

SECRET

①
SWH
4-23-09

IN THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF MISSOURI
WESTERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

(1) AMIR A. SHAH,
[DOB: 01/02/81]

(2) OSMAAN A. SHAH,
[DOB: 12/27/83]

(3) I2O, INC.,
d/b/a DIRECTPO,
d/b/a VISTACLICK,

(4) LIU GUANG MING,
[DOB: Unknown]

and

(5) PAUL F. ZUCKER,
[DOB: 05/14/53]

Defendants.

No. 09-00141-01/09-CR-W-HFS

COUNT ONE:

18 U.S.C. § 371

(Conspiracy)

NMT: 5 years

NMT: \$250,000

NMT: 3 Years Supervised Release

Class D Felony

COUNTS TWO through SIX:

18 U.S.C. § 1030(a)(2) and 2

(Fraud in Connection with Computers)

NMT: 5 years

NMT: \$250,000

NMT: 3 Years Supervised Release

Class C Felony

COUNT SEVEN:

18 U.S.C. § 1030(a)(5) and 2

(Fraud in Connection with Computers)

NMT: 10 years

NMT: \$250,000

NMT: 3 Years Supervised Release

Class C Felony

COUNTS EIGHT through SIXTEEN:

18 U.S.C. § 1037(a)(1) and 2

(Fraud in Connection with Email)

NMT: 3 years

NMT: \$250,000

NMT: 1 Year Supervised Release

Class E Felony

COUNTS SEVENTEEN through

FORTY-TWO:

18 U.S.C. § 1037(a)(2) and 2

(Fraud in Connection with Email)

NMT: 3 years

NMT: \$250,000

NMT: 1 Year Supervised Release

Class E Felony



<u>Defendants/Counts:</u>)	COUNTS FORTY-THREE through
)	FIFTY-ONE:
AMIR SHAH - ALL COUNTS)	18 U.S.C. § 1037(a)(3) and 2
OSMAAN SHAH - ALL COUNTS)	(Fraud in Connection with Email)
I2O, INC. - ALL COUNTS)	NMT: 3 years
LIU GUANG MING - 1, 7-16, 43-51)	NMT: \$250,000
PAUL ZUCKER - 1, 7-16, 43-51)	NMT: 1 Year Supervised Release
)	Class E Felony
)	
)	FORFEITURE ALLEGATION
)	18 U.S.C. § 1030(i) and (j)
)	18 U.S.C. § 1037(c)
)	21 U.S.C. § 853
)	
)	\$100 Mandatory Special Assessment
)	(Each Count)

INDICTMENT

THE GRAND JURY CHARGES:

GENERAL ALLEGATIONS

At all times relevant to this indictment:

Introduction

1. That between on or about January 1, 2004, and continuing thereafter to on or about the date of this Indictment, in the Western District of Missouri and elsewhere, defendants AMIR SHAH, OSMAAN SHAH, I2O INC. d/b/a DIRECTPO, d/b/a VISTACLICK, LIU GUANG MING, and PAUL ZUCKER, and other persons known and unknown to the Grand Jury, were engaged in an unlawful spam email operation that was conducted through the commission of several federal criminal offenses, including Conspiracy, in violation of 18 U.S.C. § 371, Fraud in Connection with Computers, in violation of 18 U.S.C. § 1030, and Fraud in Connection with Email, in violation of 18 U.S.C. § 1037.

2. The defendants' spam email scheme targeted college students all across the United States. The defendants developed individualized email-extracting programs which they used to unlawfully harvest student email addresses from the University of Missouri and over two thousand (2,000) other United States universities and colleges. The defendants then used this unlawfully-gained database of email addresses, numbering well over 8 million, to send targeted spam emails selling various products and services to those college students. The defendants conducted at least thirty-one spam email campaigns directed at college students, using this unlawfully-obtained email database.

3. The defendants employed several fraudulent means to accomplish the goal of sending out as much spam email as possible to college students, in order to make as much money as possible. The defendants would use false and intentionally-misleading information in the spam emails suggesting the defendants had an association with the university or college that the student receiving the spam attended. The defendants used fictitious names and purported to be "campus representatives" from the college of the student receiving the spam. The defendants also falsely claimed that the businesses who manufactured or sold the products in the spam email were "alumni-owned" companies of the student receiving the spam.

4. The defendants were successful in penetrating university and college spam email filters by using a variety of methods. The defendants initially set up hosting in China, which they called "Offshore Bullet Proof Hosting," meaning it was immune to complaints from recipients of their spam and provided them anonymity as to the origins of the spam emails. The defendants also bought and sold proxies, through which they sent their spam email to further camouflage the source of their spam emails and get through spam filters. The defendants also used bulk email

software to falsify email header information and rotate subject line entries, reply-to addresses, message body content, and URLs in their messages. The defendants also provided false information when registering their domain names. Many times during this period, the defendants actually initiated their spam campaigns, and therefore millions upon millions of spam email messages, through the University of Missouri's computer network, causing damage to the network and its users.

5. After learning of the criminal investigation into their activities in 2005 when search warrants were executed on their residence and business, the defendants modified their scheme to continue sending their spam emails to college students. Because officials at the University of Missouri had identified them as the source of the spam emails, the defendants simply removed the email addresses of students of the University of Missouri from their database, and continued to send their spam emails to other universities and colleges throughout the country. The defendants also stopped sending spam email from the University of Missouri at Columbia campus, and instead began leasing hosting and mail services from numerous companies for each subsequent spam campaign. The defendants began registering numerous domain names per spam email campaign, many times numbering well over 60 domain names, which all directed spam email recipients to identical websites selling their products. The defendants spread the hosting and mailing services for these domain names across their network of leased servers to further divide and attempt to conceal themselves as the source of all of these spam email messages.

6. In recent years, the defendants also began sending spam emails soliciting students to subscribe to their social networking website noog.com. These spam emails similarly targeted

college students and were designed to increase the number of subscribers and visitors to their website. By increasing subscribers and visitors to their website through their spam email campaigns, the defendants were attempting to use these inflated statistics to attract investors in their noog.com business venture.

7. The defendants' spam email campaigns generally made money in one of two ways: 1) by making a "referral fee" for sending spam email for products and services sold by others; or 2) by buying products in bulk themselves, and then selling those products through spam email solicitations. In all, the defendants sold over \$4.1 million worth of products through their illegal spam operation. The defendants attempted to conceal the proceeds by various methods including purchasing real property and sending large sums out of the country.

Background of 18 U.S.C. § 1037 (CAN-SPAM Act)

8. In 2003, Congress passed the CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing) Act, making fraud in connection with electronic mail (hereafter "email") a federal crime. The Act became effective January 1, 2004.

9. "Spam" is a commonly used term for unsolicited bulk commercial email. Certain kinds of fraudulent techniques are used by "spammers" to misrepresent and disguise their identity, location, or the nature of their message in order to defeat spam filtering programs and other spam blocking techniques employed by Internet service providers and email users, get into email user accounts, and trick recipients into opening and acting on spam emails. For example, the origin of a spam email can be disguised by inserting false "header information" (which includes addressing information such as the "*from*," "*reply-to*," or "*subject*," lines), by routing

the email through another computer that cannot be traced to the spammer, or by using false information to register a domain name used to send the spam.

10. Under 18 U.S.C. § 1037, it is unlawful for a person to send “multiple commercial electronic mail messages” if such a person (1) accesses a protected computer without authorization to send such email messages; (2) sends them through a protected computer to relay or retransmit them with the intent to hide their origin; (3) materially falsifies the header information in the messages; or (4) uses materially false registration information for two or more domain names that are used to send the messages.

11. **“Multiple commercial electronic mail messages”** 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. For purposes of this Indictment, multiple commercial electronic mail messages sent in violation of 18 U.S.C. § 1037 will be referred to as “unlawful spam email” or “spam email.”

12. An email’s header information or a domain’s registration information is **“materially false”** under 18 U.S.C. § 1037 if it is altered or concealed in a manner that would impair the ability of a recipient of the message, an Internet access service processing the message on behalf of the recipient, a person alleging a violation of the CAN-SPAM Act, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation.

13. The term **“protected computer”** means: a computer (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government

and the conduct constituting the offense affects that use by or for the financial institution or the Government; or B) which is used in or affecting 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;

Other Relevant Definitions for this Indictment

14. Because this Indictment charges crimes that have been committed over the Internet and using computer technology, and this Indictment necessarily contains terms that may not be universally understood, definitions of those terms are included below:

- a. **Addresses:** Every device on the Internet has an address that allows other devices to locate and communicate with it. An Internet Protocol (IP) address is a unique number that identifies a device on the Internet. Other addresses include Uniform Resource Locator (URL) addresses, such as “http://www.usdoj.gov,” which are typically used to access web sites or other services on remote devices. Domain names, host names, and machine addresses are other types of addresses associated with Internet use.
- b. **Botnet:** Derived from “robot network,” a botnet is a network of computers infected with malicious software that allows a third party to control the entire computer network without the knowledge or consent of the computer owners. Each of the infected computers is referred to as a “bot.” A botnet can be used by spammers to send spam through the network of infected bot computers, using each of the infected computers to transmit the spam email, in order to hide the true origin of the spam, help the spammer to remain anonymous, and evade anti-spam filters and other spam-blocking techniques.
- c. **Domain:** A domain is a group of Internet devices that are owned or operated by a specific individual, group, or organization. Devices within a domain have IP addresses within a certain range of numbers, and are usually administered according to the same set of rules and procedures.
- d. **Domain Name:** A domain name is the logical, text-based equivalent of the numeric IP address. Because it is “logical,” and text-based, a domain name – for example, “www.usdoj.gov” – is more easily remembered by humans than is an exclusively numeric IP address, such as “149.101.225.20.” Like an IP address, a domain name consists of a sequence of characters separated by periods. Domain names are organized hierarchically and read from right to left. The right-most

component is the “top level domain.” This includes the “.com,” “.gov,” and “.edu,” domains, as well as many others. Top level domains are owned and managed by the Internet sanctioning organizations. The second part of the domain name is owned by the registrant who first registered the name with the sanctioning organizations. Domain name owners can then create sub-domains to provide access to resources they own and/or control.

- e. **Domain Name Service (“DNS”):** DNS is the Internet resource for converting the text-based domain names into IP addresses. DNS server computers maintain a database for resolving domain host names and IP addresses, allowing users of computers configured to query the DNS to specify remote computers by the easier-to-remember domain host names (in text), rather than by the difficult-to-remember numerical IP addresses. DNS also thus makes it possible to “move” a host on the Internet (which would entail a change in the underlying IP address), while still preserving the availability of the resource based on its text-based name. Users would still request the resource by its (text-based) domain name, and DNS would resolve the name to the new IP address.
- f. **Email Harvesting:** Email harvesting is the process of obtaining lists of email addresses for use in spam email campaigns. Email harvesting is sometimes also referred to as “mining,” “drilling,” or “extracting” for emails. Email harvesters use various methods, including purchasing or trading lists of email addresses from other spammers, use of special software (sometimes known as “harvesting bots” or “harvesters” or “extractors”), which search Web pages, postings on Usenet, mailing list archives, and other online sources to obtain email addresses from data available online. There are many other techniques a spammer may employ to harvest email addresses.
- g. **Email Header:** The beginning of an email message, that contains detailed information (IP address and domain names) of the origin of the email (“From” designation); the destination of the email (“To” designation); as well as date, routing, and possibly subject matter information. Because email headers contain a lot of technical data that is confusing to most email users, the email header is usually “hidden” by default by most email programs. A “forged email header” refers to a tactic used to hide the source address of an email by placing false information in the “From:” field of the email header.
- h. **Instant Messaging (“IM”):** IM is a communications service that allows two users to send messages through the Internet to each other in real-time. Users subscribe to a particular messaging service (e.g., AOL Instant Messenger (AIM), MSN Messenger) by supplying personal information and choosing a screen-name to use in connection with the service. When logged in to the IM service, users can search for other users based on the information that other users have supplied, and they can send those users messages or initiate a chat session. Most IM services

also allow files to be transferred between users, including music, video files, and computer software. Due to the structure of the Internet, a transmission may be routed through different states and/or countries before it arrives at its final destination, even if the communicating parties are in the same state.

