

AFFIDAVIT

STATE OF WASHINGTON)
COUNTY OF KING) ss

KENNETH A. SCHMUTZ, being first duly sworn on oath, deposes and says:

I. INTRODUCTION and BACKGROUND

A. Warrants Requested

1. I make this affidavit in support of an application for a search warrant for:

a) the property located at and in a residential apartment located at:

1200 Western Avenue, Apartment 17E
Seattle, Washington 98101

As explained more fully below, this apartment is both the residence of Robert Alan Soloway, and the base of operations for "Newport Internet Marketing," a company that is solely owned by Robert Alan Soloway. As is also explained more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal laws exist, and are present at the premises, and/or in computers located on the premises at 1200 Western Avenue, Apartment 17E, Seattle, Washington 98101.

b) a storage unit, more specifically,

Storage Unit A145
Public Storage Inc.
12465 Northup Way
Bellevue, WA 98005

As explained more fully below, this storage unit is rented by Robert Alan Soloway, and according to Soloway's own sworn statements, is used for the storage of business records for Soloway's business. As is further explained below, there is thus

1 probable cause to believe that evidence, fruits, and instrumentalities of violations of
2 federal laws exist, and are present at this storage unit.

3 **B. Agent Background**

4 2. I am a Special Agent of the Federal Bureau of Investigation (FBI), and
5 have been so employed since January 2004. I am currently assigned to the Seattle
6 Office's Cyber Crime Squad, which investigates various computer-related crimes,
7 including computer intrusions and Internet-related frauds.

8 3. I have both a Bachelors of Science, and a Masters of Science degree in
9 Business Information Systems from Utah State University. Those degree programs
10 involved, among other things, human computer interface, programming in three
11 languages (C + +, COBOL, Pascal), and designing and creating Internet web pages.
12 Prior to my work as a Special Agent, I worked for thirteen years in a variety of
13 capacities in the computer technology field; holding positions, for example, in which I
14 designed, implemented, and supported computer systems for credit unions, performed
15 quality assurance testing for a leading network operating system company, and
16 managed a group of software engineers in a high-paced technology company. I have
17 also taught computer classes at the community college level, including courses on
18 Windows NT Server, Networking Essentials, and Introduction to Programming. I
19 recently obtained industry certification in CompTia's Net+ program.

20 4. As an FBI agent, I have received specialized training, and gained
21 experience in interviewing and interrogation techniques, arrest procedures, search
22 warrant applications, the execution of searches and seizures, federal computer crimes,
23 computer evidence identification, computer evidence seizure and processing, and
24 various other federal criminal laws and procedures. I have investigated dozens of cases
25 involving the use of computers and the Internet to commit federal crimes, and have
26

1 personally participated in the execution of multiple search warrants involving the search
2 and seizure of computers and related equipment.

3 **C. Sources of Information**

4 5. The information contained in this affidavit has been compiled through my
5 own investigatory efforts, with knowledge obtained from a variety of sources and
6 methods, including the review of documents and electronic records. I have also drawn
7 from information provided by numerous companies in response to official requests,
8 from interviews I have conducted of victims and witnesses, and from information
9 obtained from other law enforcement officers. Because this affidavit is submitted for
10 the limited purpose of establishing probable cause in support of the application for a
11 search warrant, it does not set forth each and every fact that I or others have learned
12 during the course of this investigation.

13 **D. Relevant Statutes**

14 6. This affidavit is made in support of search warrants to obtain evidence,
15 instrumentalities, and fruits of violations of the federal statutes identified below, which
16 provide, in pertinent part, as follows:

17 **18 U.S.C. § 1028A (Aggravated Identity Theft)**

18 (a)(1) . . . Whoever, during and in relation to . . . [certain
19 specified] felony violation[s] . . . knowingly transfers, possesses, or uses,
20 without lawful authority, a means of identification of another person shall,
in addition to the punishment provided for such felony, be sentenced to a
term of imprisonment of 2 years.

