

United States District Court

EASTERN

DISTRICT OF

MICHIGAN

UNITED STATES OF AMERICA

CRIMINAL COMPLAINT

v.

CASE NUMBER:

**DANIEL J. LIN,
JAMES J. LIN,
CHRIS CHUNG, and
MARK M. SADEK.**

04-80383

I, Insp. Karl Hansen, the undersigned complainant, being duly sworn, state that the following is true and correct to the best of my knowledge and belief. On or about January 2004 through April 20, 2004, in Wayne and Oakland county, in the Eastern District of Michigan, defendant(s) did *(Track Statutory Language of Offense)*

did, intentionally and materially falsify header information in multiple commercial electronic mail messages and intentionally initiate the transmission of such messages through protected computers and aid and abet one another in the same; and devised a scheme to defraud, for obtaining money by means of false representations and for the purpose of the scheme placed in a post office a fraudulent medical product to be delivered by the Postal Service, and aided and abetted one another in the same, that is, **Daniel Lin, James Lin, Christopher Chung and Mark Sadek** cooperated with one another to advertise fraudulent diet patches via multiple unsolicited commercial e-mail containing deceptive headers. **Daniel Lin, James Lin, Christopher Chung, and Mark Sadek** then sold fraudulent diet patches to respondents depositing said patches in the U. S. Mail, all in violation of Title 18, United States Code, Sections 1037, 1341, and 2.

in violation of Title 18 United States Code, Section(s) 1037, 1341 and 2.

I further state that I am a(n) Postal Inspector, U.S. Postal Inspection Service, and that this complaint is based on the following facts:

See Attached Affidavit Hereby Incorporated by Reference.

Continued on the attached sheet and made a part hereof: Yes No

Signature of Complainant
Inspector K.A. HANSEN
U.S. Postal Inspection Service

Sworn to before me and subscribed in my presence,

Date

at Detroit, Michigan
City and State

Hon. Virginia M. Morgan, U.S. Magistrate Judge
Name & Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT

Karl A. Hansen, being sworn, states as follows:

1. I am a United States Postal Inspector and have been so employed for the past five years. I am currently assigned to the Mail Fraud Team and investigate fraud offenses carried out using the United States Mail. I know the following to be true through investigation and personal knowledge.

BACKGROUND

2. On January 1, 2004, Public Law 108-187, also known as the "Controlling the Assault of Non-Solicited Pornography and Marketing Act" or "CAN SPAM Act" of 2003, became effective. The criminal provisions of this Act are codified at Title 18, United States Code, Section 1037. The stated purpose of the legislation was: "To regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet".
3. Section 1037 of Title 18, United States Code, provides as follows:

"(a) In General.--Whoever, in or affecting interstate or foreign commerce, knowingly--

"(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,

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

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

"(4) registers, using information that materially falsifies the identity of the

actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or
“(5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses, or conspires to do so, shall be punished as provided in subsection (b).

4. The CAN SPAM act of 2003 includes the following definitions:
 1. Multiple.--The term “multiple” means more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period.
 2. Electronic mail address.--The term “electronic mail address” means a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the “local part”) and a reference to an Internet domain (commonly referred to as the “domain part”), whether or not displayed, to which an electronic mail message can be sent or delivered.
 3. Header information.--The term “header information” means the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message.
 4. Initiate -- The term “initiate”, when used with respect to a commercial electronic mail message, means to originate or transmit such message or to procure the origination or transmission of such message, but shall not include actions that constitute routine conveyance of such message. For purposes of this

paragraph, more than one person may be considered to have initiated a message.

5. Protected Computer-- The term "protected computer" has the meaning given that term in Section 1030(e)(2)(B) of Title 18, United States Code.
5. Title 18, United States Code, Section 1030(e)(2)(B) defines a protected computer as a computer: "...which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States".
6. In January 2004, I began investigating a company located in the Eastern District of Michigan that was selling fraudulent medical products via unsolicited commercial e-mail or "SPAM." The company was operating under several business names including "**AIT Herbal**", "**Avatar Nutrition**", "**PHD LLC**", "**DJL LLC**", and "**Phoenix Avatar**" (collectively, "the Avatar Companies"). These products were offered for sale through several Internet websites, which could be accessed by "clicking" on the text contained in the unsolicited commercial e-mail. Although I am aware based on my investigation that these companies are using numerous domain names to sell their products, the websites that are the focus of this affidavit are: **www.countupandlookaway.com**, **www.timezsquarepatry.com**, **www.cisetefuts.com**, and **www.partnerprorgamz.com**. Once an order is placed for these products using the Internet, the products are shipped via U.S. Mail to the customers.
7. On January 26, 2004, I spoke via telephone with Steve Wernikoff, Staff Attorney with the Federal Trade Commission (FTC) in Chicago, Illinois. Mr. Wernikoff informed me that the FTC was investigating various corporate entities operating out of the Detroit Metropolitan area including "**AIT Herbal**", "**Avatar Nutrition**" and "**Phoenix Avatar**". The FTC established an e-mail address of UCE@FTC.gov (UCE stands for Unsolicited Commercial E-Mail) to allow citizens to forward SPAM e-mail that they receive. Mr. Wernikoff further explained that since the effective date of the CAN-SPAM Act, the FTC had received over 10,000 complaints regarding SPAM messages sent by the Avatar companies. According to Mr. Wernikoff, the Avatar companies were suspected of

sending e-mail by use of "open proxy" computers. An open proxy computer is a computer that can be used to transfer e-mail, (without permission of the computer's owner) to send bulk e-mail. Proxy computers are used by spammers because they hide the true source or origin of the bulk e-mail, making it appear as if the e-mail was sent from the Internet address of the proxy computer.