- i. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other via standard telephone lines, high-speed telecommunications links (e.g., fiber optic cable), and wireless transmissions. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- j. **Internet Protocol Address (“IP address”):** An Internet Protocol (IP) address is a unique, 32-bit numeric address used to identify computers on the Internet. An IP address consists of four groups of numbers, each from 0 to 255, separated by dots, such as “149.101.225.20.” Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source and to its destination. IP addresses are typically assigned by Internet service providers (“ISPs”), such as AOL, Earthlink, or Comcast. An ISP might assign a different IP address to a customer each time the customer makes an internet connection (so-called “dynamic IP addressing”), or it might assign an IP address to a customer permanently or for a fixed period of time (so-called “static IP addressing”). Even if an IP address is dynamically assigned, the computer will retain the originally assigned IP address if the computer never disconnects from the network after the initial IP address assignment or the user does not manually reset it. Regardless of whether it is dynamically assigned or static, the IP address used by a computer attached to the Internet must be unique for the duration of a particular session; that is, from connection to disconnection. ISPs typically log their customer’s connections, including IP addresses. The ISP can thus identify which of its customers was assigned a specific IP address during a particular session.
- k. **Internet Service Provider “ISP”:** Many individuals and businesses obtain their access to the Internet through businesses known as Internet Service Providers (“ISPs”). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines such as cable TV, DSL or fiber optic service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs’ servers; remotely store electronic files on their customers’ behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting

information, account application information, and other information both in computer data format and in written record format. ISPs reserve and/or maintain computer disk storage space on their computer system for the use of the Internet service subscriber for both temporary and long-term storage of electronic communications with other parties and other types of electronic data and files. E-mail that has not been opened is stored temporarily by an ISP incident to the transmission of the e-mail to the intended recipient.

- l. **Mail Server:** A server set up to receive email from another server and distribute it to users, and to send email from those users to other servers.
- m. **Name Server:** A server connected to a network that maintains a DNS database, and resolves domain names to IP addresses using that database (i.e., the server that determines that "www.usdoj.gov" equals IP address "149.101.225.20" so that computers can connect over the Internet.)
- n. **Proxy Server:** A proxy server is a computer that offers a computer network service to allow clients to make indirect network connections to other computers or network services. An "open proxy" is a computer that will accept client connections from any IP address and make connections to any Internet resource. A proxy server can be used to camouflage the originating source IP address of an email communication, as the IP address of the originating source of the communication will be replaced in the header by the IP address of the proxy server, making it difficult for recipients, Internet providers, or law enforcement to trace the email back to its original source. Spammers often send their spam emails through proxy computers to hide their identity, avoid being detected, and evade anti-spam filters and other spam blocking techniques. A "proxy scanner" is usually a phrase used to describe a program or server designed or used to search the Internet for proxies. A "proxy list" is simply a list of computers that can be used as proxies, which usually consists of a list of the respective IP addresses. A "fresh" proxy list usually refers to a proxy list that is updated frequently, as proxies used by spammers get blacklisted quickly.
- o. **Realtime Blackhole List (RBL):** The Realtime Blackhole List (RBL) refers to the first system that created a list of known sources of spam email. There are now many different organizations and software that principally attempt to accomplish the same goal, that is identify, in realtime, known sources of spam email. These lists are compiled so that a spam filter can check an incoming email message against this realtime database of spam sources, and block any incoming emails from those known spam sources. The benefit of the list being compiled and updated in realtime is a response to how quickly spammers rotate the sources of their messages to avoid being blocked.

- p. **Server:** A server is a centralized computer that provides services for other computers connected to it via a network. The other computers attached to a server are sometimes called "clients." In a large company, it is common for individual employees to have client computers at their desktops. When the employees access their e-mail, or access files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client's computer via the network. Notably, server computers can be physically stored in any location: it is common for a network's server to be located hundreds (and even thousands) of miles away from the client computers. Servers can serve as a location to store shared files, and can be used to store backup information regarding network activity. In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a web site is known simply as a "web server." Similarly, a server that only stores and processes e-mail is known as a "mail server."
- q. **Spam filter:** A spam filter simply refers to the process of filtering email to organize it according to specified criteria or set of rules designed to prevent spam email from being delivered to a email user. There are many types of spam filters used. Most email providers use a combination of techniques to block spam email, or at least mark suspected spam emails for their email users. A common spam filtering technique is a "host-based" filter, which is a filter that focuses on who is sending the email, i.e. if the email comes from a known bad host, the email is blocked. Another common spam filtering technique is a "rule-based" filter, which is a filter that uses a method of analysis of the email content to judge its likelihood of being spam. For example, it may check for common words used in spam like "Viagra" or "Online Pharmacy," or common phrases such as "click here," in addition to checking the host sending the email. The filter then rejects a message if the email has too many known spam elements in the message. Another spam filtering technique is known as a "Bayesian filter" which calculates the statistical probability of email being spam, based upon previous analyses of known spam messages. There are many other spam filter techniques and they are constantly evolving as the techniques used by spammers evolve.
- r. **Viruses:** A virus is a malicious computer program designed by a hacker to (1) incapacitate a target computer system, (2) cause a target system to slow down or become unstable, (3) gain unauthorized access to system files, passwords, and other sensitive data such as financial information, and/or (4) gain control of the target system to use its resources in furtherance of the hacker's agenda. Once inside the target system, a virus may begin making copies of itself, depleting system memory and causing the system to shut down, or it may begin issuing system commands or altering crucial data within the system. Other malicious programs used by hackers include, but are not limited to: "worms" that spawn copies that travel over a network to other systems, "trojan horses" that are hidden in seemingly innocuous files such as email attachments and are activated by

unaware authorized users, and “bombs” which are programs designed to bombard a target email server or individual user with messages, overloading the target or otherwise preventing the reception of legitimate communications.

- s. **Website:** A location on the Internet at which an individual or organization provides information to others about itself. It may also provide links to other Internet sites with common interests or goals.
- t. **Web Host:** This usually refers to a company that stores and hosts websites and delivers those sites for viewing on the Internet. This company provides the servers, hardware, connections to the Internet, etc., where the website is located. The user stores the website’s HTML files and graphics on this server.

Roles in the Conspiracy

15. **AMIR AHMAD SHAH (hereafter “A. SHAH”)** – the co-owner and president of I2O, INC. A. SHAH served as the overall leader of the spam operation described herein, and is the self-proclaimed “idea guy” behind most of I2O, INC.’s schemes. A. SHAH served as the face of the company to negotiate contracts with product suppliers and performed computer and network administration tasks for all aspects of the operation. A. SHAH currently resides at 1520 Washington Avenue, Unit #301, St. Louis, Missouri, 63103.

16. **OSMAAN AHMAD SHAH (hereafter “O. SHAH”)** – the other co-owner of I2O, INC, and A. SHAH’s younger brother. O. SHAH served as the equivalent of a Chief Operating Officer for the conspiracy, and was the “computer guy” who was in primary control of most computer-related tasks in the conspiracy, including creating the individualized email extractors used to harvest student email addresses, administrating the network of websites, designing web sites, and other programming and implementation matters. O. SHAH currently resides at 1301 Fieldcrest, Columbia, Missouri, 65203.

17. **LIU GUANG MING (hereafter “MING”)** – MING partnered with A. SHAH and O. SHAH (hereafter “the SHAHS” when referring to both A. SHAH and O. SHAH) and

rented them access to forty servers under his control in China for hosting websites, sending spam email, and for searching for proxies through which to send spam email. MING also provided hosting and mailing services to other spammers, with the SHAHS acting as the middle-men in the transactions.

18. **PAUL FREDRIC ZUCKER (hereafter "ZUCKER")** – ZUCKER was a spammer sending spam email for his own products who partnered with the SHAHS when the SHAHS were leasing space on MING's servers in China. ZUCKER also purchased proxies from the SHAHS. When ZUCKER was able to provide more reliable proxies himself, he sold proxies to the SHAHS for their spam email campaigns. ZUCKER currently resides at 171 Alder Avenue, Wayne, New Jersey, 07470.

19. **"PROGRAMMER 1"** – an unindicted co-conspirator, associate and former employee of the SHAHS, who created the original email extractor program for the SHAHS. "PROGRAMMER 1" also aided the SHAHS with programming, web design, and various other services throughout the conspiracy.

20. **"PROGRAMMER 2"** – an unindicted co-conspirator, and former employee of the SHAHS, who helped the SHAHS with programming and development of features for their websites.

21. **"WEB DESIGNER 1"** – an unindicted co-conspirator, associate and former employee of the SHAHS, who helped with the design of websites used by the SHAHS and ZUCKER for their spam email campaigns.

22. **"OFFICE MANAGER 1"** – an unindicted co-conspirator, relative, and current employee of the SHAHS, who was hired to manage VISTACLICK PAKISTAN. VISTACLICK

PAKISTAN was set up as a branch office for the SHAHS in Pakistan to do work for the SHAHS on I2O, INC. business, and primarily work for the SHAHS on the development of NOOG.COM.

Company Information

23. **I2O, INC.**, was incorporated in the State of Missouri on November 6, 2003. A. SHAH is the listed president and O. SHAH is the listed secretary. Both A. SHAH and O. SHAH are listed as its Board of Directors. I2O, INC. used 1301 Fieldcrest, Columbia, Missouri, as its corporate address from November of 2003 until July of 2008. The residence at 1301 Fieldcrest, Columbia, Missouri, is the address the SHAHS used as their primary residence while attending the University of Missouri at Columbia. In July of 2008, the corporate address was changed to 746 Spring Hill Farm Drive, Ballwin, Missouri. This is the address used as a residence by the SHAHS' parents.

