility on Northup
22 Way in Bellevue, Washington, and keeps his business records there.

23 53. As part of this investigation, I have obtained records from Public
24 Storage, which confirm that Robert Soloway leased Storage Unit A145, at the Public
25 Storage facility located at 12465 Northup Way, Bellevue, WA 98005 on April 18,
26 2005, and that he has continuously leased that storage unit ever since.

1 54. As part of this investigation, I have confirmed with the management of
2 the Harbor Steps Apartment Complex that Robert Soloway has rented Apartment 17E,
3 at the Harbor Steps Complex, located at 1200 Western Avenue, Seattle, Washington
4 98101, since November 28, 2003, and that he has continued to rent and occupy that
5 same apartment ever since.

6 **III. COMPUTER and ELECTRONIC EVIDENCE**

7 55. Based on the information in this affidavit, I believe that one or more
8 computer systems are located at 1200 Western Avenue, Apartment 17E, Seattle,
9 Washington, 98101, and that the computer system(s) located at the premises are
10 instrumentalities of crime and constitute the means by which violations of Title 18
11 U.S.C. Sections 1037(a)(2) and(a)(3) (Fraud in Electronic Mail), Title 18 U.S.C.
12 Section 1341 (Mail Fraud), Title 18 U.S.C. Section 1343 (Wire Fraud), Title 18
13 U.S.C. Section 1028(A) (Aggravated ID Theft), and Title 18 U.S.C. Section
14 1956(a)(1) (Money Laundering) have been committed. Therefore, I believe that there
15 is probable cause to seize the computer system(s) as instrumentalities of criminal
16 activity.

17 56. In addition, it has been my experience that it is common for those
18 engaging in computer fraud and e-mail fraud to use computers or other electronic media
19 to store information such as passwords, account numbers, identification documents or
20 means of identification, and correspondence with banks or other institutions regarding
21 accounts they may have accessed. It is my belief that any number of the items sought
22 in this affidavit may be found stored electronically. Based on my experience and my
23 consultation with Special Agent CART examiner Russell E. Fox, Seattle FBI, (who has
24 nine years of computer forensics experience and specialized training and experience in
25 searching for electronic evidence), I also know that electronic evidence can be moved
26 easily from one computer or electronic storage medium to another. As a result, I

1 believe that electronic evidence may be stored on any computer or electronic storage
2 medium present at the search sites.

3 57. In addition, based on my training and experience and that of Russell Fox,
4 I know that in most cases it is impossible to successfully conduct a complete, accurate,
5 and reliable search for electronic evidence stored on a computer or other electronic
6 storage media during the physical search of a search site. This is true for a number of
7 reasons, including but not limited to the following:

8 a. Technical Requirements: Searching computers and other electronic
9 storage media for criminal evidence is a highly technical process requiring specific
10 expertise and a properly controlled environment. The vast array of computer hardware
11 and software available requires even computer experts to specialize in particular
12 systems and applications, so it is difficult to know before a search which expert is
13 qualified to analyze the particular system(s) and electronic evidence found at a search
14 site. As a result, it is impossible to bring to the search site all of the necessary
15 personnel, technical manuals, and specialized equipment to conduct a thorough search
16 of every possible computer system. In addition, electronic evidence search protocols
17 are exacting scientific procedures designed to protect the integrity of the evidence and
18 to recover even hidden, erased, compressed, password-protected, or encrypted files.
19 Since computer evidence is extremely vulnerable to inadvertent or intentional
20 modification or destruction (both from external sources or from destructive code
21 embedded in the system such as a "booby trap"), a controlled environment is essential
22 to ensure its complete and accurate analysis.

23 b. Volume of Evidence. The volume of data stored on many
24 computers and other electronic storage media is typically so large that it is impossible
25 to search criminal evidence in a reasonable period of time during the execution of the
26 physical search of a search site. A single megabyte of storage space is the equivalent

1 of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000
2 megabytes, is the equivalent of 500,000 double-spaced pages of text. A fifteen
3 gigabyte storage device would, therefore, contain the equivalent of 7.5 million pages of
4 data, which, if printed out, would completely fill a 10' x 12' x 10' room to the ceiling.
5 Computer hard drive capacities of hundreds of gigabytes are now commonplace.
6 Consequently, the volume of data within a typical non-networked computer system is
7 equivalent to many millions, and possibly billions, of printed pages.

8 c. Hidden or Obfuscated Evidence. Computer users can conceal data
9 within computers and electronic storage media through a number of methods, including
10 the use of innocuous or misleading filenames and extensions. For example, files with
11 the extension “.jpg” often are image files; however, a user can easily change the
12 extension to “.txt” to conceal the image and make it appear as though the file contains
13 text. Similarly, computer users can encode communications to avoid using key words
14 that would be consistent with the criminal activity. Computer users also can attempt to
15 conceal electronic evidence by using encryption technologies. For example, some
16 encryption systems require that a password or device, such as a “dongle” or
17 “keycard,” be used to obtain a readable form of the data. In addition, computer users
18 can conceal electronic evidence within another seemingly unrelated and innocuous file
19 using a process known as “steganography.” For example, by using steganography, a
20 computer user can conceal text in an image file in such a way that it cannot be read
21 when the image file is opened using ordinary means. As a result, law enforcement
22 personnel may have to search all the stored data to determine which particular files
23 contain items that may be seized pursuant to the warrant. This sorting process can take
24 a substantial amount of time, depending on the volume of data stored and other factors.