8. I have reviewed the data collected in investigations done by Microsoft Corporation and by the FTC regarding the spam e-mails associated with the Avatar companies. The FTC, as of April 20, 2004, had identified 97 domain names, found in links within spam messages they reviewed, that are for websites that advertise products such as the "Med Diet Patch," the "Slim Form Patch," and a "penis enlargement pill." Microsoft Corporation has also identified some 36 domain names that they also found in spam e-mail messages received by Microsoft customers and have associated them with the above products, and also "Super Viagra," sold from these domains. The websites that are the focus of this affidavit, www.countupandlookaway.com, www.timezsquarepatry.com, www.cisetefuts.com, and www.partnerprorgamz.com, all advertise products sold by the Avatar companies and were all found in links contained in spam e-mails received by both in the Microsoft customers and the FTC spam database.

9. I have reviewed a printed copy of the webpage from www.countupandlookaway.com/m2/ and it reveals the following representations:

1. Med Diet Patch is a cutting-edge, advanced appetite suppressant, metabolism booster, and energy enhancer all in one! With Med Diet Patch, there are no more starvation diets and no difficult and dangerous exercises! It works all day & all night long!
2. Med Diet Patch is 100% all natural and is made with fucus (bladderwrack), an extract of marine algae. fucus (bladderwrack) has been used as a homeopathic remedy for over 100 years to speed up the metabolic rate and break down fatty tissues. (It burns up calories faster)
3. Amazingly, weight-loss is only one of the many benefits associated with the ingredients in Med Diet Patch's proprietary blend! Regular use of Med Diet Patch

will nourish your muscles, remove toxins, and even reduce cholesterol levels; just to name a few!

UNDERCOVER PURCHASE OF MED-DIET PATCH
PERSONS AND ADDRESSES ASSOCIATED WITH THE AVATAR COMPANIES

10. On January 9, 2004 the FTC made a test purchase of the "Med Diet Patch", a product sold by the target company by placing an online order with the website: **www.countupandlookaway.com/M2/**. This website was contained as a link in the SPAM e-mail which was received by the FTC at its e-mail address of **uce@ftc.gov**. A diet patch called the "Premium Diet Patch," was received in a package that bore a return address of **"Avatar Nutrition P.O. Box 251570, West Bloomfield, MI 48325-1570"**. The parcel was affixed with delivery confirmation tag number "2301 0370 0001 3787 6376". A check of the U.S. Postal Service website's "Track & Confirm" function showed that the item had been mailed on January 13, 2004 at 7:46 a.m. from the West Bloomfield, Michigan, Post Office, and had been delivered to the FTC's undercover mailbox on January 15, 2004.

11. On January 27, 2004, I spoke with employees at the West Bloomfield, Michigan, Post Office regarding the business run out of **P. O. Box 251570**. **"AIT Herbal Marketing"** was identified as the company run from the subject box, and I was told that a **Mark Sadek** conducted **AIT Herbal's** business from the West Bloomfield Post Office. I was informed that **Sadek** was known to enter the Post Office a few times a week and mail a total of approximately 100 parcels. I was told that initially, these parcels had consisted of an equal mix of international (Global Priority and Global Express) mail and domestic (Priority and Express) mail. Recently; however, **Sadek's** mailings had shifted to primarily Priority and Express Mail. I was informed that **Sadek** had been mailing parcels for approximately four to five months. While at the Post Office, I obtained information about the credit card used to pay for **Sadek's** mailings. The card was a National City Bank "Business Check Card" in the corporate name **"DJL, LLC"** and bore a card number of **"4802 6700 1123 0019"**.

12. I also obtained the Postal Service Form 1093 (Application for Post Office Box or Caller Service) for **P. O. Box 251570**. The box was opened by "**Mark Sadek**" in the organization names "**AIT Herbal Mkt.**" and "**AVATAR**". The physical address provided was "**7080 Ten Hill Dr. W. Bloomfield, MI 48322.**" In addition, the following information was listed as identification provided upon opening the box: "S 320 585 585 812", "passport", and "Tax ID 421547290".
13. On or about January 28, 2004, the Michigan State Police forwarded a document summarizing information from Michigan Driver's License S 320 585 585 812. According to the document, License S 320 585 585 812 is assigned to **Mark Marwan Sadek**, date of birth 10/21/1976.
14. I had been informed by the FTC that FTC had previously received a consumer complaint against a company by the name of "**PHD, LLC**" for marketing fraudulent medical products such as a diet patch. The complaint records listed an address for **PHD, LLC** of **630 Woodward Avenue, 4th Floor, Detroit, MI 48226**.
15. On January 28, 2004, I spoke via telephone with the assigned letter carrier for **630 Woodward Avenue, Detroit, Michigan 48226**. The letter carrier said that the location consisted of a restaurant and two night clubs. The restaurant is called "Mavericks" and the clubs are the "Good Life Lounge" and "Club Flux". The letter carrier stated that among the mail delivered to the address was mail addressed to "**AIT Herbal Marketing**". The letter carrier said that the mail for AIT Herbal was accepted by one of the two greeters (one male, one female) for the restaurant. The letter carrier indicated that the mail consisted of priority mail parcels using delivery confirmation or Express Mail parcels. It appeared to the letter carrier that the parcels were merchandise returns. The letter carrier said that in conversations with the female greeter at the restaurant, she had remembered that "**James Lin**" was the intended recipient of the mail. During a subsequent conversation on March 16, 2004, the letter carrier informed me that mail addressed to "**634 Woodward Avenue, Detroit, Michigan 48226**" was also delivered to the restaurant and that most of the **AIT Herbal** mail was addressed to "**634 Woodward Avenue**". The letter carrier also said her understanding was that the owner of Maverick's had taken a tub of mail to **James Lin** recently.