24. **I2O, INC.**, does business through many entities, all of which were created by A. SHAH and owned by I2O, INC.:

- a. On September 12, 2001, A. SHAH caused and directed the creation of an entity called "DIRECTPO" through the registration of a fictitious name filing with the Missouri Secretary of State. "DIRECTPO" was initially registered as "AMIR SHAH d/b/a DIRECTPO." The listed address given for the entity was 746 Spring Hill Farm Drive, Ballwin, Missouri. In May of 2004, the registration was changed to "I2O, INC. d/b/a DIRECTPO" and the listed address was changed to 1301 Fieldcrest, Columbia, Missouri;
- b. On May 28, 2004, A. SHAH caused and directed the creation of an entity called "VISTACLICK" through the registration of a fictitious name filing with the Missouri Secretary of State. "VISTACLICK" was registered as "I2O, INC. d/b/a VISTACLICK." The listed address given for the entity was 1301 Fieldcrest, Columbia, Missouri;
- c. On May 28, 2004, A. SHAH caused and directed the creation of an entity called "FUNDING JUNCTION" through the registration of a fictitious name filing with the Missouri Secretary of State. "FUNDING JUNCTION" was registered as

"I2O, INC. d/b/a FUNDING JUNCTION" The listed address given for the entity was 1301 Fieldcrest, Columbia, Missouri;

- d. On May 28, 2004, A. SHAH caused and directed the creation of an entity called "VERIDIO" through the registration of a fictitious name filing with the Missouri Secretary of State. "VERIDIO" was registered as "I2O, INC. d/b/a VERIDIO" The listed address given for the entity was 1301 Fieldcrest, Columbia, Missouri;
- e. On May 28, 2004, A. SHAH caused and directed the creation of an entity called "OIBA" through the registration of a fictitious name filing with the Missouri Secretary of State. "OIBA" was registered as "I2O, INC. d/b/a OIBA" The listed address given for the entity was 1301 Fieldcrest, Columbia, Missouri;
- f. On May 28, 2004, A. SHAH caused and directed the creation of an entity called "TEXTBOOK REGISTRY" through the registration of a fictitious name filing with the Missouri Secretary of State. "TEXTBOOK REGISTRY" was registered as "I2O, INC. d/b/a TEXTBOOK REGISTRY" The listed address given for the entity was 1301 Fieldcrest, Columbia, Missouri;
- g. On November 22, 2006, A. SHAH caused and directed the creation of an entity called "YOUR CITY DEVELOPMENT" through the registration of a fictitious name filing with the Missouri Secretary of State. "YOUR CITY DEVELOPMENT" was registered as "AMIR SHAH d/b/a YOUR CITY DEVELOPMENT" The listed address given for the entity was 746 Spring Hill Farm Drive, Ballwin, Missouri.

25. A. SHAH and O. SHAH, through I2O, INC. and its various entities, opened and controlled the following bank accounts:

- a. U.S. Bank account number XXXXXXXXX-6708 in the name of OSMAAN SHAH;
- b. U.S. Bank account number XXXXXXXXX-2816 in the name of AMIR SHAH d/b/a FUNDING JUNCTION;
- c. U.S. Bank account number XXXXXXXXX-2743 in the name of AMIR A. SHAH d/b/a YOUR CITY DEVELOPMENT;
- d. U.S. Bank account number XXXXXXXXX-9795 in the name of I2O, INC.;
- e. U.S. Bank account number XXXXXXXXX-4348 in the name of DIRECTPO;

Background

26. Beginning in or before 2001, the SHAHS began harvesting email addresses from colleges and universities across the United States. They sent spam emails selling products to students using this database of email addresses. During 2002 and 2003, the SHAHS also formed relationships with other spammers through discussions on America Online Instant Messenger Chat (AIM). The SHAHS discussed various spamming techniques, including the best software to use, how to penetrate spam filters, and how to obtain proxies through which to send email.

27. In or before 2002, the SHAHS partnered with co-defendant MING who resided in China, with whom they communicated via AIM, to provide what they called "Offshore Bullet Proof Hosting." A. SHAH, O. SHAH, and MING advertised their services via AIM to other spammers. One of their advertisements read:

Servers are located in China and run by some of their largest ISPs. Our tech support team manages servers around the clock with constant contact from China to US. We have several sites sending millions of emails per day. Unlike other hosts, you will NOT need to switch domain names or experience periods of downtime. Our uptime guarantee is 90%. If you are serious about bulk mailing, you have come to the right place.

The SHAHS solicited customers and collected the money, which they sent to MING. MING performed the network administration duties in China, and worked to keep the websites operational despite complaints from spam email recipients or ISPs.

28. One of the customers of the SHAH/MING "Offshore Bullet Proof Hosting" service was co-defendant ZUCKER. ZUCKER also provided O. SHAH tips and tricks of the spamming trade during their discussions on AIM. On or about June 30, 2003, O. SHAH was communicating with ZUCKER via AIM chat, and asked ZUCKER, "im gonna try to blast out some mail at my university . . . you don't happen to have any proxies which I could try do you?"

Could I buy proxies from you?" ZUCKER replied, "How many do you need?" O. SHAH responded, "well I just wanted to test it out really, see how fast I could send over there. im gonna mail for like 2 hours I think I should be able to get out a million." ZUCKER said, "Give me about an hour. No charge." Later that same day, O. SHAH told ZUCKER, "im sending some mail now, at about 110,000 per hour."

29. ZUCKER and O. SHAH continued to communicate via AIM chat about spamming, as O. SHAH began to learn from ZUCKER how to send spam more effectively. On or about July 14, 2003, O. SHAH communicated with ZUCKER via AIM chat, and said, "man im using some of those proxies to mail for myself. im processing 1 million emails an hour . . . delivering about 65%." O. SHAH told ZUCKER, "kinda exciting really." ZUCKER responded, "it's a rush." O. SHAH said, "Ha yea."

30. Between on or about October 6, 2003, and on or about October 13, 2003, A. SHAH traveled to China to meet with MING in person to discuss their business, and other opportunities they could pursue. One of the ideas A. SHAH and MING discussed was setting up proxy scanners on MING'S system that could provide customers access to "fresh" lists of working proxies 24 hours a day, which would be available for the customer to download.

31. Due to the speed of the University of Missouri at Columbia's (hereafter "MU") network, O. SHAH continued to send his spam emails from campus. O. SHAH accomplished this by either connecting via the wireless Internet service provided by MU from anywhere on campus, or by connecting directly to the MU network through an ethernet cable connection in a classroom or other MU building. On or about October 6, 2003, O. SHAH chatted via AIM with A. SHAH (who was in China with MING) about sending spam from campus. O. SHAH said,

"im just doing it from school now." A. SHAH said, "Really?" O. SHAH replied, "no worries." Later that same day, O. SHAH said, "okay I am blasting college right now. by the way . . . good lod amir . . . the bandwidth . . . OH MY . . . I can send 2 million an hour . . . here at school" A. SHAH asked, "Where? Damn" O. SHAH said, "well I went into A&S and am plugged into the cable not using the wireless." A. SHAH said, "Nice." O. SHAH said, "waaay faster. jease this is sick."

32. The SHAHS began to receive complaints from university administrators. These complaints were usually received through the website the SHAHS were sending spam to direct students to visit. The SHAHS usually set up an online help or chat feature on the website, which was designed for a customer to submit any questions they had through the website when ordering a product. Because the SHAHS had otherwise hidden their identity as the source of the spam email, email administrators attempting to reach them used this online chat feature to voice their concerns. On or about October 8, 2003, O. SHAH communicated with A. SHAH via AIM and pasted in the below online chat he had with a college administrator:

[Email Admin] is Calling for help.

Sarah: Hello, this is Sarah. I am a live help operator with UniversityMagazines.com. Can I assist you in any way?

[Email Admin]: I'm a system admin at a private college and need to have email addresses removed from your mailing list.

Sarah: Hello *[Email Admin]*, which university are you affiliated with?

UniversityMagazines.com uses a network of campus affiliates across the nation to market its promotions through newspapers, bulletins, etc.

[Email Admin]: *[College]* . . . *[College].edu*

Sarah: Okay great. I will forward this message to our managing offices, and make sure that your campus representative has been notified.

Sarah: Thank you for using our live help!

[Email Admin]: Have the campus rep contact me please *[Email Admin phone number]*

A. SHAH replied, "hahaa . . . nice . . . good work." Later the next day, on or about October 9, 2003, O. SHAH communicated via AIM with an unknown individual where he joked, "if only these people knew when they were ordering that the entire operation is being run by one man." The person responded, "yes . . . you are good." O. SHAH said, "one man, who uses the name 'Sarah' . . . sarah mitchell . . . thats me."

33. The SHAHS continued to send spam emails to their lists of universities and colleges, and began to receive more complaints from their administrators. On or about October 9, 2003, O. SHAH was communicating with A. SHAH via AIM, and told him, "I have mailed 5 of 13 files . . . im going to DELIVER 2 million . . . as I said . . . and we should get 1/1000 from that at the rate we are going cause each file is 200,000." A. SHAH said MING told him their sites were not getting too many complaints. O. SHAH responded, "we get a few complaints from admins from schools in our contact form." A. SHAH said, "yeah." O. SHAH said, "I worry about them, but whatever." A. SHAH said, "What they say?" O. SHAH replied, "just stuff like, remove all email addresses from our school or we will take further action." A. SHAH replied, "yeah . . . no worries." Four days later, O. SHAH was still sending spam email for this campaign, and he told A. SHAH via AIM on or about October 13, 2003, "I got a million emails to deliver still man." They discussed whether they should get another IP address to avoid getting blocked. O. SHAH said, "I don't think its going to get blocked. Anyways . . . no worries we made our kill . . . haha."

34. Toward the end of 2003, the SHAHS continued to use MU's network to send spam emails. On or about November 24, 2003, O. SHAH bragged to "WEB DESIGNER 1" via AIM chat that, "last night I snuck into A&S . . . was in a class room for like an hour and a half

consuming the entire schools bandwidth . . . soooooo fast.” On or about December 1, 2003, O. SHAH told A. SHAH via AIM chat, “wow . . . same classroom . . . no one here.” A. SHAH responded, “haha.” O. SHAH said, “I’m blasting at around 800,000 an hour.” Later he told A. SHAH, “Literally . . . SAME DOOR WAS OPEN.” A. SHAH said “lol.” O. SHAH said, “no one has been in the class since me . . .” A. SHAH replied, “haha . . . hahaha.” On or about January 1, 2004, O. SHAH communicated via AIM chat with an unknown individual and said, “im in A&S . . . lol . . . can you believe it . . . still not locked up.” They responded, “hahaha . . . thats awesome. What are you mailing? Cameras?” O. SHAH said, “yea . . . just finishing up.”

35. In 2003, the SHAHS conducted at least three spam campaigns that targeted universities and students. Between April and May of 2003, they sent spam email selling teeth whiteners. Between August and November of 2003, they sent spam emails for magazine subscriptions. Between November and December of 2003, they sent spam emails advertising spring break travel offers.

36. On or about March 11, 2004, O. SHAH learned that a former customer from “Offshore Bullet Proof Hosting” was being sued under the CAN-SPAM Act. O. SHAH told MING, “Hey Liu, one of the guys we hosted a while back has a lawsuit against him from Microsoft, AOL, Earthlink, and Yahoo. Can you believe that? It is all over the news here.” O. SHAH was referring to the lawsuit filed on March 10, 2004, by AOL, Earthlink, Microsoft, and Yahoo against some of the most prolific spammers of that time. One of the individuals named in that lawsuit had paid the SHAHS for hosting and mailing services through the SHAH/MING “Offshore Bullet Proof Hosting” service in 2003. In 2005, the book entitled *Spam Kings: The Real Story Behind the High-Rolling Hucksters Pushing Porn, Pills, and @*#?% Enlargements*

was written about many spammers, but focused on the rise and fall of some of the individuals named in that lawsuit.

37. On February 23, 2005, search warrants were executed on the SHAH residence located at 1301 Fieldcrest, Columbia, Missouri, and on their business address 1711 Parris Road, Columbia, Missouri. At that time, it was determined that the SHAHS possessed files containing over 3 million student email addresses from 2002 and files containing over 5 million student email addresses from 2003 on their computers. Also during 2002 and 2003, the SHAHS sent spam to email addresses beyond just their database of student email addresses. It was determined that the SHAHS possessed files containing over 37.5 million AOL email addresses, over 33.7 million MSN email addresses, over 10.8 million Hotmail email addresses, over 5.2 million Yahoo email addresses, and over 4 million United Kingdom email addresses.