21 "Means of identification" is defined at 18 U.S.C. § 1028(d)(7), for purposes of
22 § 1028 and 1028A, as follows:

23 (7) the term "means of identification" means any
24 name or number that may be used, alone or in conjunction
25 with any other information, to identify a specific individual,
including any -
26

1 Unique electronic identification number, address, or routing
code; . . .

2 **18 U.S.C. § 1037 (Fraud and Related Activity in Connection with Electronic**
3 **Mail)**

4 (a) . . . Whoever, in or affecting interstate commerce, knowingly -

5 (2) uses a protected computer to relay or retransmit multiple
6 commercial electronic mail messages, with the intent to deceive or
7 mislead recipients, or any Internet access service, as to the origin of such
messages, [or]

8 (3) materially falsifies header information in multiple commercial
electronic mail messages and intentionally initiates the transmission of
such messages,

9 (b) (1) . . . [shall be punished with a fine, and imprisonment] for not
10 more than 5 years, or both, - if

11 (A) the offense is committed in furtherance of any felony under the laws
of the United States; . . .

12 **18 U.S.C. § 1341 (Mail Fraud)**

13 Whoever, having devised or intending to devise any scheme or
14 artifice to defraud, or for obtaining money or property by means of false
or fraudulent pretenses, representations, or promises . . . for the purpose
15 of executing such scheme or artifice or attempting so to do, places in any
post office or authorized depository for mail matter, any matter or thing
16 whatever to be sent or delivered by the Postal Service, or deposits or
causes to be deposited any matter or thing whatever to be sent or
17 delivered by any private or commercial interstate carrier, or takes or
receives therefrom, any such matter or thing, or knowingly causes to be
18 delivered by mail or such carrier according to the direction thereon . . .
shall be fined under this title or imprisoned not more than 20 years, or
both.

19 **18 U.S.C. § 1343 (Wire Fraud)**

20 Whoever, having devised or intending to devise any scheme or
21 artifice to defraud, or for obtaining money or property by means of false
or fraudulent pretenses, representations, or promises, transmits or causes
22 to be transmitted by means of wire, radio, or television communication in
interstate . . . commerce, any writings, signs, signals, pictures, or sounds
23 for the purpose of executing such scheme or artifice, shall be fined under
this title or imprisoned not more than 20 years, or both.
24

1 **18 U.S.C. § 1956(a)(1) (Money Laundering)**

2 Whoever, knowing that the property involved in a financial
3 transaction represents the proceeds of some form of unlawful activity,
4 conducts or attempts to conduct such a financial transaction which in fact
5 involves the proceeds of specified unlawful activity -

6 (A)(i) with the intent to promote the carrying on of specified
7 unlawful activity;

8 shall be sentenced to [a fine or imprisonment of up to 20 years, or
9 both].

10 **E. Location, and Items to Be Searched and Seized**

11 7. The application requests authority to search:

12 a) the residence of Soloway, located at 1200 Western Avenue, Apartment
13 17E, Seattle, WA 98101, as well as any computers or other electronic storage media
14 found therein. The premises are more specifically described as an apartment on the top
15 floor of the building located at 1200 Western Avenue, Seattle, Washington 98101. The
16 apartment is the first door on the left after exiting the elevator. The door is clearly
17 marked with "17E." The premises are additionally described in Attachment A,
18 attached hereto and incorporated by reference herein.

19 b) a storage unit leased by Soloway, located at Storage Unit A145, Public
20 Storage Inc, 12465 Northrup Way, Bellevue, WA 98005, as well as any computers or
21 other electronic storage media found therein. The storage locker is additionally
22 described in Attachment A, attached hereto and incorporated by reference herein.

23 8. Based on the information set forth below, there is probable cause to
24 believe that Soloway is engaged in criminal activities in violation of the statutes
25 referenced above, and that he has done so, and continues to do so, using one or more
26 computers located at the residential premises identified above, (or stored at the above
27 referenced storage unit). The United States seeks authority to search and to seize, from
28 those premises and/or those computers, items that constitute evidence, fruits and
instrumentalities of violations of Title 18, United States Code, Sections 1028A(a)(1),

1 1037(a)(2) and (a)(3), 1341, 1343, and 1956. The items to be searched and seized are
2 further specified in Attachment B, attached hereto and incorporated by reference
3 herein.

4 **F. Background on Computer and Internet Technologies**

5 9. This application is based on an investigation of activities related to
6 computer and Internet technologies that may not be common knowledge. The
7 following explanation of relevant terms and technologies is based on my training and
8 experience, and is consistent with the results of the investigation.