16. On January 28, 2004, I conducted a search utilizing the State of Michigan's Bureau of Commercial Services' website for "Maverick's Bar & Grill". The result of the search was a company named "630 Woodward, LLC", with a registered agent of "David W. Johnson" at an address of "1320 Chapin, Birmingham, MI 48009".
17. On January 28, 2004, I printed an article from the electronic version of the *Detroit Free Press* newspaper regarding the Good Life Lounge. The article (published August 22, 2003) began with the sentence: "The Lowdown: Dan Stollman and Dave Johnson, the partners behind the year-old restaurant Maverick's, have expanded their presence with the Good Life Lounge".
18. On March 16, 2004, I received via e-mail, a copy of corporate record searches conducted by the FTC. The following is a summary of that information:

Company Name: Mavericks Bar & Grill Inc.
Registered Agent: David D. Johnson
Registered Office: 1350 Chapin Ave. Birmingham, MI 48009

DBA Name: A I T Marketing & Consulting
Business Address: 1350 Chapin Ave. Birmingham, MI 48009-5166
Contact Name: Chris Chung
Contact Address: 7080 Ten Hill Dr. West Bloomfield, MI 48322

Company Name: DJL, LLC
Registered Agent: Daniel Lin
Registered Office: 1350 Chapman, Birmingham, MI 48009

19. On March 16, 2004, I contacted a delivery supervisor at the Birmingham, Michigan, Post Office regarding 1350 Chapman, Birmingham, Michigan 48009. I was informed that there is no street named "Chapman" in Birmingham, while there is a "Chapin" street. A subsequent check with the Birmingham Post Office revealed that mail is received at 1350 Chapin in the last name of "Johnson".
20. A review of bank records received from the **DJL, LLC** account (described more fully in paragraph 27) at National City Bank revealed automatic payments to Chase Manhattan Mortgage. On April 16, 2004, I received documents submitted pursuant to a subpoena

presented to Chase Manhattan Mortgage Corporation. The documents detailed a real estate transaction between "John Lin" and "James J. Lin". The Department of Housing and Urban Development (HUD) settlement statement indicated that John Lin, living at "391 West Street 4th Floor, New York NY 10014" had purchased the premises at "935 North Maple Avenue, Royal Oak, MI 48067" from James J. Lin. Included in the documents were photocopies of driver's licenses for John and James J. Lin. One such license was New York driver license number "677 864 754" issued in the name "John J. Lin" and reflecting an address of "55W 14th St. Apt. 12H, New York, NY 10011". The second license was Michigan operator license number "L 500 367 441 749" issued in the name "James Joseph Lin" and reflecting an address of "7080 Ten Hill Dr. West Bloomfield, MI 48322-4237". Both licenses reflected a date of birth of September 28, 1977.

CONNECTIONS BETWEEN "AVATAR" COMPANY PERSONS AND ADDRESSES
AND INTERNET ADDRESSES ASSOCIATED WITH SPAMMING

21. The website www.spamhaus.org is a spam tracking information website. I have conducted searches using this website looking for information relating to known persons or addresses associated with the Avatar companies. I conducted a query of the Spamhaus Block List (SBL), a list of previously reported SPAM organizations maintained by Spamhaus.org. According to SBL advisory file 4598, "Daniel Lin" is listed as engaging in proxy spamming from the IP network blocks of 66.58.39.96/29 and 63.211.23.0/24.1 The advisory was posted on December 12, 2003, which is prior to the effective date of 18 U.S.C. § 1037. Also included was Spamhaus' research into the publicly available registration information of the block of IP addresses of 66.58.39.96/29. Listed under the block "CustName" was "Den Lin" and under the address block was

I In this affidavit, and in the databases listing the Internet Protocol addresses of the sources of alleged unsolicited commercial email, ranges of Internet Protocol addresses are often identified using Classless Inter-Domain Routing (CIDR) notation. Under this notation, a range of Internet Protocol address numbers is expressed by listing the first address in the range (the "network prefix"), followed by a slash and a notation of the number of bits that are used to identify the network. This allows breaking up networks into relatively small segments. Thus, the notation 192.168.1.0/24 refers to a network with 256 addresses, beginning at 192.168.1.0 and running through to 192.168.1.255, inclusively. Similarly, the notation 192.168.1.104/29 would refer to a smaller (8-node) network that begins at 192.168.1.104 and continues through 192.168.1.111, inclusively. A fuller explanation of CIDR notation is available at <http://public.pacbell.net/dedicated/cidr.html>.