25 d. Deleted or Downloaded Files. Computers and other electronic
26 storage media allow suspects to delete files to attempt to evade detection or to take

1 other steps designed to frustrate law enforcement searches for information. However,
2 searching authorities can recover computer files or remnants of such files months or
3 even years after they have been downloaded onto a hard drive, deleted, or viewed via
4 the Internet. When a person "deletes" a file on a home computer, the data contained in
5 the file do not actually disappear; rather, the data remain on the hard drive until they are
6 overwritten by new data. As a result, deleted files, or remnants of deleted files, may
7 reside in free or "slack" space (i.e., in space on the hard drive that is not allocated to an
8 active file or that is unused after a file has been allocated to a set block of storage space)
9 for long periods of time before they are overwritten. A computer's operating system may
10 also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that
11 have been viewed via the Internet are automatically downloaded into a temporary Internet
12 directory or "cache." The browser typically maintains a fixed amount of hard drive space
13 devoted to these files, and the files are only overwritten as they are replaced with more
14 recently viewed Internet pages. Thus, the ability to retrieve the residue of an electronic
15 file from a hard drive depends less on when the file was downloaded or viewed than on a
16 particular user's operating system, storage capacity, and computer habits.

17 58. In accordance with the information in this affidavit, law enforcement
18 personnel will execute the search of computers systems seized pursuant to this warrant
19 as follows:

20 a. Upon securing the search site, law enforcement personnel will
21 seize the computer systems and transport them to an appropriate law enforcement
22 laboratory for review. The computer systems will be reviewed by appropriately trained
23 personnel to extract and seize any data that falls within the list of items to be seized
24 pursuant to the warrant.

25 b. In order to search fully for the items identified in the warrant, law
26 enforcement personnel may examine all of the data contained in the computer systems

1 to view their precise contents and determine whether the data fall within the list of
2 items to be seized pursuant to the warrant. Because of the above-described technical
3 requirements, volume of evidence, and the ability of suspects to delete, download, hide
4 and/or obfuscate evidence, the analysis of electronically stored data may entail any or
5 all of several different computer forensics techniques. Such techniques may include,
6 but are not limited to, surveying various file "directories" and the individual files they
7 contain (analogous to looking at the outside of a file cabinet for the pertinent files in
8 order to locate the evidence and instrumentalities authorized for seizure by the
9 warrant); "opening" or reading the first few "pages" of such files in order to determine
10 their precise contents; "scanning" storage areas to discover and possibly recover
11 recently deleted data; scanning storage areas for deliberately hidden files; and
12 performing electronic "keyword" searches through all electronic storage areas to
13 determine whether occurrences of language contained in such storage areas exist that
14 are related to the subject matter of the investigation.

15 59. In order to search for data that fall within the list of items to be seized
16 pursuant to the warrant, law enforcement personnel will seize and search the following
17 items (heretofore and hereinafter referred to as "computer systems"), subject to the
18 procedures set forth above:

19 a. Any computer equipment and storage device capable of being used
20 to commit, further, or store evidence of the offense listed above;

21 b. Any computer equipment used to facilitate the transmission,
22 creation, display, encoding or storage of data, including word processing equipment,
23 modems, docking stations, monitors, printers, plotters, encryption devices, and optical
24 scanners;

25 c. Any magnetic, electronic or optical storage device capable of
26 storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs,

1 DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory
2 calculators, electronic dialers, electronic notebooks, and personal digital assistants;

3 d. Any documentation, operating logs and reference manuals
4 regarding the operation of the computer equipment, storage devices or software;

5 e. Any applications, utility programs, compilers, interpreters, and
6 other software used to facilitate direct or indirect communication with the computer
7 hardware, storage devices, or data to be searched;

8 f. Any physical keys, encryption devices, dongles and similar
9 physical items that are necessary to gain access to the computer equipment, storage
10 devices or data; and

11 g. Any passwords, password files, test keys, encryption codes or
12 other information necessary to access the computer equipment, storage devices or data.

13
14 **IV. CONCLUSION**

15 60. Based on the facts and evidence presented in this affidavit, I believe there
16 is probable cause to believe that fruits, instrumentalities and evidence of violations of
17 Title 18 U.S.C. Sections 1037(a)(2) and(a)(3) (Fraud in Electronic Mail), Title 18

18 ///////////////

19 ///////////////

20 ///////////////

21 ///////////////

22 ///////////////

23 ///////////////

24 ///////////////


25 ///////////////

26 ///////////////

1 U.S.C. Section 1341 (Mail Fraud), Title 18 U.S.C. Section 1343 (Wire Fraud), Title
2 18 U.S.C. Section 1028(A) (Aggravated ID Theft), and Title 18 U.S.C. Section
3 1956(a)(1) (Money Laundering) as set forth in Attachment B, exist at:

4 1200 Western Avenue, Apartment 17E, Seattle, WA, 98101, and in computers
5 and/or other electronic storage devices located therein, and at

6 Storage Unit A145, Public Storage Inc., 12465 Northup Way, Bellevue, WA
7 98005, and in computers and/or other electronic storage devices located therein.

8
9
10 
11 KENNETH A. SCHMUTZ, Special Agent
12 Federal Bureau of Investigation

13 Subscribed to and Sworn to before me this 23 day of May, 2007.

14
15 
16 MARY ALICE THEILER
17 United States Magistrate Judge
18
19
20
21
22
23
24
25
26
27
28