COUNT ONE
(Conspiracy)

38. The General Allegations set forth in paragraphs One through Thirty-Seven of this Indictment are re-alleged as if stated fully here.

39. Between on or about January 1, 2004, and continuing through on or about the date of this Indictment, within the Western District of Missouri and elsewhere, AMIR SHAH, OSMAAN SHAH, I2O INC. d/b/a DIRECTPO, d/b/a VISTACLICK, LIU GUANG MING, and PAUL ZUCKER, and other persons both known and unknown to the Grand Jury, did knowingly and intentionally combine, conspire, confederate, and agree with one another to:

- a. Intentionally access a protected computer without authorization and in excess of their authorization, and thereby obtain information from a protected computer, which was a computer involved with interstate or foreign commerce or communication; and did so in furtherance of a criminal offense, that is, Fraud in Connection with Electronic Mail, in violation of 18 U.S.C. § 1037 and the offense

was committed for commercial advantage or private financial gain. All in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(i) and (ii);

- b. Knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer, and cause loss during a one-year period aggregating at least \$5,000 in value, in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and 1030(c)(4)(A);
- c. Knowingly access a protected computer without authorization, and intentionally initiate the transmission of multiple commercial electronic email messages from or through such computer, in violation of Title 18, United States Code, Section 1037(a)(1), 1037(b)(2);
- d. Knowingly use a protected computer to relay and 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, in violation of Title 18, United States Code, Section 1037(a)(2), 1037(b)(2);
- e. Knowingly materially falsify header information in multiple commercial electronic mail messages, and intentionally initiate the transmission of such messages, in violation of Title 18, United States Code, Section 1037(a)(3), 1037(b)(2).

THE OBJECT OF THE CONSPIRACY

40. The object of the unlawful spam email conspiracy was personal financial gain to the co-conspirators, who received money and other things of value as a result of their illegal activities when the recipients of the unlawful spam emails, sent in furtherance of the conspiracy, responded to various commercial offers or advertisements contained in, and promoted by, the spam emails.

MANNER AND MEANS OF THE CONSPIRACY

41. The defendants employed several means to accomplish the common goal of sending out as much unlawful spam email as possible in order to make as much money as possible, including but not limited to the following:

- a. It was part of the conspiracy that its members would and did create computer programs which they used to harvest email addresses from universities and colleges in the United States;
- b. It was further part of the conspiracy that its members would and did use their email extracting programs each year to refresh their database of student email addresses;
- c. It was further part of the conspiracy that its members would and did initiate spam email campaigns directed at college students with products such as digital cameras, MP3 players or Ipods, magazine subscriptions, spring break travel offers, pepper spray, and teeth whiteners, as well as solicitations to join their social networking website noog.com;
- d. It was further part of the conspiracy that its members would and did create websites to market and sell products and services advertised by their spam emails;
- e. It was further part of the conspiracy that its members would and did draft the content of the spam emails with carefully crafted language designed to entice the most recipients to purchase the offered product or service;
- f. It was further part of the conspiracy that its members would and did impersonate real students or create fictitious students or "student representatives" for each of their spam email campaigns, and used these aliases or fictitious names when communicating with students who received their spam emails, both in the initial spam email, and also in any follow-up contact with the student via email or chat;
- g. It was further part of the conspiracy that its members would and did attempt to make the students who received their spam email believe that the sender of the spam email was affiliated with, or a part of, the university or college to which they were sending spam email;
- h. It was further part of the conspiracy that its members would and did use false and misleading information in the content of their spam emails implying or directly stating that the company providing the product or service offered in the spam email was a business or company owned and operated by "alumni" of the university or college receiving the spam email;
- i. It was further part of the conspiracy that its members would and did buy and sell lists of "proxy computers" or "proxies" to relay or retransmit multiple commercial email messages in order to deceive and mislead recipients, or any Internet access service, as to the origin of the spam;

- j. It was further part of the conspiracy that its members would and did use proxy finder programs to maintain a constant and fresh list of available proxies to use to then send unlawful spam email;
- k. It was part of the conspiracy that its members would and did create and operate computer networks, in the Western District of Missouri and elsewhere, for transmitting unlawful spam email;
- l. It was further part of the conspiracy that its members would and did pay and direct others to perform network administration services and programming for computer systems used to send unlawful spam email;
- m. It was further part of the conspiracy that its members would and did communicate with each other via email, instant messaging, and Internet relay chat in order to manage the unlawful spam email operation;
- n. It was further part of the conspiracy that its members would and did set up a hosting service in China, which they advertised as "Offshore Bullet Proof Hosting," which was a network which included over forty servers to provide hosting and mailing services for themselves and other spammers;
- o. It was further part of the conspiracy that its members would and did set up a network of domestic hosting and mail servers, which they used to divide and conceal the source and size of their spam email campaigns,
- p. It was further part of the conspiracy that its members would and did use this network of domestic hosting and mail servers to host dozens of identical websites per campaign, many times numbering over sixty websites, in order to divide, obscure, and conceal the source of the emails, and to attempt to keep the source of their spam emails from being blocked by spam filters;
- q. It was further part of the conspiracy that its members would and did use services such as "whoisguard" protection while registering these dozens of domains names, in order to conceal the registry information for these domain names from any person who received a spam email from them;
- r. It was further part of the conspiracy that its members would and did use bulk mail programs such as Group Mail, Supermailer, and Dark Mailer, to send spam email and avoid spam filters by rotating subject lines, reply addresses, message content and URLs, and other information in the email header and email body content;
- s. It was further part of the conspiracy that its members would and did use these mass mailing software programs to materially falsifying email header information, and employed such software to send unlawful spam email;

- t. It was further part of the conspiracy that its members would and did send unlawful spam email and paid others to do so;
- u. It was further part of the conspiracy that its members would and did purchase real property in order to conceal and hide the proceeds of their unlawful spam campaigns;
- v. It was further part of the conspiracy that its members would and did send large sums of money to banks out of the country to conceal and hide the proceeds of their unlawful spam campaigns;

OVERT ACTS

42. In furtherance of the conspiracy, and to accomplish the objects of the conspiracy, one or more members of the conspiracy committed and caused to be committed various overt acts within the Western District of Missouri and elsewhere, including, but not limited to, the following:

Creating I2O, INC.

43. It was part of the conspiracy that the SHAHS caused and directed the creation of I2O, INC., of which they were the co-owners, and all of its various business entities, including DIRECTPO and VISTACLICK, as well as directed the creation of several bank accounts in the names of these entities, all as described in paragraphs 23-25 of this Indictment, which is incorporated by reference.

44. Between on or about May 1, 2004, and October 31, 2004, the SHAHS hired and paid three employees to work for I2O, INC. These three employees were paid an hourly wage out of U.S. Bank account number XXXXXXXXX-4348 in the name of DIRECTPO. The three employees were "PROGRAMMER 1," "PROGRAMMER 2" and "WEB DESIGNER 1." All three performed work for the SHAHS to help the development of the websites the SHAHS used to sell the products promoted by their spam campaigns.

Harvesting Student Email Addresses

45. The computer-intrusion related offenses charged in Count Two through Count Six, regarding the use of email extractor programs to unlawfully harvest student email addresses, were within the scope of the conspiracy and were committed by the conspirators in furtherance of the conspiracy. These offenses are alleged and incorporated into this count as overt acts.

46. On or about September 3, 2004, O. SHAH communicated with "PROGRAMMER 1" by AIM chat about how to develop and fix problems with the email extractor program "PROGRAMMER 1" had previously written. "PROGRAMMER 1" had previously created an email extractor program he called "Flex Collector." On or about September 3, 2004, "PROGRAMMER 1" sent O. SHAH via AIM chat a link to the updated version called "Reflex." O. SHAH replied, "man thanks so much . . . this is so sweet . . . so far so good." Later that day, the program was not working properly, and O. SHAH asked "PROGRAMMER 1" to fix it. "PROGRAMMER 1" replied, "alright . . . gimme a sec, im gonna fix the drilling too."

47. On or about September 4, 2004, "PROGRAMMER 1" communicated with O. SHAH via AIM chat and said, "it ought to be fixed . . . ill put it up." O. SHAH said, "okay awesome." "PROGRAMMER 1" said, "should say version 1.3" O. SHAH said, "alright cool, I got it . . . wow this thing is really coming along . . . perfection is nearing." "PROGRAMMER 1" replied, "hah, right."

48. Later that same day, on or about September 4, 2004, O. SHAH used "Reflex" to harvest student emails. O. SHAH told "PROGRAMMER 1" via AIM chat, "oh man . . . by the way . . . mizzou tried to hack!" "PROGRAMMER 1" replied, "oh yea, really, I was gonna say." O. SHAH said, "but reflex defeated." "PROGRAMMER 1" said, "hahahaa." O. SHAH said,

“Can you believe that . . . they use an encryption.” O. SHAH then described to “PROGRAMMER 1” how he modified reflex to make it work. “PROGRAMMER 1” said, “lol, nice. Thats quite a counterhack.” O. SHAH said, “yea . . . they got defeated for yet another year . . . maybe next time . . .”

49. On or about February 23, 2005, in the Western District of Missouri, the SHAHS possessed the two email extracting programs created by “PROGRAMMER 1,” that is “Flex Collector” and “Reflex.” The SHAHS also possessed hundreds of programs that were modifications of the email extraction programs created by “PROGRAMMER 1.” These modified programs were individualized email extracting programs, which the SHAHS named for the university or college they were designed to extract email addresses from.

50. On or about February 23, 2005, in the Western District of Missouri, the SHAHS possessed numerous text files containing email addresses from colleges and universities from all across the United States. The SHAHS possessed individual “text” files that were named for the particular university or college that the emails were from. The SHAHS also possessed a “text” file which contained over 8 million university and college email addresses. This list contained email addresses from at least two thousand (2,000) different universities and colleges from across the United States.

Sending Spam Email Through the University of Missouri Computer Network and Causing Damage to the Missouri Computer Network

51. The computer intrusion related offense charged in Count Seven, regarding the unlawful use of the University of Missouri network to send spam email, is within the scope of the conspiracy and was committed by the conspirators in furtherance of the conspiracy. This offense

is alleged and incorporated into this count as an overt act. In 2004, the SHAHS conducted at least seven spam email campaigns directed at college students. During each campaign, spam email messages were sent from MU's campus, in the Western District of Missouri, as described in Count Seven.

52. In or about February of 2004, the SHAHS conducted a spam email campaign selling pepper spray to college students. During this campaign, the SHAHS sent their spam emails from the MU campus, through its network. On or about February 9, 2004, O. SHAH communicated with A. SHAH by online chat, where he said, "just getting situated." A. SHAH replied, "1 million . . . ready, go . . . one million every day . . . ready go" O. SHAH replied, "haha." A. SHAH said, "1 million . . . just want to done blow it up." On or about February 12, O. SHAH told A. SHAH via AIM chat, "I can mail hella more tonight." O. SHAH told A. SHAH, "I should be blasting quite fast." A. SHAH replied, "good deal." O. SHAH responded, "im plugged into the cable . . . what you don't realize is I can turn off EVERYONE on the network." Later that day, O. SHAH said, "aight . . . well im blasting again . . . just getting a big load out before the weekend." O. SHAH also told A. SHAH, "well . . . hey I gotta get out of this room . . . cause there is a class here coming . . ." A. SHAH responded, "lol . . . ok" O. SHAH said, "aight . . . moved to a different class."

53. On or about October 12, 2004, O. SHAH sent spam email for the TEXTBOOK REGISTRY campaign through the MU network. On or about October 12, 2004, administrators at MU discovered and were monitoring the SHAH TEXTBOOK REGISTRY spam email campaign being sent through their computer network. Network administrators were able to pinpoint the location on campus, Cornell Hall, where the email transmissions were coming from

into their network. Security officials went to that location and discovered O. SHAH sitting in a classroom with a laptop computer connected to the Internet.

54. Between December of 2004, and January of 2005, the SHAHS conducted a spam email campaign selling digital cameras to college students. During this campaign, the SHAHS sent their spam emails from on the MU campus, through its computer network. On or about December 1, 2004, O. SHAH was communicating via online chat with A. SHAH, and described another time he sent spam email from the MU campus. O. SHAH said, "sweet, well I just finished blasting out an 8th of the list . . . it is looking good though man." A. SHAH asked, "Where r u?" O. SHAH said, "I can't believe it . . . on campus." Later that same day, O. SHAH asked, "do you want me to just mail like 2 mill? 4 files?" A. SHAH responded, "haha" O. SHAH said, "well I will mail the same amount tomorrow."

Spamming Through Botnets and Using Materially False Headers

55. The spam email-related offenses charged in Count Eight through Count Sixteen, regarding the use of proxies or botnets to send spam email, were within the scope of the conspiracy and were committed by the conspirators in furtherance of the conspiracy. These offenses are alleged and incorporated into this count as overt acts.

56. The spam email-related offenses charged in Count Forty-Three through Count Fifty-One, regarding the use of false header information to send spam email, were within the scope of the conspiracy and were committed by the conspirators in furtherance of the conspiracy. These offenses are alleged and incorporated into this count as overt acts.

57. In or about September of 2004, the SHAHS conducted a spam email campaign selling magazines to college students. During this campaign, spam emails sent by the SHAHS

were sent through a botnet into the MU computer network. Some examples include, but are not limited to the following:

- a. One email message had been routed through a computer network that technicians discovered had over one hundred viruses on it, including the w32.beagle virus. The w32.beagle virus is a mass-mailing worm that spreads through file sharing networks. This virus will forge SMTP addresses that are saved on the computer and send email messages using the forged email address; including rotating subject lines and attachment names.
- b. One spam email was sent through an ISP which serves North and South Dakota. Technicians discovered that the source computer from the ISP was infected with the w32.beagle virus, along with 47 other viruses, including a troj-agent-1. This version of the w32.beagle virus also contained a backdoor program that would notify the creator when the infected machine had been compromised and was ready to accept commands. The troj-agent-1 virus is used for sending commercial spam. The trojan downloads instructions from a pre-configured website every minute, and these instructions tell the computer what email to send and to whom.

58. In or about October of 2004, the SHAHS conducted a spam email campaign soliciting students to join their online business venture called TEXTBOOK REGISTRY. During this campaign, spam emails sent by the SHAHS were sent through a botnet into the MU computer network. One email message had actually been routed into the MU computer network from a virus-infected computer in the MU computer network (that is, one of the virus infected "bots" that was a part of the botnet was a MU computer). SpamCop.net, an Internet service used by many Internet service providers to identify sources of spam, alerted the MU network administrators that one of its machines was being used to send spam out to other computers.

59. Between on or about March 1, 2004, and on or about July 1, 2004, O. SHAH communicated numerous times by online chat with ZUCKER about obtaining proxies for sending spam email and sold proxies to ZUCKER. On March 15, 2004, ZUCKER asked O. SHAH, "Are you still in the proxy business?" O. SHAH responded, "Hey, yea im still doing the

proxies, my guy in china is managing it though.” O. SHAH and ZUCKER chatted numerous times in the following weeks and ZUCKER negotiated the price and discussed the terms and types of proxies. On May 15, 2004, ZUCKER asked, “Would it be possible to buy 40-50,000 proxy credits to get my service through my honeymoon (I will be out of the country for 8 days)?” O. SHAH responded, “Yes, it is.”

60. Between on or about May 25, 2004, and June 2, 2004, from a computer in the Western District of Missouri, O. SHAH provided ZUCKER approximately 45,000 proxies which were used to send spam email.

61. Between on or about March 1, 2004, and on or about July 1, 2004, ZUCKER sent wire transfer payments, through PayPal, to A. SHAH and O. SHAH, which were payments for lists of proxies used for sending spam email.

62. Between on or about August 1, 2004, and on or about February 23, 2005, O. SHAH communicated numerous times by online chat with ZUCKER about purchasing proxies for sending spam email and arranging payment to buy proxies from ZUCKER. ZUCKER told O. SHAH that his proxy service was \$75.00 a week and that ZUCKER could provide “1500-2500 twice a day.” ZUCKER told O. SHAH it was funny that ZUCKER was providing proxies now for O. SHAH, to which O. SHAH responded, “ha, yea well the one Im getting from our system are all used up, cause we have a few big mailers downloading them all day long.”

63. Between on or about August 1, 2004, and on or about February 23, 2005, O. SHAH paid ZUCKER for his “proxy service,” where ZUCKER would email O. SHAH lists of proxies for sending spam email. During this time period, ZUCKER sent O. SHAH approximately seventy-five email messages, to a computer in the Western District of Missouri,

each containing between 1,500 to 2,500 proxies. An example includes, but is not limited to the following:

- a. On or about December 1, 2004, ZUCKER sent out an email to himself, to which all of the other recipients were "blind-copied" or "bcc:" recipients. O. SHAH received the message. The subject read: "12_1_1 1230pm." The message read, "Hi All, for those of you using Dark Mailer, I am now separating the proxies into socks and http. If you are using DM, it imports many of the socks proxies in as http, and you won't get as many connections and the mailer won't work as well as it should . . . If you have any questions, let me know. Thanks, Paul." The message also contained approximately 1,738 proxies.

64. Between on or about August 1, 2004, and on or about February 23, 2005, A. SHAH and O. SHAH, sent wire transfer payments through Western Union and PayPal to ZUCKER. These transfers were payments for lists of proxies used for sending spam email.

65. On or about February 3, 2005, O. SHAH communicated by online chat with ZUCKER about obtaining a bulk email software program called "Dark Mailer." O. SHAH asked, "Do you know where I can get DM . . . free by any chance . . . lol." ZUCKER responded, "yeah from me. it's like super mailer but with a lot more features. hold on I'll send it to you." ZUCKER then sent an email to O. SHAH with the "Dark Mailer" program attached in a zip file.

66. On or about February 23, 2005, in the Western District of Missouri, the SHAHS possessed at least three bulk email software programs. These included Dark Mailer, Supermailer, and Group Mail.

67. Between on or about January 1, 2004, and on or about February 23, 2005, the SHAHS communicated numerous times with MING by AIM chat, regarding all aspects of their partnership, including hosting for the SHAHS and for other spammers, and setting up proxy scanners on his system and creating a business partnership to sell access to those proxies. On or about December 19, 2004, MING communicated with O. SHAH via AIM chat, and said,

“business is running as usual.” O. SHAH asked, “hosting and proxies still selling right?” MING replied, “yes, proxy selling good.” O. SHAH said, “good . . . good . . . sorry for the late payment . . . you received my wire right?” MING said, “no problem at all.” On or about January 20, 2005, O. SHAH communicated with MING via AIM chat, and told him, “sorry for the delay on the wire . . . I’ll have it tomorrow . . . I thought it was already sent.” MING said, “oh, np . . . this time when your wire reach, it may take 3 days to setup in other ISP . . . this ISP is down . . . simple as before :-). . . nothing new.” O. SHAH replied, “okay :-). . . no problem . . . im surprised, but no big deal, it was up for a long time . . . he he.”

68. In 2003, the SHAHS sent wire transfer payments to MING totaling approximately \$32,380 for web hosting services and proxy lists.

69. On or about the dates listed in the table below, A. SHAH and O. SHAH, sent wire transfer payments in the amounts listed below from U.S. Bank account number XXXXXXXXXX-4348 in the name of DIRECTPO, in the Western District of Missouri, to bank accounts in China, under the control of MING, which were payments for web hosting and proxies used in their spam email campaigns:

Paragraph Number	Date of Overt Act (On or about)	Amount of Money (approximately)
70	January 6, 2004	\$2,030
71	February 5, 2004	\$2,040
72	February 25, 2004	\$1,130
73	April 5, 2004	\$2,600
74	April 16, 2004	\$1,130
75	April 23, 2004	\$1,900
76	August 4, 2004	\$2,030

77	September 13, 2004	\$1,830
78	October 12, 2004	\$1,830
79	November 12, 2004	\$1,830
80	December 12, 2004	\$2,030
81	January 20, 2005	\$2,000
82	March 8, 2005	\$2,215
83	May 10, 2005	\$2,130
84	August 2, 2005	\$1,545
85	December 13, 2005	\$2,100
	TOTAL	\$30,370

Relaying and Retransmitting Spam From Protected Computers and Using False Claims and Misleading Information in Spam Emails

86. The spam email-related offenses charged in Count Seventeen through Count Forty-Two, regarding the relaying and retransmitting of spam from protected computers to intentionally mislead or deceive the recipients of the spam email and the Internet access services as to the origin of the spam email, were within the scope of the conspiracy and were committed by the conspirators in furtherance of the conspiracy. These offenses are alleged and incorporated into this count as overt acts.

87. In or about April of 2004, the SHAHS conducted a spam campaign selling teeth whitener kits to college students. During this campaign, the SHAHS used false information in their spam email and in the registration of their domain names to avoid being detected as the source of the spam email, and to avoid being contacted by upset spam email recipients. On or about April 6, 2004, A. SHAH was communicating with an upset spam email recipient via chat through one of the SHAH websites, and asked O. SHAH via AIM, "some guy wants our mailing

address . . . what should I say?" O. SHAH replied, "haha" A. SHAH said the guy wants the address "to file a claim." O. SHAH replied, "okay . . . tell him to use the contact form . . . haha . . . or you can give him our bogus address if you want which is 2227 Commerce Street–Suite 101, New York, New York, 10014." A. SHAH said, "he says, I'm going to go down to the courthouse . . . haha" O. SHAH replied, "well give him the whole campus representative ask him what school he is at . . . say you are the second to complain from that school . . . we are having problems with a campus rep there."

88. In or about October of 2004, the SHAHS conducted a spam email campaign soliciting students to join the website they designed to run a textbook buy-back business called TEXTBOOK REGISTRY. During this campaign, the SHAHS used very specific language designed to confuse students by implying an association with the university or college the students attended. On or about October 11, 2004, O. SHAH communicated via AIM chat with A. SHAH, and told him, "well I sent 50,000, about 26,000 delivered, not that bad I guess . . . 6 so far." A. SHAH replied, "haha . . . great . . . so we should expect maybe 50 people total out of 400k emails." O. SHAH said, "im just trying to see which email is best . . . then I will blast." Later that day, O. SHAH said, "we CAN get as many kids as we need . . . it may require sending more emails, but whatever . . . once again, we can mail it all again next semester to get more kids if we want." A. SHAH replied, "we I really just want to con these kids into doing it." O. SHAH said, "we need to express more urgency I think . . . that is always the key and the emails we sent don't express this urgency really." A. SHAH replied, "well I know." O. SHAH said, "I mean we could always email everyone again . . . like in 2 days from these first schools with urgency . . . so no big deal." A. SHAH said, "right . . . well we were going to purge the list and then email those

kids that didn't sign up . . . telling them that they didn't sign up." O. SHAH said, "yea . . . that's fine."