"PRIVATE ADDRESS WEST BLOOMFIELD MI 48322-4237". In this same Spamhaus entry, under "CUST NAME," the service provider "Cyberonic Internet," was listed. Bank records for the account of DJL, LLC, (more fully described in paragraph 27) show three payments of \$59.99 on 1/22/04 to "Cyberonic Internet Commu."

22. On April 21, 2004 I conducted a query using the Google™ search engine for information regarding the IP address block 63.211.23.0/24. I located a March 25, 2003, newsgroup post that originally appeared in the newsgroup: news.admin.net-abuse.email regarding the IP address block 63.211.23.0/24. The post read "I have proxypot logs showing penis enlargement spam from that network. The spam run only lasted 2 hours; he must have realized it was not a real proxy". The post indicated that it had come from an Alan Curry, and included a contact phone number of (574) 735-0828. Later that day, I called the number and left a message asking Mr. Curry to call me. During various telephone and e-mail communications, Mr. Curry indicated that he had established a "proxypot", which allows one to track persons attempting to send SPAM through appears to be an open proxy. Mr. Curry said that he had recorded several instances of the IP block 63.211.23.0/24 being used to attempt unauthorized access of his proxypot from between March 6, 2003 and May 24, 2003. Mr. Curry said that he recorded the attempted transmission of 18332 messages to 74002 recipients, all of it originating from 63.211.23.0/24. The IP address of 63.211.23.0/24, according to publicly available registration information obtained by spamhaus, showed Daniel Lin listed as an "Admin-contact."
23. I subsequently caused to be served a federal Grand Jury subpoena for records from Cyberonic Internet Communications. The records indicated that the IP address block 66.058.039.097-102 (a block that overlaps 66.58.39.96/29), had previously been assigned to "Daniel Lin" at "7080 Ten Hill Dr. West Bloomfield, MI 48322". The address of 7080 Ten Hill Dr. W. Bloomfield, MI 48322 was used on the Postal Service Form 1093 (Application for Post Office Box or Caller Service) for P. O. Box 251570, which was the P.O. Box opened by "Mark Sadek" in the organization names "AIT Herbal Mkt." and "AVATAR". The address was also listed as the return address on the parcel delivered in the test purchase of the "Premium Diet Patch" which was mailed to the FTC in January 2004.

24. Further research of the Spamhaus' "Registry of Known Spam Operators," for a number of blocks of IP addresses associated with **Daniel Lin** that included references both to the address of **935 N. Maple Ave., Royal Oak, Michigan**, and to the address of **55 W. 14th Street, New York, New York**.
25. On April 19, 2004, I conducted a general search for the terms "**Daniel Lin**" and "**SPAM**" using the Google™ search engine. As a result of my search, I found an entry into the SPAM Block List maintained by SPAMHAUS pertaining to **Daniel Lin**. SBL entry 10174 (last updated on October 28, 2003) indicated that IP address range **38.119.36.0/27** was suspected of being used for "Actively scanning and abusing open proxies continuously". I then conducted an inquiry regarding that block of addresses using the website www.samspace.org. The inquiry revealed that the block of addresses was assigned to "**CMYC LLC, at 391 West Street Suite 5, New York, NY 10014**". This is the same address that was listed as the address of **John Lin** in the mortgage papers received from Chase Manhattan. I have also reviewed a copy of the main page of the website www.avatarnutrition.com that had been captured by the FTC on January 21, 2004. The website indicated that the address of Avatar Nutrition was "**391 West Street, Suite 5, NY, NY 10014**" and that the telephone number was "**866-248-1101**" a telephone number listed for "AIT Herbal" as detailed more fully in paragraph 28. Finally, on April 20, 2004, I was informed by the U.S. Postal Service delivery supervisor at the Village Station Post Office in New York, New York (the delivery unit responsible for 391 West Street, New York, NY 10014) that the last names Johnson, Lin, and Espinoza receive mail at **391 West Street, Apartment 4**. I was also informed that **391 West Street Apartment 5** and **Suite 5** are not valid delivery addresses.
26. I have been advised by the FTC that an anti-SPAM activist sent a message on January 22, 2004 to his anti-SPAM e-mail distribution list inquiring about the IP range 38.112.121.0/24. (This denotation represents a block of IP addresses from 38.112.121.0-255.) The activist reported that this range of IP addresses had connected to an open proxy computer that the activist was running as a "honeypot." A "honeypot," is a computer that appears to be a standard open proxy computer but, instead of allowing the traffic to be relayed through the proxy computer, it logs, or records, the IP addresses

of computers that attempt to relay communications through it. On February 18, 2004, I received via e-mail, a copy of documents submitted pursuant to an FTC civil investigative demand (CID) presented to Cogent Communications. The documents were ownership records for Internet Protocol Addresses assigned to the range 38.112.121.0/24. The records from Cogent Communications indicated that 38.112.121.0/24 was assigned to "Chris Chung" with a telephone number of **866-248-1101**. The organization name was listed at "PHD LLC" with a service address of: "**151 Front St. W. RACO, Toronto, M5J2N1**" and a billing address of "**630 Woodward Ave, Detroit MI 48226**". The address of **630 Woodward Ave., Detroit MI 48226** is the address of "Maverick's Bar and Grill," and is also the location where mail addressed to "AIT Herbal Marketing" had been delivered, and where "James Lin" had received mail. The address of: "**151 Front St. W. RACO, Toronto, M5J2N1**" is the business address of Switch and Data Toronto, Ltd., Canada, formerly known as RACO (Remote Access Company, Ltd.). This company provides "co-location" services, and is discussed in further detail in paragraph 34 below.

