UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	**CRIMINAL CASE NO.**
	:	**MAGISTRATE No. 07-00243M**
	:	
	:	
v.	:	**VIOLATIONS: 18 U.S.C. §§ 371, 1037, 2**
ADAM SWEANEY	:	**(Conspiracy, Fraud Relating to Email, Aiding and Abetting)**
Defendant.	:	

INFORMATION

At all times relevant to this Information:

INTRODUCTION

1. The Department of Justice – Antitrust Division is a division of a federal government agency that is involved in the furtherance of the administration of justice. Its computers affect interstate and foreign commerce and are used in furtherance of the administration of justice.

2. "Spam" refers to sending massive amounts of unwanted and unsolicited emails to computer users, which often offer for sale counterfeit services and products. "Proxies" refers to compromised computers that are controlled remotely by someone other than an authorized computer user. A compromised computer is one which has been infected by a malicious program or code without the knowledge or consent of the computer owner. Proxies are commonly used by those engaged in computer fraud, including spam and "phishing" – attempts to defraud consumers by getting them to interact with counterfeit email or websites that appear to be trusted and known. When thousands of proxies are linked together, they become a powerful

tool which can be utilized for criminal activity.

COUNT 1: CONSPIRACY

THE CONSPIRACY

3. From a date uncertain but from at least on or about May 8, 2006, and continuing through in or about April 27, 2007, in the District of Columbia and elsewhere, defendant SWEANEY did willfully and knowingly combine, conspire, agree, and confederate with others known and unknown to commit offenses against the United States, that is:

A. engaging in a scheme to intentionally access protected computers without authorization and in so doing, recklessly causing damage to those computers, in violation of 18 U.S.C. Section 1030(a)(5)(A)(ii);

B. accessing protected computers without authorization for the purpose of transmitting multiple commercial electronic mail messages from such computers, in violation of 18 U.S.C. Section 1037(a)(1); and

C. engaging in a scheme to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises and causing to be transmitted electronic communications in interstate or foreign commerce, in violation of 18 U.S.C. Section 1343.

THE GOAL OF THE CONSPIRACY

4. The goal of the conspiracy was for defendant SWEANEY, and others known and unknown, to enrich themselves by gaining access to compromised computers without authorization, by selling access to compromised computers, and by sending massive amounts of spam emails from the compromised computers.

MANNER AND MEANS OF THE CONSPIRACY

5. In order to achieve the goal of the conspiracy, defendant SWEANEY, along with others known and unknown, used the following manner and means, among others:

A. Defendant SWEANEY would obtain access to compromised computers, known as proxies, from others known and unknown, which could be remotely controlled by others, including those interested in anonymously sending massive amounts of unwanted spam email.

B. Defendant SWEANEY would advertise and sell his access to proxies and to email addresses. Typically, defendant SWEANEY would offer subscriptions to the proxies he had accessed, and during this time, defendant SWEANEY would establish a site from which interested parties could access the proxies and use them for any purpose. Defendant SWEANEY would charge a fee for access to his available proxies.

C. Those that purchased proxy access from defendant SWEANEY would access the compromised computers without rightful authorization or consent from the computer users. To enrich themselves, those that gained access to the compromised computers would use the compromised computers to launch massive spam mailings and for other illegal purposes, sometimes using email addresses defendant Sweaney also would make available. By utilizing these proxies, those involved in sending massive amounts of spam email could mask their identity and the origin of the spam email and could increase the likelihood that their spam email would be received by the intended recipients and would not be captured by filtering and security software.

OVERT ACTS

6. Among the overt acts committed by defendant SWEANEY and his coconspirators during and in furtherance of the conspiracy were the following:

1. On July 07, 2006, defendant SWEANEY posted a message on a website and on-line forum frequented by those involved in illegal use of spam emails. The subject line of the message read "proxy slots available." The text read "we have socks 4 proxy slots available msg for more details aim/skype:promail757 If you need some new email databases msg us. We have about anything u (sic) want!!!" A similar message had been posted by defendant SWEANEY on May 10, 2006. The subject line of that message read "peas." The text read "We have a few open slots for peas! Msg promail757 on aim/skype for samples." "Peas" in this instance is internet jargon for proxies. Aim and Skype are internet based communication platforms that allow for individuals to send instant and private messages to and from each other. Likewise, on May 08, 2006, defendant SWEANEY posted a message entitled: "50 million gi domains delivery 87% $...." The text of the post read "last month sents 50 million gi small domains, delivery 87% price $500.00 Also still have full FTP server setup with lots of data…plus updated last weekend with some fresh files/shyt… PM for more info." In this instance gi represents the internet in general. Defendant SWEANEY was offering to sell 50 million global internet addresses to any interested party for the price of $500.00 and was stating that the 50 million email addresses being sold have an 87% delivery rate.

2. On July 21, 2006 a Federal Bureau of Investigation (FBI) Special Agent, acting in an undercover capacity, contacted via instant message defendant SWEANEY about the purchase of proxies. Defendant SWEANEY responded to the undercover Agent (UCA) providing a twenty minute free trial of the proxies via a website. The UCA verified the proxies were active and purchased a week of access from defendant SWEANEY. At that time, defendant SWEANEY enabled the UCA access to the proxies via the website.

3. On August 15, 2006, the UCA again contacted defendant SWEANEY. Defendant SWEANEY advised that he was selling access to over 6000 proxies for $200 per week. Additionally, defendant SWEANEY advised the UCA that defendant SWEANEY had for sale hotmail.com email addresses at a rate of $10 per million addresses. Defendant SWEANEY indicated to the UCA that defendant SWEEANEY had approximately 18,000,000 hotmail addresses for sale. Defendant SWEANEY stated the fee for two weeks of proxy service and the hotmail.com email addresses totaled $550 rather than $580, granting a discount for two weeks of service paid at one time.

4. On August 15, 2006, the UCA purchased from defendant SWEANEY access to the proxies and the hotmail email addresses for $550. Upon receiving payment, defendant SWEANEY provided the UCA access to the proxy list and the list of hotmail email addresses. Defendant SWEANEY further stated the UCA's originating Internet Protocol Address (IPA) is required to allow him to "lock down" the server, meaning restrict access to only users permitted by defendant SWEANEY. Access to the proxies was provided to the UCA from August 15, 2006 until August 30, 2006.

5. On August 30, 2006, the UCA again contacted defendant SWEANEY, who offered to renew the UCA's subscription to access the proxies and to sell a list of approximately fourteen (14) million Yahoo! Email addresses for $540.00. The UCA purchased both proxy access and the Yahoo! Email addresses by sending a payment of $540 via PayPal to defendant SWEANEY. Upon receiving payment, defendant SWEANEY provided access to the proxy list and the list of yahoo email addresses. Access to the proxies was provided to the UCA from August 30, 2006 until September 30, 2006.

5. On February 13, 2007, the UCA again contacted defendant SWEANEY, who again offered to renew the UCA's subscription to access the proxies for $200.00 per week. On February 22, 2007 the UCA purchased two weeks of proxy access from SWEANEY. In return, defendant SWEANEY provided the UCA with access to the proxies from approximately February 23, 2007 until March 7, 2007.

6. One of the unique proxies provided to the UCA by defendant SWEANEY was assigned to a computer which is the property of the United States Government, Department of Justice - Antitrust Division, in Washington, D.C.

(Conspiracy, in violation of Title 18, United States Code, Section 371)

COUNT 2: FRAUD RELATING TO EMAIL

7. The government re-alleges paragraphs 2 and 4-6 as if fully restated.

8. From on or about a date uncertain but from at least May 8, 2006 to on or about, April 27, 2007, defendant SWEANEY did knowingly access protected computers without authorization and from such computers did intentionally initiate the transmission of more than 1,000 electronic mail messages in any 24-hour period, 1,000 email messages in any 30-day

period, or more than 10,000 electronic mail messages during a 1-year period, the access and transmission of which affected interstate and foreign commerce.

(Fraud Relating to Email, Aiding and Abetting, in violation of 18 U.S.C. Sections 1037 (a)(1), (b)(2)(A) and 2)

JEFFREY A. TAYLOR
UNITED STATES ATTORNEY
FOR THE DISTRICT OF COLUMBIA

By: _____/s/_____
G. Bradley Weinsheimer
Assistant United States Attorney
555 4th St., N.W.
Washington, D.C. 20530
(202) 514-6991
Bar No. 431796