89. Later that same day, on or about October 11, 2004, the SHAHS continued to discuss via AIM how to best confuse college students into subscribing to their website. O. SHAH said, "I mean we have like 20 people signed up, they obviously looked at the site, and it is just funny . . . we conned them." A. SHAH said, "aww." O. SHAH said, "I think I should just send it all . . . haha . . . 700,000 everyday." A. SHAH replied, "we need to see just how good we can target . . . get an entire school . . . including the IT guys . . . to sign up . . . haha." Later that same day, O. SHAH said, "I was worried that no one would signup . . . lol . . . we have conned 29 people now . . . ha." O. SHAH also told A. SHAH, "we will get the kids . . . no worries . . . we just have to mail more . . . and remail . . . and remail . . . lol . . . alright well im gonna get out of my class, I will mail more later at my next class."

90. Later that same day, on or about October 11, 2004, A. SHAH began to lose hope that their TEXTBOOK REGISTRY campaign was going to work. A. SHAH told O. SHAH via AIM chat, "forget it." O. SHAH replied, "we'll get plenty of kids and books, we will just mail as much as we need." A. SHAH said, "let's just do teeth whitening." O. SHAH said, "I mean if we need to mail a million or two to get 10,000 kids . . . then so be it . . . who cares." A. SHAH said, "don't give me that . . . 50% return rate . . . no excuses." O. SHAH replied, "well we have to write better emails then . . . more forceful . . . we should say it is mandatory." A. SHAH said, "say that your account has still be verified and you will be unable to sell your books back without this account." O. SHAH replied, "alright well then thats what we will do . . . ha."

91. Later that same day, on or about October 11, 2004, the SHAHS were reviewing the results of their “test” campaign for the TEXTBOOK REGISTRY website, and reviewing which email got the most “hits” on their website from students. O. SHAH told A. SHAH via AIM chat, “well I have a ways to go, but im going to mail 400k today . . . I think the forceful one will get them way better.” O. SHAH continued, “bottom line . . . we will get kids . . . Im gonna have to force it.” A. SHAH replied, “force away . . . scare the bitches.”

92. During the SHAHS’ spam campaigns, the defendants would falsely claim that the business whose product they were selling was “alumni-owned” to increase sales. These same emails purporting to offer “alumni-owned” products were sent to the full list of universities and colleges. Some examples include, but are not limited to:

- a. On or about April 1, 2004, one of the defendants’ spam emails read, “Each year, several alumni-owned companies offer various specials to our students and faculty. This month, the university has been offered a special discount on custom fitted teeth whitening systems. Alumni-owned, Custom Bright, Inc., is offering its products to students and faculty at significant discounts all this month. We encourage you to visit their website and take advantage of this alumni offer.”
- b. On or about April 2, 2005, one of the defendants’ spam emails read, “Each year, several alumni-owned companies offer various specials to our students and faculty. This month, the university has been offered a special discount on custom fitted teeth whitening systems. Alumni-owned, Simple Bright, is offering its products to students and faculty at significant discounts all this month.”
- c. On or about March 15, 2008, one of the defendants’ spam emails read, “I wanted to take a moment to remind you of this month’s campus-wide alumni discount. A generous quantity of professional teeth whitening systems has been delivered to campus representatives (like myself) for distribution.”
- d. On or about March 1, 2009, one of the defendants’ spam emails read, “As many of you may be aware, our campus has been offered a special discount on professional custom-fitted teeth whitening systems from a company run by our very own alumni. There will be several campus representatives (like myself) giving out more information over the next 2 weeks.”

93. During the SHAHS' spam campaigns, the defendants would also falsely imply that the business or service they were offering was sponsored or sanctioned by the university or college of the student receiving the spam, when they were not. Some examples include, but are not limited to:

- a. On or about October 15, 2004, one of the defendants' spam emails read, "With higher tuition and course material costs, we are working hard to find new ways of saving students money. This semester, we have implemented a new textbook buyback program that will get students better payouts at the semester ending buyback and may also increase used textbook availability. You MUST complete your registration before the end of this week if you wish to be eligible for this semester's buyback."
- b. On or about May 11, 2004, one of the defendants' spam emails read, "Each year we work with a particular company to offer university students a great gift for semester's end. The majority of students surveyed on campus have said that a portable MP3 player is one thing they have thought about buying for a long time. At your request, we are now working with Campus MP3 to provide great MP3 players to students, faculty, friends, and family."
- c. On or about February 15, 2008, one of the defendants' spam emails read, "Earlier this year, we received many requests to create a new web system that would allow students to better interact with their peers and professors. We have since moved forward with this project and are pleased to deliver some new features very soon."

94. On February 23, 2005, federal search warrants were executed on the SHAHS' residence at 1301 Fieldcrest, Columbia, Missouri, and at the SHAHS' business address of 1711 Parris Road, Columbia, Missouri. After these search warrants were executed, the SHAHS modified their scheme to continue sending their spam emails to college students.

95. In or about February of 2005, the SHAHS removed the email addresses of MU students from their database of student emails. The SHAHS did not send spam emails into MU, nor did they send spam email from the MU's campus anymore. The SHAHS did this to avoid further problems from MU, which had identified them as the source of the spam email to law

enforcement. Other than removing the MU students' email addresses from their list, the SHAHS continued to send spam emails to all the colleges and universities that they had previously.

96. Beginning in or before 2007, and continuing thereafter on the dates specified in the table below, the SHAHS modified their scheme further, and paid for the registration of numerous domain names for each spam email campaign, each pointing to an identical website selling their products. The SHAHS also spread the hosting and mailing services for each of these domains between numerous separate web hosting companies, in order to conceal their identities, mislead recipients and Internet service providers as to the source of the email, and to penetrate spam filters:

Paragraph Number	Date(s) of Overt Act(s)	Campaign	Number of Domains Registered (at least)	Sample Domain Names Used
97	On or about February 1, 2007	Noog.com	6	surveyproject.org surveydirect.org campuschange.org
98	On or about February 16, 2007	Teeth Whiteners	10	whiteningtoday.com whiteningnow.com discoverwhitening.com
99	Between April 11, 2007 and April 15, 2007	Ipods	24	myschoolipods.com studentipods.com campusipods.com
100	Between August 14, 2007 and September 28, 2007	Magazines	62	semestersavings.com semesterdiscounts.com saveatcollege.com
101	Between November 12, 2007 and November 19, 2007	Digital Cameras	45	collegedecember.com estudentoffers.com mycollegedeals.com

Paragraph Number	Date(s) of Overt Act(s)	Campaign	Number of Domains Registered (at least)	Sample Domain Names Used
102	Between January 22, 2008 and January 24, 2008	Noog.com	46	collegefuture.com campusfuture.com campusinput.com
103	On or about February 17, 2008	Teeth Whiteners	16	whiteningservices.com whiteningovernight.com whiteninglabs.com
104	Between April 14, 2008, and April 22, 2008	Ipods	39	mycampusnanos.com campusnanos.com schoolipods.com
105	Between August 14, 2008 and September 9, 2008	Magazines	53	collegetitle.com universitymagazines.com campusnewstand.com
106	Between September 26, 2008 and November 13, 2008	Noog.com	36	campustogether.com campusunite.com collegetogether.com
107	Between November 24, 2008 and December 1, 2008	Digital Cameras	64	giftsforcampus.com giftsoncampus.com holidayatcollege.com
108	Between February 3, 2009 and April 12, 2009	Noog.com	43	campusassist.com campusfavor.com campusfavortrade.com
109	Between February 5, 2009 and April 12, 2009	Teeth Whiteners	77	schoolwhitening.com collegewhite.com campuswhite.com

110. During the SHAHS' spam campaigns, the SHAHS would also use dozens of different subject lines per campaign. This allowed the SHAHS to rotate the subject lines so that the messages would appear to spam filters to be different. For example, during the SHAH

magazine campaign from September 2008 to November 2008, the SHAHS used at least 56 different subject lines, including but not limited to:

Sample Subject Lines from 2008 Magazine Campaign		
2008-2009 Subscriptions	Fall Semester Welcome	Subscription News
1 st Semester Notice	Important 1 st Semester Notice	Subscription Update
Academic Discount Available	Important Reading Material Discount	Welcome Back Discount
Annual Subscription Reminder	Important Reading Material Information	Fall Reminder
ATTN: Campus Offer	Important Reading Material Notice	Student Reminder
ATTN: Fall Semester Discount	Important Reading Material Reminder	Reading Material Information
ATTN: Students & Faculty	Important Semester Information	Magazine Gift Code
Campus Discount Notice	LAST NOTICE: Student Offer Ending	Campus Offer Ending
Campus Discount Reminder	Magazine Discount Reminder	Subscription Offer Ending
Campus Gift Code	Magazine Special	Campus Offer Ending Soon
Campus Magazine Subscriptions	FINAL REMINDER: Educational Discount	Reading Material Notice
Campus Notice	Educational Discount Ending	Reading Material Reminder
Campus Reminder	LAST NOTICE: Subscription Offer Ending	School Year Reminder
Campus Subscription Reminder	Semester Discount Information	Last Discount Reminder
Educational Discount Available	Student Discount Ending	Campus Discount Ending
Educational Discount Notice	Student Subscription Reminder	Last Chance Notice

Fall Notice	Subscription Discount Reminder	Subscription Gift Code
Fall Notification	Discount Code Expiration Notice	Subscription Information
Fall Semester Notice	FINAL REMINDER: Campus Discount	

111. Putting all of these elements together, the SHAHS' spam campaigns used false and misleading language, and rotated subject line, content, URLs, and reply addresses within the same campaign, in order to penetrate university spam filters. Each of the different domain names contained in the spam emails would direct the spam recipient to identical websites for the defendants' product or service (in the below examples, Noog.com).

- a. The following three messages are all examples of spam emails sent during the 2008 Noog.com campaign from October to November, in which the SHAHS were soliciting students to join Noog.com:

On or about	Subject Line	Content	URL
10/09/08	New Campus Communication Tool	We have implemented a new online instant messenger and course note sharing system for the 2008-2009 school year. This new initiative has been headed up by StudyResource.org; its goal is to help our students meet their fellow classmates and exchange information.	StudyResource.org
10/10/08	Student Network Registration	We have implemented a new online account for students to instant message and share question/answer sessions with their classmates. If your professors have not already given you activation information for your account, please visit the link below. We hope to have students registered by the end of next week.	Collegecollaborate.org

10/10/08	Online Account Registration	We recently implemented new online accounts for student-to-student instant messaging and course collaboration. Your account allows you to add your classes to the system and chat/share with your classmates. We are registering users through StudySimple.org that will be linked via your school email address. Please take time to activate your account and add your course schedule to the system.	Studysimple.org
----------	-----------------------------	---	-----------------

- b. The following three messages are all examples of spam emails sent during the 2009 Noog.com campaign from February to April, in which the SHAHS were soliciting students to join Noog.com:

On or about	Subject Line	Content	URL
02/23/09	New Student Tool	As you may be aware, students are being encouraged to join our new online campus portal designed to help our students better interact with their classmates! By adding your classes to this system you can instantly become connected with classmates and other students with the same major. The purpose of this free service is to allow students to give/receive help from other students on their campus. We are pushing everyone to join in order to make this tool more useful to everyone.	Campusfavor.com

02/24/09	Campus Network Forming	In a nationwide attempt to create an interactive student community, several campuses have teamed up to create deedMate.com. This new online platform was designed to help students network/meet other students while doing simple favors for each other. This is a great tool that can be used to get tutoring, suggestions, and academic advice from your peers. As a service to our students, we encourage you to sign in and utilize it to offer/receive help from your fellow students. It's a great way to meet new people on campus!	deedMate.com
02/24/09	Student System	We have been working on adding new web technologies to help our students meet, interact, and study with each other. Our latest tool was created by studentkindness.com; it allows students to post questions, answers, and offer their services to each other. The goal is to get our students to help each other out! This online platform is now live for our campus.	Studentkindness.com

Creation of Noog.com and Spamming to Gain Subscribers to the Website

112. In or about December of 2006, A. SHAH traveled to Pakistan to meet with "MANAGER 1" to create an overseas office for I20, INC. called "VISTACLICK PAKISTAN," where the SHAHS and "MANAGER 1" hired two additional employees to work for I20, INC. full-time. The SHAHS have since hired additional employees for their VISTACLICK PAKISTAN office.

113. On or about the dates listed in the table below, A. SHAH and O. SHAH caused and directed the transfer of the money from U.S. Bank account XXXXXXXXX-4348 in the name

of DIRECTPO, in the Western District of Missouri, to a bank account in Pakistan under the name and control of VISTACLICK PAKISTAN or "MANAGER 1," in the amounts listed below:

Paragraph Number	Date of Overt Act (On or about)	Amount of Money (approximately)
114	March 21, 2008	\$9,000
115	May 12, 2008	\$9,000
116	June 30, 2008	\$12,000
117	September 4, 2008	\$9,000
118	October 28, 2008	\$9,000
119	December 19, 2008	\$12,000
	TOTAL	\$60,000

120. In or before 2007, the SHAHS caused and directed the creation of the website NOOG.COM. The SHAHS marketed NOOG.COM as a "social utility site." The SHAHS designed it to be similar to platforms such as Facebook and MySpace, but only open to college students. The SHAHS claimed it would be a "hybrid of social networking and academic services." The SHAHS directed and controlled the operation of NOOG.COM from their residences 1301 Fieldcrest, Columbia, Missouri, and 1520 Washington Avenue, Unit #301, St. Louis, Missouri. The SHAHS have also used 746 Spring Hill Farm Drive, Ballwin, St. Louis, Missouri, for the administration and operation of NOOG.COM.

121. In or before July of 2007, the SHAHS purchased, with funds from U.S. Bank account XXXXXXXXX-4348 in the name of DIRECTPO, in the Western District of Missouri, computer equipment to build their own servers to host NOOG.COM.

122. Between on or about July 30, 2007, and December 4, 2008, the SHAHS paid CyberCon.com, located at 210 N. Tucker, Suite 700, St. Louis, Missouri, with funds from

U.S. Bank account XXXXXXXXX-4348 in the name of DIRECTPO, in the Western District of Missouri, for hosting and Internet connectivity services for NOOG.COM.

123. The SHAHS asked "PROGRAMMER 1" to modify his email extractor program "Reflex" to work as a data extractor for NOOG.COM. The SHAHS asked "PROGRAMMER 1" to modify the extractor to collect data from other websites which offer services to college students, in order to populate NOOG.COM quickly with information. An example includes, but is not limited to:

- a. Between on or about February 13, 2008, and February 19, 2008, the SHAHS asked "PROGRAMMER 1" to modify "Reflex" to be used to harvest information from a legitimate commercial website. This legitimate website had compiled university and college class schedules, professor names, and other similar data in a user-friendly database for its users. The SHAHS wanted "PROGRAMMER 1" to modify "Reflex" to harvest or mine this data for use on NOOG.COM. This would enable the SHAHS to quickly populate NOOG.COM with all of this information, without any contractual relationship or other agreement with the legitimate commercial website, and therefore allow the SHAHS the benefit of the legitimate commercial website's work, without the hours and cost of doing it on their own.

124. The SHAHS conducted at least four separate spam campaigns, as described in Counts 31, 35, 39 and 41, designed to solicit college students to subscribe to NOOG.COM. The SHAHS were attempting to drive up the number of subscribers to NOOG.COM in order to make NOOG.COM to appear more successful in order to attract investors to NOOG.COM.

Unlawful Proceeds of Spam Campaigns

125. On or about September 29, 2004, the SHAHS communicated with each other by online chat about what to do with the proceeds of their spam campaigns. O. SHAH asked, "So how are we going to launder all the money? . . . I mean we should definitely not have this kind of money sitting there . . ." A. SHAH responded, "I agree, that's why we are putting it into home or

maybe we can put some into the muslim fund.” O. SHAH replied, “We can do that too, or we can open up a small portfolio of our own . . .” A. SHAH said, “I’d rather do other stuff . . .invest in new ideas . . . houses.” O. SHAH said, “Yea. Let’s do it then.”

126. When a student received a spam email sent by the defendants and purchased one of their products or services, the student paid by credit card online through an online processing service such as Paypal or Authorize.net. The online processing service would then deposit the proceeds directly into U.S. Bank account XXXXXXXXX-4348 in the name of DIRECTPO, in the Western District of Missouri, under the control of A. SHAH and O. SHAH.

127. The total amount of proceeds the SHAHS received from their spam campaigns, which was deposited into U.S. Bank account XXXXXXXXX-4348 in the name of DIRECTPO, in the Western District of Missouri, totaled approximately \$4,191,966.57.

128. On or about the dates listed in the table below, A. SHAH and O. SHAH caused and directed the transfer of money from U.S. Bank account XXXXXXXXX-4348 in the name of DIRECTPO, in the Western District of Missouri, to U.S. Bank account XXXXXXXXX-2816 in the name of AMIR SHAH d/b/a FUNDING JUNCTION, in the amounts listed below:

Paragraph Number	Date of Overt Act (On or about)	Amount of Money (approximately)
129	September 4, 2007	\$3,000
130	September 12, 2007	\$10,000
131	October 16, 2007	\$10,000
132	November 6, 2007	\$5,000
133	September 16, 2008	\$11,000

134	October 8, 2008	\$10,000
135	November 20, 2008	\$2,000
	TOTAL	\$51,000

136. On or about the dates listed in the table below, A. SHAH and O. SHAH caused and directed the transfer of money from U.S. Bank account XXXXXXXXXX-4348 in the name of DIRECTPO, in the Western District of Missouri, to U.S. Bank account XXXXXXXXXX-2743 in the name of AMIR A. SHAH d/b/a YOUR CITY DEVELOPMENT, in the amounts listed below:

Paragraph Number	Date of Overt Act (On or about)	Amount of Money (approximately)
137	November 27, 2006	\$20,000
138	January 2, 2007	\$10,000
139	July 11, 2007	\$6,500
140	August 17, 2007	\$3,000
141	September 26, 2007	\$3,000
	TOTAL	\$42,500

142. Between on or about December, 2002, and October, 2004, A. SHAH and O. SHAH caused and directed the payment of money from U.S. Bank account XXXXXXXXXX-4348 in the name of DIRECTPO, in the Western District of Missouri, for the residence located at 1301 Fieldcrest, Columbia, Boone County, Missouri, in the amount of approximately \$191,123, which included a final payoff which was sent via wire transfer on or about October 1, 2004 in the amount of approximately \$46,275.02.

143. Between on or about June, 2007, and November, 2008, A. SHAH and O. SHAH caused and directed the payment of money from U.S. Bank account XXXXXXXXXX-4348 in the

name of DIRECTPO, in the Western District of Missouri, for the luxury loft located at 1520 Washington Avenue, Unit #301, St. Louis, St. Louis City County, Missouri, in the amount of approximately \$251,861, which included a final payoff which was paid on or about November 19, 2008, in the amount of approximately \$182,950.81.

144. Between on or about November, 2006, and December, 2008, A. SHAH and O. SHAH caused and directed the payment of money from U.S. Bank account XXXXXXXXXX-4348 in the name of DIRECTPO, in the Western District of Missouri, for the residence located at 5417 Idaho Avenue, St. Louis, St. Louis City County, Missouri, in the amount of approximately \$33,698.42.

145. On or about January 21, 2009, A. SHAH and O. SHAH purchased a cashier's check from U.S. Bank in the amount of approximately \$8,800, with approximately \$7,000 from U.S. Bank account XXXXXXXXXX-4348 in the name of DIRECTPO and approximately \$1,800 from U.S. Bank account XXXXXXXXXX-6708 in the name of OSMAAN SHAH, in the Western District of Missouri, which was payment for a 2002 Lexus sedan, VIN #JTHBD192920050629.

146. On or about September 28, 2005, A. SHAH and O. SHAH caused a check to be issued in the amount of approximately \$24,000, from U.S. Bank account XXXXXXXXXX-4348 in the name of DIRECTPO, in the Western District of Missouri, which check was payment for a 2001 BMW four door, VIN #WBADT634X1CF07532.

147. All in violation of Title 18, United States Code, Section 371.

COUNT TWO through SIX
(Fraud in Connection with Computers - 18 U.S.C. § 1030(a)(2))

148. The General Allegations set forth in paragraphs One through Thirty-Six of this Indictment are re-alleged as if stated fully here.

149. On or about the dates listed below, within the Western District of Missouri and elsewhere, AMIR SHAH, OSMAAN SHAH, I2O INC. d/b/a DIRECTPO, d/b/a VISTACLICK, and others both known and unknown to the Grand Jury, aiding and abetting each other and others, intentionally accessed a computer without authorization and in excess of their authorization, and thereby obtained information from a protected computer, to wit: AMIR SHAH, OSMAAN SHAH, and I2O INC. d/b/a DIRECTPO, d/b/a VISTACLICK, aiding each other and others, created and used a computer program known as an email extractor to harvest student email addresses from approximately two thousand (2,000) universities and colleges in the United States, each of which is a computer involved with interstate or foreign communication;

150. It is further alleged as follows:

- a. The offense was committed in furtherance of a criminal or tortious act in violation of the Constitution or laws of the United States or of any State, that is, Fraud in Connection with Electronic Mail, in violation of 18 U.S.C. § 1037; and
- b. The offense was committed for commercial advantage or private financial gain;

Count	Year	Between on or about	and on or about
2	2004	May 1	December 1
3	2005	May 1	December 1
4	2006	May 1	December 1
5	2007	May 1	December 1
6	2008	May 1	December 1

151. All in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(i) and (ii), and Title 18, United States Code, Section 2.

COUNT SEVEN

(Fraud in Connection with Computers - 18 U.S.C. § 1030(a)(5))

152. The General Allegations set forth in paragraphs One through Thirty-Seven of this Indictment are re-alleged as if stated fully here.

153. Between on or about January 1, 2004, and on or about February 23, 2005, in the Western District of Missouri and elsewhere, AMIR SHAH, OSMAAN SHAH, I2O INC. d/b/a DIRECTPO, d/b/a VISTACLICK, LIU GUANG MING, and PAUL ZUCKER, and others both known and unknown to the Grand Jury, aiding and abetting each other and others, knowingly caused the transmission of a program, information, code and command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, to wit: AMIR SHAH, OSMAAN SHAH, I2O INC. d/b/a DIRECTPO, d/b/a VISTACLICK, LIU GUANG MING, and PAUL ZUCKER, aiding and abetting each other and others, sent out millions of spam emails through the University of Missouri computer network to college students all across the country, which is a computer used in interstate or foreign commerce or communication, and the damage to said protected computer, caused a loss of at least \$5,000 to one or more persons during any one-year period; to wit: the computer network at the University of Missouri sustained damage from:

- a. the large amount of computer network resources and bandwidth used during the defendants' transmission of millions of spam emails through its system;
- b. the substantial amount of time, money, and resources spent by the University of Missouri responding to and fixing problems caused to the University of Missouri's network and its email users by the defendants' spam email campaigns; and,
- c. the amount of time, money, and resources spent by the University of Missouri to protect and defend its network from future spam emails campaigns by the

defendants, all in addition to many other expenses to the University of Missouri and its email users.

154. All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and 1030(c)(4)(A), and Title 18, United States Code, Section 2.

COUNT EIGHT through SIXTEEN
(Fraud in Connection with Email - 18 U.S.C. § 1037(a)(1))

155. The General Allegations set forth in paragraphs One through Thirty-Seven of this Indictment are re-alleged as if stated fully here.

156. On or about the dates listed below, within the Western District of Missouri and elsewhere, AMIR SHAH, OSMAAN SHAH, I2O INC. d/b/a DIRECTPO, d/b/a VISTACLICK, LIU GUANG MING, and PAUL ZUCKER, and others known and unknown to the Grand Jury, aiding and abetting each other and others, did, in and affecting interstate and foreign commerce, knowingly access a protected computer without authorization, and intentionally initiate the transmission of multiple commercial electronic mail messages from or through such computer;

Count	Year	Month(s)	Campaign
8	2004	April	Teeth Whiteners
9	2004	May	MP3 Players/Ipods
10	2004	August - October	Magazines
11	2004	October	Textbooks
12	2004-5	December - February	Digital Cameras
13	2005	February - April	Teeth Whiteners
14	2005	May	MP3 Players/Ipods

Count	Year	Month(s)	Campaign
15	2005	August - October	Magazines
16	2005-6	November - January	Digital Cameras

157. All in violation of Title 18, United States Code, Section 1037(a)(1), punishable under Title 18, United States Code, Section 1037(b)(2)(A), and Title 18, United States Code, Section 2.

COUNT SEVENTEEN through FORTY-TWO
(Fraud in Connection with Email - 18 U.S.C. § 1037(a)(2))

158. The General Allegations set forth in paragraphs One through Thirty-Six of this Indictment are re-alleged as if stated fully here.

159. On or about the dates listed below, within the Western District of Missouri and elsewhere, AMIR SHAH, OSMAAN SHAH, and I2O INC. d/b/a DIRECTPO, d/b/a VISTACLICK, and others known and unknown to the Grand Jury, aiding and abetting each other and others, did, in and affecting interstate and foreign commerce, knowingly use, and cause others to use, a protected computer to relay and 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;

160. It is further alleged as follows:

- a. The volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24 hour period or 25,000 during any 30 day period;
- b. The offense caused loss to one or more persons aggregating \$5,000 or more in value during any 1-year period;
- c. As a result of the offense, any individual committing the offense obtained anything of value aggregating \$5,000 or more during any 1 year period.

Count	Year	Month(s)	Campaign
17	2004	April	Teeth Whiteners
18	2004	May	MP3 Players/Ipods
19	2004	August - October	Magazines
20	2004	October	Textbooks
21	2004-5	December - February	Digital Cameras
22	2005	February - April	Teeth Whiteners
23	2005	May	MP3 Players/Ipods
24	2005	August - October	Magazines
25	2005-6	November - January	Digital Cameras
26	2006	February - March	NCAA Basketball
27	2006	April - July	Teeth Whiteners
28	2006	September - November	Magazines
29	2006-7	November - January	Digital Cameras
30	2007	February	Teeth Whiteners
31	2007	February	Noog.com
32	2007	April	MP3 Players/Ipods
33	2007	August - November	Magazines
34	2007-8	November - January	Digital Cameras
35	2008	January - February	Noog.com
36	2008	January - April	Teeth Whiteners
37	2008	March - July	MP3 Players/Ipods
38	2008	August - November	Magazines
39	2008	October - November	Noog.com
40	2008-9	November - February	Digital Cameras
41	2009	February - April	Noog.com
42	2009	February - April	Teeth Whiteners

161. All in violation of Title 18, United States Code, Section 1037(a)(2), punishable under Title 18, United States Code, Section 1037(b)(2), and Title 18, United States Code, Section 2.

COUNT FORTY-THREE through FIFTY-ONE
(Fraud in Connection with Email - 18 U.S.C. § 1037(a)(3))

162. The General Allegations set forth in paragraphs One through Thirty-Seven of this Indictment are re-alleged as if stated fully here.

163. On or about the dates listed below, within the Western District of Missouri and elsewhere, AMIR SHAH, OSMAAN SHAH, I2O INC. d/b/a DIRECTPO, d/b/a VISTACLICK, LIU GUANG MING, and PAUL ZUCKER, and others known and unknown to the Grand Jury, aiding and abetting each other and others, did, in and affecting interstate and foreign commerce, knowingly and materially falsify and cause others to materially falsify header information in multiple commercial electronic mail messages, and intentionally initiate the transmission of such messages;

164. It is further alleged as follows:

- a. The volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24 hour period or 25,000 during any 30 day period;
- b. The offense caused loss to one or more persons aggregating \$5,000 or more in value during any 1-year period;
- c. As a result of the offense, any individual committing the offense obtained anything of value aggregating \$5,000 or more during any 1 year period.

Count	Year	Month(s)	Campaign
43	2004	April	Teeth Whiteners
44	2004	May	MP3 Players/Ipods

Count	Year	Month(s)	Campaign
45	2004	August - October	Magazines
46	2004	October	Textbooks
47	2004	December	Digital Cameras
48	2005	February - April	Teeth Whiteners
49	2005	May	MP3 Players/Ipods
50	2005	August - October	Magazines
51	2005-6	November - January	Digital Cameras

165. All in violation of Title 18, United States Code, Section 1037(a)(3), punishable under Title 18, United States Code, Section 1037(b)(2), and Title 18, United States Code, Section 2.

FORFEITURE ALLEGATION

166. The General Allegations set forth in paragraphs One through Thirty-Six and the allegations of Count One through Fifty-One of this Indictment are re-alleged and incorporated by reference as if stated fully here, for the purpose of alleging forfeiture pursuant to the provisions of Title 18, United States Code, Sections 1030(i) and (j), 1037(c), and Title 21, United States Code, Section 853.

167. If convicted of the offenses set forth in Counts One through Fifty-One of this Indictment, the defendants, AMIR SHAH, OSMAAN SHAH, I2O INC. d/b/a DIRECTPO, d/b/a VISTACLICK, LIU GUANG MING, and PAUL ZUCKER, shall forfeit any and all property, real or personal, constituting or traceable to gross proceeds obtained from the commission of said offense, and any equipment, software, or other technology used or intended to be used to commit

or facilitate the commission of said offense. Such property includes, but is not limited to, the following specific items:

- a. A sum of money including, but not limited to, **\$4,191,966.57** in United States currency, representing the amount of proceeds obtained as a result of the offense, for which the defendants are jointly and severally liable.

Contents of Bank Accounts

All United States currency or other monetary instruments credited to or contained in the following accounts:

- b. U.S. Bank account number XXXXXXXXX-6708 in the name of OSMAAN SHAH;
- c. U.S. Bank account number XXXXXXXXX-2816 in the name of AMIR SHAH d/b/a FUNDING JUNCTION;
- d. U.S. Bank account number XXXXXXXXX-2743 in the name of AMIR A. SHAH d/b/a YOUR CITY DEVELOPMENT;
- e. U.S. Bank account number XXXXXXXXX-9795 in the name of I2O, INC.;
- f. U.S. Bank account number XXXXXXXXX-4348 in the name of DIRECTPO;

Real Property

- g. The real property located at 1301 Fieldcrest, Columbia, Boone County, Missouri, more particularly described as:

Lot Three (3) in Block (2) of Westwood Hills Subdivision in the City of Columbia, Boone County, Missouri, as shown by the plat thereof recorded in Plat Book 7, Page 16, Records of Boone County, Missouri;

- h. The real property located at 1520 Washington Avenue, Unit #301, St. Louis, St. Louis City County, Missouri, more particularly described as:

Parcel 1:

Unit 301 of Ely Walker Condominiums in Block 832 of the City of St. Louis as shown on the Plat thereof recorded in Plat Book 05222007, Page 0259, together with an undivided share of common and limited elements and appurtenances thereto belonging and all easements including, but not limited to, parking created, all according to and more particularly

described and shown in Declaration of Condominium and By-Laws of Ely Walker Condominiums recorded in Book 05222007, Page 0258;

Parcel 2:

Parking Space No. 11 of Ely Walker Condominiums in Block 832 of the City of St. Louis as shown on the Plat thereof recorded in Plat Book 05222007, Page 0259, together with an undivided share of common and limited elements and appurtenances thereto belonging and all easements including, but not limited to, parking created, all according to and more particularly described and shown in Declaration of Condominium and By-Laws of Ely Walker Condominiums recorded in Book 05222007, Page 0258;

- i. The real property located at 5417 Idaho Avenue, St. Louis, St. Louis City County, Missouri, more particularly described as:

Lot 14 in Block 4 of VEIHL AND HUDGEN'S SUBDIVISION and in Block 2842 of the City of St. Louis, fronting 30 feet on the West line of Idaho Avenue by a depth Westwardly of 142 feet 6 inches to an alley;

Personal Property

- j. A 2002 Lexus sedan, VIN #JTHBD192920050629, bearing Missouri license plate number CA9R6B.
- k. A 2001 BMW four door, VIN #WBADT634X1CF07532, bearing Missouri license plate number 391ZEP.

Substitute Assets

168. If any of the above-described forfeitable money or property, as a result of any act or omission by the defendants:

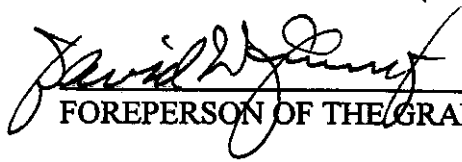
- (a) cannot be located by the exercise of due diligence;
- (b) has been transferred, sold to, or deposited with, a third party;
- (c) has been placed beyond the jurisdiction of the Court;
- (d) has been substantially diminished in value; or,

(e) has been commingled with other property that cannot be subdivided without difficulty,

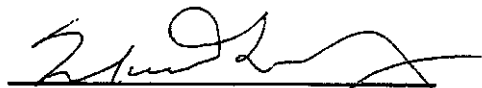
it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 1037(c), to seek forfeiture of any other property or interests of the defendants, up to the value of the forfeitable money and property described above, or to seek the return of the property to the jurisdiction of the Court so that the property may be seized and forfeited.

169. All pursuant to the provisions of Title 18, United States Code, Section 1030(i) and (j), 1037(c), and Title 21, United States Code, Section 853.

A TRUE BILL.



FOREPERSON OF THE GRAND JURY



Matthew P. Wolesky, #53253
Assistant United States Attorney

DATED: 4/23/09