27. On or about March 15, 2004, I received via Federal Express, a copy of documents submitted pursuant to an FTC Civil Investigative Demand (CID) presented to National City Bank. The documents were bank records pertaining to accounts linked to bank card number 4802 6700 1123 0119. As stated above, this National City Bank account, in the corporate name "**DJL, LLC**" was used to pay for **Mark Sadek's** mailings from the West Bloomfield, Michigan Post Office. The bank records indicated that the bank card number was linked to National City Bank account number 884282030, in the corporate name **DJL, LLC**. The signatories on the **DJL, LLC** account are listed as: "**Daniel Lin, President;**" "**James Lin, Vice President;**" and "**Mark Sadek, Director of Operations**". Also listed was a taxpayer identification number of "42-1547290". In examining these bank records, I located records showing an "online bill payment" from this account to Cogent Communications, Inc., in the amount of \$3,000 on 1/16/04. As noted above, Cogent Communications was the provider for the IP addresses of 38.112.121.0/24 that were trapped in the honeypot of the spam activist referenced above.
28. On February 18, 2004, I received via e-mail, a copy of documents submitted pursuant to an FTC civil investigative demand (CID) presented to AT&T. The documents were telephone records for toll-free number **866-248-1101**. The records indicated that **866-**

248-1101 was assigned to "**AIT Herbal Marketing**" with an address of "**7080 10 Hill Street, West Bloomf MI 48324**". Listed as a "sales contact name" was "**Mark Sadek**". This telephone number was provided as the contact number for "**Chris Chung**" according to the Cogent Communications records pertaining to the IP number range of 38.112.121.0/24. The records also indicated that the "billed number" for **866-248-1101** was telephone number 248-737-4382. I subsequently caused to be served a subpoena to SBC (the telephone company for 248-737-4382). I was informed that the service name and address for 248-737-4382 was "**James Lin**", residing at "**7080 Ten Hill RD, W Bloomfield, MI 48322**".

29. On April 21, 2004, I received via facsimile, a letter from Mr. Anders Henke, who is the system administrator of Schlund & Partner, AG, in Karlsruhe, Germany. Mr. Henke stated that his company had established what he referred to as a "proxy pot" system on his network, i.e., a system that simulates an open proxy, but does not actually forward spam messages to e-mail inboxes. Mr. Henke's letter provides a detailed explanation of the proxy pot as follows:

"The proxy pot itself is a short computer application simulating an insecurely configured HTTP-proxy and capable of connecting to smtp servers in order to send mail without actually proxying these connections to a remote smtp server. I developed it myself in late December 2002 and early January 2003 and to date, we've so far "grounded" more than 1.8 billion addressed mails with this setup.

The proxy pot itself is not advertised as being a mail server or some public proxy service, it passively waits for incoming connections to act upon. We don't give out authorization for usage to this proxypot and if someone is asking about those systems, we're admitting that those systems are not open proxies but open proxy simulations, build to catch spam attempts. So any scans and network connections to the proxy pot from foreign networks are of 'improperly access'."

30. Mr. Henke further explained that Schlund & Partner AG's proxy pot had logged approximately 5 million attempts to send messages from 30 hosts within the IP range 38.112.121.0/24. These attempts took place starting in early January 2004. In addition,

Mr. Henke notes that there were 380,000 attempts in a 24 hour period shortly before he wrote his letter. As indicated above, this IP range is assigned by Cogent Communications to **Chris Chung of PHD,LLC, 630 Woodward Avenue, Detroit.**

31. On or about April 20, 2004, I reviewed spreadsheets created by Microsoft Corporation containing information regarding nearly 40,000 spam e-mail messages that were received by Microsoft customers. In examining the information pertaining to spam messages which linked to domain names that have been associated with the Avatar companies, I noticed that many of the spam e-mail messages had an IP address recorded as a point of origin that did not appear likely to be the actual source of the spam e-mail advertising diet patches or other products. For example, the IP address that was recorded in the e-mail header as the originating IP address included IP addresses belonging to: the Administrative Office of the United States Courts, the U.S. Army Information Center, Amoco Corporation, Ford Motor Company, and the Unisys Corporation, by way of example only. This information strongly suggests to me that the spam e-mail messages selling the products of the Avatar companies had these originating IP addresses because they were being sent from proxy computers owned by these companies or agencies.

