CR 11-177 ADM/JJG

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

UNITED STATES OF AMERICA, Plaintiff, v. (1) PETERIS SAHUROVS, a/k/a "Piotrek," a/k/a "Sagade," and (2) MARINA MASLOBOJEVA, a/k/a "Marina Sahurova," a/k/a "Aminasah," Defendants.	)	**INDICTMENT** (18 U.S.C. § 1030(a)(5)(A)) (18 U.S.C. § 1343) (18 U.S.C. § 1349) (18 U.S.C. § 2)

THE UNITED STATES GRAND JURY CHARGES:

1. From in or about February 2010 through at least in or about September 2010, in the State and District of Minnesota and elsewhere, the defendants,

PETERIS SAHUROVS,
a/k/a "Piotrek,"
a/k/a "Sagade," and
MARINA MASLOBOJEVA,
a/k/a "Marina Sahurova,"
a/k/a "Aminasah,"

each aiding and abetting one another, and being aided and abetted by one another, together with others known and unknown to the grand jury, devised, intended to devise, and participated in a scheme to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, promises, and material omissions, as more fully described below.

8

PURPOSE OF THE SCHEME

2. Defendants PETERIS SAHUROVS and MARINA MASLOBOJEVA, and others acting in concert with them or at their direction, defrauded victim Internet users by (i) infecting their computers with malicious software ("malware") which caused the victim Internet users' computers to slow down or freeze up, and then (ii) deceiving victim Internet users into purchasing purported antivirus software products to fix the problems created by the malware the defendants caused to be installed.

MANNER AND MEANS OF THE SCHEME

3. Defendants PETERIS SAHUROVS and MARINA MASLOBOJEVA, and others acting in concert with them or at their direction, created fictitious advertising agencies which in turn contacted victim companies purporting to represent legitimate third-party entities that sought to place Internet-based advertisements on the victim companies' websites, when in fact the advertisements were not authorized by the third-party entities.

4. It was further part of the scheme that, through the fictitious advertising agencies, defendants PETERIS SAHUROVS and MARINA MASLOBOJEVA, and others acting in concert with them or at their direction, caused to be placed on the websites of the victim companies Internet-based advertisements that, unbeknownst to the victim companies, contained computer code which, in turn, caused

the Internet browsers of victim Internet users who visited the victim companies' websites to be "hijacked" or redirected without their consent to websites controlled by defendants PETERIS SAHUROVS and MARINA MASLOBOJEVA, and others acting in concert with them or at their direction.

5. It was further part of the scheme that, after being redirected to a website controlled by defendants PETERIS SAHUROVS and MARINA MASLOBOJEVA, and others acting in concert with them or at their direction, the victim Internet user was prompted with a series of materially false "security alert" messages which claimed that the user's computer had been infected with malware and that the victim Internet user needed to purchase an antivirus product to fix the "security issue."

6. It was further part of the scheme that, through the series of materially false "security alert" messages, defendants PETERIS SAHUROVS and MARINA MASLOBOJEVA, and others acting in concert with them or at their direction, caused victim Internet users in countries throughout the world, including the United States, to purchase software products distributed by defendants PETERIS SAHUROVS and MARINA MASLOBOJEVA, and others acting in concert with them or at their direction, including "Antivirus Soft" to purportedly fix the problems caused by the malware. As a result

of the scheme, victim Internet users were defrauded out of more than $2,000,000.00.

7. It was further part of the scheme that defendants PETERIS SAHUROVS and MARINA MASLOBOJEVA, and others acting in concert with them or at their direction, intentionally failed to pay the victim companies the fees promised by the fictitious advertising agencies for the placement of Internet-based advertisements on the victim companies' websites. As a result of the scheme, victim companies sustained losses in the form of the non-payment of fees for advertising space on the victim companies' websites.

THE STAR TRIBUNE MALWARE ATTACK

8. One of the victim companies defrauded by defendants as part of the fraud scheme described above was the Minneapolis Star Tribune ("Star Tribune").

9. At all times relevant to this indictment, startribune.com was an Internet web site owned and operated by the Star Tribune, Minnesota's largest newspaper. Much of the content found in the Star Tribune's daily newspaper can also be found on the startribune.com web site. The computer servers hosting startribune.com are located in the United States.

10. The Star Tribune obtains their online advertisements for startribune.com from three categories, one of which is referred to as "third party ad tags." For this type of advertisement, the

Star Tribune is typically contacted by an online advertising agency which represents a business or individual that wishes to advertise online. Such advertising agencies coordinate the details of the advertisement with online publishers like the Star Tribune. There are thousands of online advertising agencies throughout the country.