9 10. **Internet Protocol Address ("IP address"):** An Internet Protocol (IP)
10 address is a unique, 32 bit numeric address used to identify computers on the Internet.
11 An IP address consists of four numbers, each from 0 to 255, separated by periods.
12 Every computer connected to the Internet (or group of computers using the same
13 account to access the Internet) must be assigned an IP address so that Internet traffic
14 sent from and directed to that computer is directed properly from its source and to its
15 destination. IP addresses are typically assigned by Internet service providers ("ISPs"),
16 such as AOL, Earthlink, or Comcast. An ISP might assign a different IP address to a
17 customer each time the customer makes an internet connection (so-called "dynamic IP
18 addressing"), or it might assign an IP address to a customer permanently or for a fixed
19 period of time (so-called "static IP addressing"). Even if an IP address is dynamically
20 assigned, the computer will retain the originally assigned IP address if the computer
21 never disconnects from the network after the initial IP address assignment or the user
22 does not manually reset it. Regardless of whether it is dynamically assigned or static,
23 the IP address used by a computer attached to the Internet must be unique for the
24 duration of a particular session; that is, from connection to disconnection.

1 ISPs typically log their customers' connections, including IP addresses. The ISP
2 can thus identify which of their customers was assigned a specific IP address during a
3 particular session.

4 11. **Domain Name:** In the context of the Internet, a domain name is the
5 logical, text-based equivalent of the numeric IP address. Because it is "logical," and
6 text-based, a domain name - for example, "www.testname.com" - is more easily
7 remembered by humans than is an exclusively numeric IP address, such as
8 "23.45.35.100."

9 Like an IP address, a domain name does consist of a sequence of characters,
10 separated by periods. Domain names are organized hierarchically and read from right
11 to left. The right-most component is the "top level domain." This includes the
12 ".com," ".gov," and ".edu" domains, as well as many others. Top level domains are
13 owned and managed by the Internet sanctioning organizations. The second part of the
14 domain name is owned by the registrant who first registered the name with the
15 sanctioning organizations. Domain name owners can then create sub-domains to
16 provide access to resources they own and/or control.

17 Numerous Internet companies offer free sub-domains to their customers. These
18 companies typically have a collection of domain names that they have registered, and
19 allow their customers to create sub-domains of the domain names and control the IP
20 addresses to which those sub-domains resolve.

21 12. **Domain Name Service ("DNS"):** DNS is the Internet resource for
22 converting the text-based domain names into IP addresses. DNS server computers
23 maintain a database for resolving domain host names and IP addresses, allowing users
24 of computers configured to query the DNS to specify remote computers by the easier-
25 to-remember domain host names (in words), rather than by the difficult-to-remember
26 numerical IP addresses.

1 DNS also thus makes it possible to “move” a host on the Internet (which would
2 entail a change in the underlying IP address), while still preserving the availability of
3 the resource based on its text-based domain name. Users would still request the
4 resource by its (text-based) domain name, and DNS would resolve the name to the new
5 IP address.

6 13. **Server:** A computer that provides a service - such as e-mail or Web data -
7 to other computers (known as “clients”) via a network or the Internet. When a user
8 accesses e-mail or Internet web pages, or accesses files stored on the network itself,
9 those files are pulled electronically from the server where they are stored and are sent
10 to the client’s computer via the network or Internet. Notably, server computers can be
11 physically located in any location; for example, it is not uncommon for a network’s
12 server to be located hundreds (or even thousands) of miles away from the client
13 computers.

14 14. **Proxy Server:** A proxy server is a computer that offers a computer
15 network service to allow clients to make indirect network connections to other
16 computers or network services. An open proxy is a computer that will accept client
17 connections from any IP address and make connections to any Internet resource. A
18 proxy server can be used to camouflage the originating source IP address of an e-mail
19 communication, as the IP address of the originating source of the communication will
20 be replaced in the header by the IP address of the proxy server. Use of multiple proxy
21 servers adds to the difficulty of tracing a communication back to its true original IP
22 address source.

23 15. **Internet Service Provider (“ISP”):** A business that provides
24 connectivity to the Internet. ISPs typically provide the ability to send and receive e-
25 mail, browse the World Wide Web and download (copy) files from Internet servers.

1 Internet Service Providers often offer other Internet-related services such as hosting an
2 Internet site on a web server.

3 16. **Website:** A location on the Internet at which an individual or
4 organization provides information to others about itself. It may also provide links to
5 other Internet sites with common interests or goals.

6 17. **E-mail header:** The beginning of an e-mail message, that contains
7 detailed information (IP address and domain names) of the origin of the e-mail
8 (“From” designation); the destination of the e-mail (“To” designation); as well as date,
9 routing, and possibly subject matter information.

10 18. **Forged e-mail header:** A tactic used to hide the source address of an e-
11 mail by placing false information in the “From:” field of the e-mail header.

12 19. **Bounce back e-mail:** Errors can occur at multiple places in e-mail
13 delivery. A user may sometimes receive a bounce back message from their own e-mail
14 server, and sometimes from a recipient's e-mail server. For example, imagine that
15 Jack (jack@example.com) sends a message to Jill (jill@example.org) at a different site.
16 Once Jack's e-mail server has accepted the message, it must either pass it along to Jill's
17 e-mail server, or else deposit a bounce message in Jack's mailbox. However, problems
18 arise if Jill's e-mail server receives a message with a forged From: field, e.g., if
19 spammer@example.net sends an unsolicited bulk message claiming to be from
20 jack@example.com. In this case, Jill's mail server would send the bounce message to
21 Jack even though Jack never sent the original message to Jill. This is called a bounce
22 back e-mail or backscatter.

1 20. **Spam:** bulk (“multiple¹”) commercial e-mail messages. **“Spamming”** is
2 the abuse of electronic messaging systems by sending multiple commercial e-mail
3 messages.

4 21. **“Opt-in e-mail address”:** the e-mail address of an Internet user who has
5 signaled his/her consent to receive commercial e-mail communications.

6 22. **“WHOIS” Lookup:** A query/response protocol that is widely used for
7 querying a database in order to determine the owner of a domain name, an IP address,
8 or an autonomous system number on the Internet.

9
10 **II. THE INVESTIGATION**

11 **A. Complaints Filed with FTC, BBB and Washington Attorney General’s**
12 **Office, and Statements of Victims of Spamming, Wire Fraud, Mail Fraud, and**
13 **Identity Theft**

14 23. On October 16, 2006, an investigator with the Federal Trade Commission
15 (FTC) contacted the FBI in Seattle regarding a local resident who has been the subject
16 of approximately 100 complaints of spamming, dating back to as early as 1999. I
17 subsequently discussed the complaints with a representative of the FTC, reviewed many
18 of the complaints, and also reviewed some of the summary data that had been gathered
19 by the FTC with regard to the same. As a result, I learned that these 100 different
20 complainants related very similar experiences, that typically included the following:

21 a) The complainants reported that they had received multiple commercial
22 e-mail messages (spam) that essentially consisted of an advertisement for a “bulk” or
23 “broadcast” “e-mail service” business. In the body of the spammed message,
24

25 ¹As noted, *infra*, the term “multiple” is defined within 18 U.S.C. §1037 as “more than 100
26 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages
27 during a 30-day period, or more than 10,000 electronic messages during a 1-year period.”

1 recipients could “click” on a domain name contained in the message, in order to link to
2 the website of the company that was making the e-mail advertisement.

3 If they proceeded to the website, the visitor would see statements,
4 including purported “quotes” from various sources, regarding the ability of the
5 company to reach tens of millions of potential new customers with “broadcast e-mail,”
6 the relatively low cost of “broadcast e-mail” advertisement in relation to its
7 “effectiveness,” and the large sales benefits to be reaped from “broadcast e-mail”
8 advertising. The company represented, on the website, that customers could achieve
9 these positive sales results (e.g., a “500% increase in sales”), either through hiring the
10 company to do broadcast e-mailing on their behalf (to “geographically targeted,”
11 “interest targeted,” and “permission-based opt-in e-mail” addresses available to the
12 company), or, that they could purchase a “software kit” from the company that would
13 enable the customer to send out their own “broadcast” e-mail advertisements. The
14 website reportedly typically offered “lifetime 24/7 customer & technical support” to
15 potential purchasers of either the e-mail “service” or the “software kit,” as well as
16 “money-back guarantees” if the promised sales gains did not materialize within 90
17 days.

18 b) The complainants identified the name of the bulk e-mail business
19 variously as Newport IM Corporation, NIM, Newport Internet Marketing, Newport
20 Corp, NPR, or Broadcast Email Services. They also reported that a variety of domain
21 names were used in the initial spammed advertisements. Although the name of the
22 business and the domain names contained in the advertisements varied, each had some
23 common connections, based on the content of the spam message and the content of the
24 website reached through the domain name. Many of the complainants also reported the
25 name “Robert Soloway” as having a connection to the company, and/or often reported
26 one or the other of two common physical addresses: PO Box 1259, Seattle, WA 98111,

1 or 1200 Western Avenue, 17E, Seattle, Washington. These addresses were seen by the
2 complainants, for example, as an address to which they could send payments to
3 purchase the "broadcast e-mail" service or software. The addresses were also
4 reportedly seen by some complainants after doing additional on-line research, including
5 WHOIS lookups, in an attempt to identify who was responsible for the initial spam they
6 had received, and in their attempts to contact the sender and request that the spamming
7 to them be stopped.

8 c) The complainants generally reported that they had difficulty in
9 identifying the source of the initial spammed messages, because they uniformly
10 contained false "From:" headers. The "From:" headers were either blank, contained
11 the same e-mail address as the "To:" header, or contained an invalid e-mail address.
12 Many of the complainants reported that they had attempted to contact the originator of
13 the e-mail by clicking on the domain name listed in the body of the unsolicited e-mail,
14 and then making a request, through the website, that their e-mail address be removed.
15 Despite their attempts and requests to have their e-mail addresses removed from the list
16 of recipients, however, none of the complainants was successful in doing so. Instead,
17 the volume of spam to them from the company typically increased after they had
18 communicated their request that it be stopped.

19 d) Some of the complainants reported that they had paid for broadcast e-
20 mail services from the company, or had purchased the broadcast e-mail software
21 (typically at a cost of \$149.00). These complainants commonly reported that neither
22 the "broadcast service" or the software was what it was represented to be; that it
23 resulted in spam to addresses that were neither targeted or "opt-in," and as a result of
24 which they had received numerous complaints or been "black-listed" for spamming
25 activity. The purchasers of the software often reported that the product simply did not
26 work, at all. Purchasers of both the "service" and the software reported that the

1 company refused to provide either support, responses to complaints, or the
2 "guaranteed" refund. Many reported that after they had complained or reversed
3 payment charges, they were threatened with additional fees and referral to collection.

4 e) Other of the complainants reported that the company had spammed,
5 fraudulently using e-mail addresses or domain names that belonged to them in the
6 "From:" field in a forged header. These complainants reported that they, in turn, had
7 been the target of complaints and adverse actions because they were falsely being
8 blamed as the originators of spam.

9 24. After receiving the above referenced information from the FTC, I
10 performed a search of business records for the State of Washington, and learned that
11 Newport Internet Marketing Corporation, doing business as NIM Corporation, had
12 been incorporated in California in 1998, and registered with the Washington State
13 Secretary of State as a foreign corporation in December of 2004. The address of
14 record for the corporation, in Washington, was 1200 Western Avenue, Suite 17E,
15 Seattle, Washington, 98101. I next contacted an inspector from the United States
16 Postal Service, who reported that the recipient of record for mail at 1200 Western
17 Avenue, Suite 17E, Seattle, Washington, 98101 was Robert Soloway. The postal
18 inspector also reported that the address of "PO Box 1259, Seattle, WA 98111" was the
19 address for a rented U.S. Postal mail box, at the downtown Seattle Post Office location
20 (301 Union St., Seattle, WA). Postal records revealed that PO Box 1259 had been
21 rented by "Robert Soloway/NIM Corporation" on March 26, 2004. Soloway also
22 indicated, on that form, that the address for "NIM Corporation" was 1200 Western
23 Ave., E17, Seattle, Washington 98101.

24 25. On December 1, 2006, I interviewed AG, who was one of the victims
25 who had complained to the FTC about spamming by Robert Soloway and NIM. AG
26 reported to me, as follows:

27 KENNETH A. SCHMUTZ SEARCH WARRANT AFFIDAVIT - 13
28 USAO #2007R01674/Soloway, Robert A.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101-1271
(206) 553-7970at

1 a) AG has owned a web-hosting business, in Minnesota, since 1996. As
2 part of that business, he owns, designs, and maintains domains and websites for himself
3 and other clients. Since 2003, he has owned his own servers that he has leased and
4 managed for website hosting. In connection with his web-hosting business, AG owns
5 over 400 domains, some of which are used by his clients. Because spam places a
6 burden on the servers that he uses for web-hosting, AG has learned as much as possible
7 about spam, including how to identify fraudulent "From:" information in e-mail
8 headers, and how to track the actual locations of servers hosting websites. He has also
9 worked with the Internet Corporation for Assigned Names and Numbers ("ICANN") as
10 well as other registrars and hosting companies to report forged domain registration and
11 improper use of websites, as well as other online security violations.

12 b) AG stated that he began receiving spam from Newport Internet
13 Marketing in August, 2005; first in his own business and personal e-mail accounts, and
14 then, increasingly, in e-mail accounts that were created when he established new
15 domain names for his clients. AG was able to link the spam to a Robert Soloway
16 through the use of a WHOIS lookup on the domain name that was included in the body
17 of the spam messages. AG also clicked on the domain name listed in the body of the e-
18 mail and was taken to a website that marketed mass e-mail services and products using
19 the name "Broadcast Email Services" and "Newport Internet Marketing" ("NIM").

20 c) AG reported that he had never opted-in to any program offered by
21 Robert Soloway or NIM. AG reported that he had attempted to contact Soloway over
22 100 times by phone, e-mail, fax, and third party complaints, to request that Soloway
23 discontinue sending spam to AG's domains. Soloway would not respond to AG's
24 attempts to communicate, and had never stopped sending spam to domains used by AG
25 or that AG had set up for his clients. In fact, Soloway was continuing to spam AG's
26 domains in December of 2006, when I spoke with him. Often, after AG entered an e-

1 mail address into the "removal" list on Soloway's websites, the account would begin
2 receiving even more spam than before, including spam for generic Viagra, "sexual
3 desire patches," prescription drugs, penis enlargement, pornographic material, stock
4 market "pump and dump" schemes, online casinos, and diploma mill schemes. AG
5 reported to me that he has ~~not~~^{felt} compelled to shut down e-mail addresses that he had
6 established for his clients due to Soloway's unrelenting spam to them.

7 d) Based on his own professional experience in the web-hosting field, AG
8 was able to make some analysis of the spam he received from NIM
9 Corporation/Broadcast Email Services. This included his assessment that the spam
10 communications from these companies contained headers that were forged. Some of
11 the "From:" fields were blank, some had the same name in both the "From:" and the
12 "To:" header field, and others had fake domain names in the "From" field.

13 e) AG reported that on April 17, 2006, at around 11:00 pm, he received
14 approximately 20 spam e-mails from e-mail addresses with the domain name "i-
15 frane.com." AG did a look up on the domain name "i-frane.com" and found that it
16 was not a registered domain, had not been registered in the previous six months, and
17 was available for sale. AG then immediately purchased and registered the domain
18 name "i-frane.com" and set up an e-mail server to capture e-mail that was bounced
19 back to that server. AG did this to catch all the e-mails sent with the "From" address
20 of i.frane.com that bounced back because they were not sent to a valid e-mail address.
21 This information would, in turn, give an indication of how many spam messages were
22 being sent out using "i.frane.com" as the "From:" address. On April 24, 2006, one
23 week after AG had purchased the i.frane.com domain, the e-mail server had received
24 34,784 bounce back spam messages that had been sent out with a forged "i.frane.com"
25 "From:" header. The number of bounce backs subsequently increased to 174,549 -
26 99% of which AG found to contain links to Soloway's web sites in the message body.

1 f) From further analysis of the recorded bounce backs and other
2 information provided to me by AG, it was determined that the spam that had been sent
3 by NIM Corporation/Broadcast Email Services had been sent to thousands of domains
4 using the standard prefixes of advertising@, billing@, feedback@, home@, help@,
5 accounts@, contact@, admin@, guest@, administrator@, orders@, postmaster@,
6 mail@, root@, support@, webmaster@, service@, test@, uucp@, info@, and sales@.
7 (When an e-mail server is set up for the first time, the process used for that set-up
8 automatically and by default creates a group of accounts with standard prefixes.) These
9 default accounts appear to be among the ones that Soloway is routinely using for
10 spamming activities.

11 g) AG reported to me that the spam sent by Soloway has created
12 substantial harm and loss to him both personally and professionally. Included in the
13 costs to him are the need to devote from two to three hours, daily, to efforts to remove
14 spam from his clients' accounts, or to take special precautions in establishing accounts
15 in order to protect them from Soloway's spamming activity.

16 26. On November 29, 2006, an FBI agent interviewed GN. GN had also
17 filed a spamming complaint against Soloway with the FTC. In that interview, and in
18 his complaint to the FTC, GN reported as follows:

19 a) GN stated that in September 2006 he had registered two domain names
20 for his businesses. A few weeks later, GN began to receive spam with forged headers.
21 The "From:" field in the header was either blank, or contained the same information as
22 the "To:" field. That address was GN's e-mail address. The spammed message
23 advertised the ability to mass e-mail "8,000,000 people". The domain contained in the
24 body of the e-mail from which to find out more about the mass mailing system was
25 "www.emailadvertisinginc.com."

1 b) When GN visited the website at the address of
2 www.emailadvertisinginc.com, it appeared to be a website for NPR Corporation,
3 purportedly with an address of 1001 4th Ave - #1259, Seattle, WA, 98111. A second
4 address, however, of NIM, Box 1259, Seattle, WA 98111 was provided in the section
5 of the website for placing software orders by mail. The website also contained a
6 "Charity" section, (in which representations were made about charitable donations
7 purportedly made by the company), that displayed a signature of "Rob Soloway."

8 c) Over the following two months, GN received similar spam messages
9 identifying either "www.emailadvertisinginc.com", "www.newportcorp.cn", or
10 "www.colidsilver.com" as the pertinent domain, in the body of the spam message.
11 Although active at different periods of time, GN found that all three domain names
12 appeared to link to what was essentially - or even exactly - the same website, in terms
13 of its content.

14 d) GN requested to be removed from Soloway's mailing list by using the
15 removal option under the "Contact Us" tab on the website. After GN requested to be
16 removed, however, GN received an increased amount of spam from Soloway. The
17 spam was sent to the default e-mail accounts GN was using on his domains.

18 27. The address of 1001 4th Ave - #1259, Seattle, WA, 98111, which was
19 noted by GN to have been published as the purported address for NPR, was likewise
20 reported by a number of other recipients of the common spam as the spamming
21 company's address. As part of my investigation I researched that address, and learned
22 that it had been an office space for a local bank in past years, but that it had not been
23 occupied by any tenant in recent years.

1 28. On December 12, 2006, an FBI agent interviewed DM. In October, 2006,
2 DM began receiving spam on the twelve domain names that he owned. The spam
3 marketed advertisement of a way to mass e-mail "8,000,000 people." The domain
4 listed in the body of the e-mail to take advantage of the offer was
5 "www.emailadvertisinginc.com." DM realized the email was fraudulent because the
6 header of the e-mail was forged. The "To:" field and the "From:" field were the
7 same. One of the e-mails, for example, contained DM's own address of "sales@d...
8 m...com in both the "From" field and the "To:" field in the header, and he knew he
9 did not send the e-mail to himself. Nor had DM opted-in to any offers to receive
10 unsolicited e-mail.

11 DM did a WHOIS lookup on the Internet to see who was the owner of the
12 domain emailadvertisinginc.com, and learned that it was registered to a Chinese name.

13 29. As part of my investigation in this case, I have learned from the Postal
14 Inspection Service that they have received and reviewed approximately 100 complaints
15 that have been filed with the Better Business Bureau (BBB), against Robert Soloway
16 doing business as Newport Internet Marketing Corporation, also know as Newport IM
17 Corporation (NIM). These complaints were dated between October 2003 and April
18 2007. Like the complaints to the FTC, these included complaints from individuals
19 who had received spam e-mails from NIM; people who had purchased "broadcast
20 email" software from NIM that failed to function as advertised, and who were unable
21 to receive a full refund as promised; people who had purchased a broadcast e-mail
22 service from NIM to advertise their companies' services to "select, quality, opt-in e-
23 mail addresses," only to discover that NIM had sent their information out as spam; and
24 people whose e-mail addresses or domain names had been used without their
25 permission and fraudulently inserted into forged "From:" headers in spammed e-mail
26