32. From the above investigation, the evidence shows that the same persons and addresses associated with the Avatar companies, that is, **James Lin, Daniel Lin, Christopher Chung and Mark Sadek**, are also persons and addresses associated with Internet addresses that have been the focus of complaints of "proxy" spamming. Based on my training and experience, and on the information I have received from the FTC and other sources in this investigation, I am aware that spammers use open proxy servers to launch their unsolicited email so that the originating IP address of the spam will appear to be that of the proxy server, and not any computer or network traceable to the spammer. For this reason, I believe that when the Internet addresses associated with the above identified subjects connected to the proxy servers listed above, their reason for doing so was to send unsolicited e-mail in a manner that would obscure their true origin.

FINANCIAL CONNECTIONS BETWEEN THE AVATAR COMPANIES,
CERTAIN PERSONS, AND INTERNET ADDRESSES ASSOCIATED WITH SPAM

33. On or about March 25, 2004, I received via Federal Express, a copy of documents received pursuant to an FTC civil investigative demand (CID) presented to First Data Corporation. The documents were records of **AIT Herbal's** account with First Data to handle their credit card transactions. The merchant application reflected a company name of "**AIT Herbal Marketing**" at an address of "**630 Woodward Ave. Detroit, MI 48226**" and a federal tax ID number of "421547290". This was the address of "**Maverick's Bar and Grill**," and is also the location where mail addressed to "**AIT Herbal Marketing**" had been delivered, and where "**James Lin**" had received mail. The owner was listed as "**Daniel Lin**" with an address of "**Ten Hill Drive West Bloomfield, MI 48322**". The address of **7080 Ten Hill Dr. W. Bloomfield, MI 48322** was used on the Postal Service Form 1093 (Application for Post Office Box or Caller Service) for **P. O. Box 251570**, which was the P.O. Box opened by "**Mark Sadek**" in the organization names "**AIT Herbal Mkt.**" and "**AVATAR**", and was listed as the return address on the test purchase of the "Premium Diet Patch" mailed to the FTC in January 2004.
34. Upon reviewing the records received for the checking account of **DJL, LLC**, I found a payment that referenced an account at "**Switch and Data, Inc.**" I caused a Grand Jury subpoena to be served on **Switch and Data, Inc.** for production of any and all records pertaining to **DJL, LLC** and the Avatar company names. On April 7, 2004, I received via U.S. Mail, documents pursuant to a subpoena presented to **Switch and Data Corporation**. **Switch and Data Corporation** is a company that provides co-location services for companies that utilize computer networks. For example, **Switch and Data** provides rental space in a climate-controlled facility and provides services such as power, storage racks, and fire suppression systems. The renter then establishes their computer network in the rented space. The records showed that **DJL, LLC** had contracted with **Switch and Data Corporation** for co-location services in August 2002, and that **PHD, LLC** had contracted with **RACO** (a co-location business recently acquired by **Switch and Data**) in January 2004. The **Switch and Data** facility was located in Southfield, Michigan, while the **RACO** facility was located in Toronto, Ontario. It should be noted that **RACO** in Toronto was listed as the "service address" for the 38.112.121.0/24 IP range that was associated with proxy spamming and was assigned to **Chris Chung** according to the records of Cogent Communications.

35. Included in the **Switch and Data** documents received on April 7, 2004, was a "Master Services Agreement" between **Switch and Data** and **DJL, LLC**. The address for **DJL, LLC** was listed as "7080 10 Hill Drive, West Bloomfield, MI. 48322" and the "Customer's Billing Contact" was listed as "Dan Lin". Also included were copies of check authorization notices payable to Switch and Data drawn on National City Bank account 884282030 in the name **DJL, LLC**.
36. Included in the **RACO** documents received on April 7, 2004, was a "Support Services Agreement" between **RACO Remote Access Company, Limited** and **PHD LLC**. The support services agreement indicates that service will be provided at "151 Front Street West, Suite 706, Toronto, Ontario M5J2N1". As indicated above, this is the same street address that is listed in the records of Cogent Communications for the block of IP numbers of **PHD, LLC**, 38.112.121.0/24. The **RACO** documents also listed "Chris Chung" as president of **PHD, LLC**, at an address of "630 Woodward Ave, Detroit, Michigan 48226." Also included were copies of e-mails exchanged between employees of **RACO** and "Chris Chung". One such e-mail requests that **RACO** change the billing address to "DJL LLC c/o PHD LLC, 7080 Ten Hill Drive, West Bloomfield, MI 48322". In addition, it states: "The company information will stay the same: **PHD LLC, Chris Chung/Owner, 630 Woodward Ave, Detroit, MI 48226**". Another e-mail discusses the issue of access cards for the **RACO** facility. Listed as persons requiring access cards are "James Lin", "David Johnson" and "Wisam Kayhat".
37. On April 8, 2004, I received additional documents from **Switch and Data Corporation** regarding the Toronto facility. Included was a statement from "**Switch and Data Toronto LTD**" billing **PHD LLC** a fee of \$7,163.65 Canadian. According to the statement, the address for **PHD LLC** is "P. O. Box 251570, West Bloomfield, MI 48325-1570". **P. O. Box 251570**, as stated above, was the P.O. Box opened by "**Mark Sadek**" in the organization names "**AIT Herbal Mkt.**" and "**AVATAR**", and was listed as the return address on the test package of the "Med Diet Patch" which was mailed to the FTC in January 2004.