11. On or about February 17, 2010, defendants PETERIS SAHUROVS and MARINA MASLOBOJEVA, or others acting in concert with them or at their direction, sent an email to the Star Tribune in Minneapolis, Minnesota, purporting to be from "Lisa Polowski" (hereinafter "Polowski"), who claimed to be the Senior Media Buyer for "RevolTech Marketing" (hereinafter "RevolTech"), of Miami, Florida. The email indicated that RevolTech was an advertising agency representing Best Western International ("Best Western"), and that the agency wanted to place online ads for Best Western on startribune.com. In truth and in fact, RevolTech is not a real advertising agency and Best Western had not retained RevolTech to place online advertisements on its behalf.

12. On or about February 19, 2010, defendants PETERIS SAHUROVS and MARINA MASLOBOJEVA, or others acting in concert with them or at their direction, sent to startribune.com the "ad-tag" for the online advertisement for the purported Best Western advertising campaign. An ad-tag is a short computer file that is

placed on a web page that redirects the users' web browser to another Internet site to download content. This download happens without any user interaction.

13. The Star Tribune began running the Best Western ad-tag on startribune.com on or about February 19, 2010. Visitors to startribune.com were redirected by the ad-tag to a web server in the Netherlands controlled by defendants PETERIS SAHUROVS and MARINA MASLOBOJEVA, or others acting in concert with them or at their direction. Initially, the web server in the Netherlands downloaded only an image containing the purported Best Western advertisement. On or about February 21, 2010, unbeknownst to startribune.com or visitors to the website, the web server in the Netherlands redirected visitors' web browsers to a different web server in Latvia, which began downloading malware onto the visitors' computers.

14. On or about February 21, and continuing through February 22, 2010, visitors to the startribune.com website began experiencing slow system performance, unwanted pop-ups, and total system failure. When the Star Tribune learned of the problems experienced by visitors to startribune.com, it pulled all the online advertising from the website and later determined that the source of the infections was the advertisement provided by RevolTech. The Star Tribune immediately reported the incident to

law enforcement and also published articles in both its print and online newspapers to notify its readers of the virus-infected advertisement.

15. Before the Best Western ad-tag was removed, visitors to the startribune.com website began receiving pop-ups containing a fraudulent "Windows Security Alert," originating from a web server controlled by defendants PETERIS SAHUROVS and MARINA MASLOBOJEVA, or others acting in concert with them or at their direction. The "Windows Security Alert" read:

> Windows reports that computer is infected. Antivirus software helps to protect your computer against viruses and other security threats. Click here for the scan you computer [sic]. Your system might be at risk now.

Thereafter, additional pop-ups appeared on the victim users' computer screens, indicating that they needed to purchase the "Antivirus Soft" computer program for $49.95 to fix the "security issue." To purchase "Antivirus Soft," the victim users clicked on an option on one of the pop-ups to "upgrade the 'anti-virus'" program. Victim users who clicked on this option were presented with an online order form from a web server, "avgroupwebsite.com," where Antivirus Soft could be purchased. The web server "avgroupwebsite.com" was located in Latvia and controlled by defendants PETERIS SAHUROVS and MARINA MASLOBOJEVA, or others acting in concert with them or at their direction. Victim users were instructed to provide their credit card numbers in payment for

"Antivirus Soft." Payments were processed by a bank in Latvia controlled by defendants PETERIS SAHUROVS and MARINA MASLOBOJEVA, or others acting in concert with them or at their direction.

16. Victim computer users who did not purchase "Antivirus Soft" immediately became inundated with pop-ups containing fraudulent "security alerts" from a web server controlled by defendants PETERIS SAHUROVS and MARINA MASLOBOJEVA, or others acting in concert with them or at their direction. All information, data, and files stored on the computer became inaccessible.

17. Victim computer users who paid the defendants $49.95 received a download of the "Antivirus Soft" program which "unfroze" their computer and stopped the pop-ups and security notifications. Victim computer users had to either pay $49.95 to defendants PETERIS SAHUROVS and MARINA MASLOBOJEVA, or others acting in concert with them or at their direction, or over-write the computer hard-drive and lose all applications and data.

COUNT ONE
(Wire Fraud)

18. The Grand Jury hereby realleges and incorporates paragraphs 1 through 17 of this Indictment as if stated in full herein.