UNLAWFUL SPAM MESSAGES ADVERTISING
THE AVATAR COMPANIES

38. On April 7, 2004, I received via e-mail, a document containing copies of five SPAM messages forwarded to UCE@FTC.gov. Each of the messages was an advertisement for a weight loss patch and included a link directing the person to the Internet address: "www.countupandlookaway.com/m2/" (the internet address listed in ¶9 supra). The headers of the five messages indicated that they had been sent from the following e-mail addresses: "dztwt@aol.com", "qzwhzoppwku@lycos.com", "qqcwdvwqdodjuj@att.net", "hyvkh@aol.com", and "ogioiodw@att.net". Although the messages were purportedly sent from five different e-mail addresses, each had identical text:

Hello,

I finally was able to lose the weight I have
been struggling to lose for years!

And I couldn't believe how simple it was!
Amazing patch makes you shed the pounds!
It's Guaranteed to work or your money back!

If a recipient were to "click" on this message, the recipient would be sent to the website:
"www.countupandlookaway.com/m2/"

39. On April 8, 2004, I received via e-mail from the FTC, a declaration from Michael D. Jensen, M.D., regarding his opinion on the efficacy of diet patches as described in information forwarded to him by the FTC. Dr. Jensen is a Professor of Medicine at the Mayo Medical School and a member of the Endocrine Research Unit of the Mayo Clinic. His board certifications include Diplomat of the National Board of Medical Examiners, Diplomat of the American Board of Internal Medicine, Diplomat of the American Board of Internal Medicine-Endocrinology and Metabolism, and Specialist in Clinical Nutrition of the American Board of Nutrition. Regarding the "Med Diet Patch" advertised on the website: www.countupandlookaway.com/m2/ as well as the product description appearing on the "Premium Diet Patch" that was shipped to the FTC, Dr. Jensen stated that the ingredients in the patches, whether in concert or by themselves, would not achieve the weight loss as advertised.

40. On April 8, 2004, I received via Federal Express, a CD-ROM from Microsoft Corporation containing copies of thousands of SPAM messages that had been sent to Microsoft hotmail customers. The messages contained links to three Internet domains: **www.timezsquarepatry.com**, **www.cisetefuts.com**, and **www.partnerprorgamz.com**. The e-mail messages contained advertisements for three general categories of products: diet patches, erectile dysfunction medication, and penis enlargement pills. The advertisements would refer the recipient to one of three websites within a given domain. For example, an e-mail containing a link to **www.timezsquarepatry.com/m2/** would connect to an advertisement for diet patches, while an e-mail with the link **www.timezsquarepatry.com/c/** would connect to an advertisement for erectile dysfunction medication. The diet patch advertisements contained text identical to that in the e-mails that were linked to "**www.countupandlookaway.com/m2/**" in ¶38 above. The following is a sampling of the messages containing this identical text:

Purported Sender	Date	Website Link	# Addressees Sent To
hjiwzixcsowdax@msn.com	1/11/2004	www.timezsquarepatry.com/m2/	8
iteyxwhbcgyd@aol.com	1/11/2004	www.timezsquarepatry.com/m2/	6
tzpzkgf@msn.com	1/6/2004	www.cisetefuts.com/m2/	1
pkkofrolplgtq@aol.com	1/6/2004	www.cisetefuts.com/m2/	1
zizzwmcabk@msn.com	1/6/2004	www.cisetefuts.com/m2/	1
tljuvjz@msn.com	1/11/2004	www.partnerprorgamz.com/m2/	8
sdppkr@aol.com	1/11/2004	www.partnerprorgamz.com/m2/	11
kpjbg@msn.com	1/11/2004	www.partnerprorgamz.com/m2/	14

41. Further review of the Microsoft CD-ROM revealed that they recorded 8467 SPAM messages referring to a website in the **www.cisetefuts.com** domain between January 6, 2004 and January 17, 2004. In addition, 9023 SPAM messages referring to the **www.timezsquarepatry.com** domain were sent between January 11, 2004 and January 14, 2004; and 9039 SPAM messages referring to the **www.partnerprorgamz.com** domain were sent between January 11, 2004 and January 14, 2004.

42. On April 8, 2004, I received via e-mail, electronic copies of the websites for www.cisetfuts.com/m2/ and www.timezasquarepatry.com/m2/. The websites were captured by FTC staff utilizing a computer program called Teleport Pro. The program works by copying the website's files and placing them in a computer file folder. The files can then be viewed in Adobe Acrobat Reader. The www.timezasquarepatry.com/m2/ website was captured by FTC staff on January 12, 2004 and the www.cisetfuts.com/m2/ website was captured by FTC staff on January 9, 2004. Both websites appear to contain content identical to the website from which the FTC made its test purchase: www.countupandlookaway.com/m2/.
43. On April 9, 2004, I received via Federal Express, a CD-ROM containing copies of SPAM messages detected by Microsoft Corporation for the internet domain www.countupandlookaway.com. The SPAM messages were sent between January 8, 2004 and January 11, 2004. Of the 5083 messages on the CD, 1,387 messages consisted of diet patch advertisements (linking to www.countupandlookaway.com/m2/) and contained the text found in ¶38 above.
44. On April 9, 2004, and on April 15, 2004, I received notification Microsoft and from America Online that the below listed e-mail addresses were not valid addresses at any point from the period July 1, 2003 through April 7, 2004.

Confirmed as Falsified E-mail Return Address	Date	Website Link	# Addressees Sent To
hjiwzixcsowdax@msn.com	1/11/2004	www.timezasquarepatry.com/m2/	8
iteyxwhbcgyd@aol.com	1/11/2004	www.timezasquarepatry.com/m2/	6
tzpzkf@msn.com	1/6/2004	www.cisetfuts.com/m2/	1
pkkofrolplgtq@aol.com	1/6/2004	www.cisetfuts.com/m2/	1
zizzwmcabk@msn.com	1/6/2004	www.cisetfuts.com/m2/	1
tljuvjz@msn.com	1/11/2004	www.partnerprorgamz.com/m2/	8
sdppkr@aol.com	1/11/2004	www.partnerprorgamz.com/m2/	11
kpjbg@msn.com	1/11/2004	www.partnerprorgamz.com/m2/	14
dztwt@aol.com	1/9/2004	www.countupandlookaway.com/m2/	1
hyvvhk@aol.com	1/9/2004	www.countupandlookaway.com/m2/	1

45. The information summarized in the above table shows that a total of 47 e-mails with falsified headers were sent advertising the Avatar diet patch on January 11, 2004, with the link to the **www.timezsquarepatry.com** and the **www.partnerprorgamz.com**. The time frame of January 2004 corresponds with the general time frame of proxy spamming reported by the Mr. Anders Henke as described in ¶129 supra.
46. In addition to the 47 e-mails listed above that were sent with falsified headers, on April 16, 2004 I reviewed a Microsoft-provided CD containing copies of e-mails advertising the **www.countupandlookaway.com** domain. I selected 69 of the e-mails whose headers indicated that they came from a purported AOL e-mail account and that they were sent on January 11, 2004. I caused a federal grand jury subpoena to be issued to AOL for a determination as to whether the accounts were valid at the time. I was informed by AOL that of the 69 subpoenaed accounts, only two of them had been valid e-mail addresses as of January 1, 2004. The remaining 67 e-mail accounts were non-existent. An analysis of the messages revealed that the 67 false return addresses were used to send messages to 282 e-mail accounts on January 11, 2004. A total of 329 e-mails containing false e-mail headers were thus sent out within the 24-hour period of January 11, 2004 advertising the products of the Avatar companies.
47. I have consulted publicly available Internet resources to obtain domain registration information pertaining to the websites **www.countupandlookaway.com**, **www.timezsquarepatry.com**, **www.cisetefuts.com**, **www.partnerprorgamz.com**, which were the websites contained in the SPAM messages referred to herein. These domain names were registered through the domain name registration service called "gandi.net," which, according to the website for gandi.net, is located in Paris, France. In reviewing the bank records of **DJL, LLC**, I found records showing disbursements on 1/12/04 of \$92.83 and 1/16/04 of \$92.48 payable to "gandi.net, 75Paris 3 FR". This indicates that **DJL, LLC** is paying for services to the company serving as registrar to all four targeted websites: **www.countupandlookaway.com**, **www.timezsquarepatry.com**, **www.cisetefuts.com** and **www.partnerprorgamz.com**. These websites were selling products that were advertised via spam e-mail messages containing falsified return addresses.

48. The names and addresses for the registrants of the above websites, listed overseas locations including Lithuania and South Africa. For example, the owner's name and address for the domain name of **www.countupandlookaway.com** was "Adam Love, Annaberger Str. 2936, Chemnitz, Lithuania", with a telephone number of "33.371827635". Although Chemnitz is a city in Germany, I could not locate a Chemnitz, Lithuania. As to the telephone number, "33" is the country code for France, while the country code for Lithuania is "370."


CONCLUSION

49. The information contained within this affidavit is based upon information I have gained from my investigation, my personal observations, my training and experience, and/or information related to me by other postal inspectors and law enforcement officers and/or agents. Since this affidavit is being submitted for the limited purpose of securing an arrest warrant, I have not included each and every fact known to me concerning this investigation.
50. Based on all of the foregoing, I have probable cause to believe that that **Daniel Lin, James Lin, Mark Sadek and Christopher Chung** committed violations of Title 18, United States Code, Sections 1037, 1341 and 2. In particular, I have probable cause to believe that **Daniel Lin, James Lin, Mark Sadek and Christopher Chung** did aid and abet one another in knowingly, intentionally and materially falsifying header information in multiple commercial electronic mail messages and intentionally initiating the transmission of such messages through protected computers; and in devising a scheme to defraud, for obtaining money by means of false representations and for the purpose of the scheme placed in a post office a fraudulent medical product to be delivered by the Postal Service, that is, **Daniel Lin, James Lin, Mark Sadek and Christopher Chung** cooperated with one another to advertise fraudulent diet patches via multiple unsolicited commercial e-mail containing deceptive headers and sent. **Daniel Lin, James Lin, Mark Sadek, and Christopher Chung** then sold fraudulent diet patches to respondents

depositing said patches in the U. S. Mail, all in violation of Title 18, United States Code,
Sections 1037 and 1341.

Karl A. Hansen
U.S. Postal Inspector

Sworn and subscribed before me this 23rd
day of April 2004.



Honorable Virginia M. Morgan
United States Magistrate Judge