19. On or about February 19, 2010, in the State and District of Minnesota and elsewhere, the defendants,

PETERIS SAHUROVS,
a/k/a "Piotrek,"
a/k/a "Sagade," and
MARINA MASLOBOJEVA,
a/k/a "Marina Sahurova,"
a/k/a "Aminasah,"

each aiding and abetting one another, and being aided and abetted by one another, together with others known and unknown to the grand jury, for the purpose of executing the aforesaid scheme and attempting to do so, did knowingly cause to be transmitted in interstate and foreign commerce from the Netherlands to Minnesota by means of wire and radio communications, certain writings, signs, signals and sounds; to wit: an electronic mail communication to startribune.com in order to place an Internet-based advertisement containing malicious computer code on the website of startribune.com; in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT TWO
(Wire Fraud)

20. The Grand Jury hereby realleges and incorporates paragraphs 1 through 17 of this Indictment as if stated in full herein.

21. On or about February 21, 2010, in the State and District of Minnesota and elsewhere, the defendants,

PETERIS SAHUROVS,
a/k/a "Piotrek,"
a/k/a "Sagade," and
MARINA MASLOBOJEVA,
a/k/a "Marina Sahurova,"
a/k/a "Aminasah,"

each aiding and abetting one another, and being aided and abetted by one another, together with others known and unknown to the grand jury, for the purpose of executing the aforesaid scheme and attempting to do so, did knowingly cause to be transmitted in interstate and foreign commerce from Latvia to Minnesota by means of wire and radio communications, certain writings, signs, signals and sounds; to wit: an electronic communication that included an Internet advertisement containing malicious code through which defendants intentionally caused impairment to the computer of Victim A, a visitor to the startribune.com website; in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT THREE
(Conspiracy to Commit Wire Fraud)

22. The Grand Jury hereby realleges and incorporates paragraphs 1 through 21 of this Indictment as if stated in full herein.

23. From in or about February 2010 through in or about September 2010, in the State and District of Minnesota and elsewhere, the defendants,

PETERIS SAHUROVS,
a/k/a "Piotrek,"
a/k/a "Sagade," and
MARINA MASLOBOJEVA,
a/k/a "Marina Sahurova,"
a/k/a "Aminasah,"

along with others known and unknown to the grand jury, did knowingly and willfully combine, conspire, and agree with each other, and other persons known and unknown to the Grand Jury, to commit offenses against the United States, including executing a scheme to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, promises, and material omissions, as set forth above in paragraphs 2 through 17, in interstate commerce, by means of wire communication, certain signals and sounds, in violation of Title 18, United States Code, Section 1343; all in violation of Title 18, United States Code, Section 1349.

COUNT FOUR
(Unauthorized Access to a Protected Computer)

24. The Grand Jury hereby realleges and incorporates paragraphs 1 through 23 of this Indictment as if stated in full herein.

25. In or about February 21, 2010, in the State and District of Minnesota and elsewhere, the defendants,

PETERIS SAHUROVS,
a/k/a "Piotrek,"
a/k/a "Sagade," and
MARINA MASLOBOJEVA,
a/k/a "Marina Sahurova,"
a/k/a "Aminasah,"

each aiding and abetting one another, and being aided and abetted by one another, together with others known and unknown to the grand jury, did knowingly cause the transmissions of programs, information, codes, and commands, from Latvia to Minnesota; to wit: an electronic communication to startribune.com that included an Internet advertisement containing malicious code through which defendants intentionally caused impairment to the integrity and availability of data, programs, systems, and information on the startribune.com website without startribune.com's authorization by "hijacking" or redirecting the visitors to startribune.com's website away from the intended content of startribune.com's website to a web server controlled by defendants, or others acting in concert with them or at their direction, and as a result of such conduct, intentionally caused damage, without authorization, to protected computers, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

FORFEITURE ALLEGATIONS

26. The allegations in Counts 1, 2 and 3 are hereby realleged as if fully stated herein for the purpose of alleging forfeitures pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461.

27. As the result of the offense alleged in Counts 1, 2 and 3 of this Indictment, the defendants,

PETERIS SAHUROVS,
a/k/a "Piotrek,"
a/k/a "Sagade," and
MARINA MASLOBOJEVA,
a/k/a "Marina Sahurova,"
a/k/a "Aminasah,"

shall forfeit to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(C), any property constituting, and derived from, proceeds they obtained directly or indirectly as the result of such violations.

28. The allegations in Count 4 are hereby realleged as if fully stated herein for the purposes of alleging forfeitures pursuant to 18 U.S.C. §§ 982(a)(2)(B), 1030(i), and 1030(j).

29. As the result of the offense alleged in Count 4 of this Indictment, the defendants shall forfeit any and all property constituting or traceable to proceeds obtained directly or indirectly as a result of such violation, as well as any personal property that was used or intended to be used to commit or to facilitate the commission of such violation.

30. If any of the above-described forfeitable property is unavailable for forfeiture, the United States intends to seek the forfeiture of substitute property as provided for in Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

A TRUE BILL

UNITED STATES ATTORNEY

FOREPERSON

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu