U. S. Department of Justice

United States Attorney
Northern District of Illinois

Patrick J. Fitzgerald
United States Attorney

Federal Building
219 South Dearborn Street, Fifth Floor
Chicago, Illinois 60604
(312) 353-5300

FOR IMMEDIATE RELEASE
THURSDAY MAY 27, 2010
www.usdoj.gov/usao/iln

PRESS CONTACTS:
AUSA Michael Ferrara (312)886-7649
AUSA William Ridgway (312)469-6233
Randall Samborn (312)353-5318

U.S. INDICTS OHIO MAN AND TWO FOREIGN RESIDENTS IN ALLEGED UKRAINE-BASED "SCAREWARE" FRAUD SCHEME THAT CAUSED $100 MILLION IN LOSSES TO INTERNET VICTIMS WORLDWIDE

CHICAGO — An international cybercrime scheme caused internet users in more than 60 countries to purchase more than one million bogus software products, causing victims to lose more than $100 million, according to a federal indictment returned here against a Cincinnati area man and two other men believed to be living abroad. The charges allege that the defendants, through fake advertisements placed on various legitimate companies' websites, deceived internet users into falsely believing that their computers were infected with "malware" or had other critical errors to induce them to purchase "scareware" software products that had limited or no ability to remedy the purported, but nonexistent, defects. The alleged scheme is widely regarded as one of the fastest-growing and most prevalent types of internet fraud.

Two defendants, **Bjorn Daniel Sundin**, and **Shaileshkumar P. Jain**, with others owned and operated Innovative Marketing, Inc. (IM), a company registered in Belize that purported to sell anti-virus and computer performance/repair software through the internet and that operated a subsidiary called Innovative Marketing Ukraine, located in Kiev. The company appeared to close down last

year after the U.S. Federal Trade Commission filed a federal lawsuit in Maryland seeking to end the allegedly fraudulent practices.

Jain, 40, who performed the functions of IM's chief executive officer, is a U.S. citizen and is believed to be living in Ukraine. Sundin, 31, who performed the duties of IM's chief technology officer and chief operating officer, is a Swedish citizen and is believed to be in Sweden.

The third defendant, **James Reno**, 26, of Amelia, Ohio, with others owned and operated the former Byte Hosting Internet Services, which operated call centers that provided technical and billing support to victim consumers on behalf of IM. Reno is expected to present himself for arraignment at a later date in U.S. District Court in Chicago.

Sundin and Jain were each charged with 24 counts of wire fraud, and Reno with 12 counts of wire fraud, and all three were charged with one count each of conspiracy to commit computer fraud and computer fraud in a 26-count indictment returned yesterday by a federal grand jury in Chicago. The indictment also seeks forfeiture of approximately $100 million and any and all funds held in a bank account in Kiev.

The charges were announced by Patrick J. Fitzgerald, United States Attorney for the Northern District of Illinois, and Robert D. Grant, Special Agent-in-Charge of the Chicago Office of the Federal Bureau of Investigation, which conducted the global investigation. The Justice Department's Office of International Affairs and the Computer Crimes and Intellectual Property Section assisted in the investigation.

"These defendants allegedly preyed on innocent computer users, exploiting their fraudulently induced fears for personal gain. We will continue our efforts to identify and aggressively investigate similar schemes with the assistance of our law enforcement partners both at home and internationally," Mr. Grant said.

According to the indictment, after causing a series of false error messages, Sudin, Jain and others caused internet users worldwide, including throughout the United States, Sweden and Ukraine, to purchase software products bearing such names as "DriveCleaner" and "ErrorSafe," ranging in price from approximately $30 to $70, which they falsely represented would rid the victims' computers of purported defects, but actually did little or nothing to improve or repair computer performance, resulting in financial losses exceeding $100 million.

Sundin, Jain and others allegedly created at least seven fictitious advertising agencies that contacted multiple victim companies purporting to act as advertising brokers on behalf of known legitimate entities that wanted to place internet ads on the unnamed victim companies' websites, when in fact the ads were unauthorized. The victim companies allegedly were defrauded of at least $85,000 in unpaid fees promised by the fictitious ad agencies.

Unknown to the victim companies, the internet ads that were placed on their websites by these fictitious agencies contained hidden computer code that "hijacked" the internet browsers of individual victims, redirecting their computers without their consent to websites controlled by Sudin, Jain and others, the indictment alleges. The individual victims were then prompted with a series of error messages claiming that the user's computer was experiencing a critical error and the victim needed to purchase an IM-distributed software product to remedy the problem.

Reno allegedly aided and abetted Sudin, Jain and others in creating and operating the fictitious ad agencies by providing support as a technical adviser for the computer servers and networks used to facilitate their operation. The fictitious ad agencies included "BurnAds," "UniqAds," "Infyte," "NetMediaGroup," and "ForceUp," according to the indictment.

After the defendants caused a victim to be directed to an IM scareware website they controlled, the indictment alleges that the following events typically occurred:

- the IM scareware site appeared not to be a website at all, but rather a warning message from the computer user's operating system, falsely informing the user of an error and prompting the user to click on a box to address the purported error. Further error message prompts occurred regardless of whether the user clicked the box agreeing to or declining to proceed or attempted to close the error message window;

- the IM scareware displayed an animated graphic image that gave the fake appearance that the computer was being scanned for various errors or viruses. Bogus results falsely showed that critical errors were detected by the fake scan; and

- the IM scareware website then prompted the victim user to download a free trial version of an IM product, falsely promising that the software could repair the nonexistent critical errors.

As a result of the browser hijacking, multiple fraudulent scans, and false error messages the defendants and others allegedly deceived victims into purchasing the full paid versions of IM software products, such as "Malware Alarm," "Antivirus 2008," and "VirusRemover 2008." At times, the defendants defrauded victims into purchasing multiple products through a deceptive order screen that kept hidden certain pre-checked option boxes which, when checked, increased the total number of products being purchased, the indictment alleges.

The proceeds of these sales, typically by credit card, were allegedly deposited into bank accounts controlled by the defendants and others throughout the world, and then were transferred to additional bank accounts located in Europe.

The defendants and others allegedly used Byte Hosting to deflect complaints from victims who purchased IM software products. Knowing the products to be fraudulent and distributed and sold under false pretenses, Reno and others caused call center representatives to be instructed to lie to customers about the products and persuade them to remove legitimate pre-existing anti-virus software, the indictment alleges. To persuade the Byte Hosting call center representatives to continue their employment, Reno and others falsely informed them that they were not involved in a fraud scheme because United States law did not apply to IM and its business practices because IM

was based overseas. The call center employees were authorized to provide refunds to discourage victims from notifying their credit card companies or law enforcement that they were deceived into purchasing the fraudulent software products, according to the indictment.

Individuals who believe they are victims and want to receive information about the criminal prosecution may call a toll-free hotline, 866-364-2621, ext. 1, for periodic updates.

The government is being represented by Assistant U.S. Attorneys Michael Ferrara and William Ridgway.

Each count of wire fraud carries a maximum penalty of 20 years in prison and a $250,000 fine and restitution is mandatory. The Court may also impose a fine totaling twice the loss to any victim or twice the gain to the defendant, whichever is greater. If convicted, the Court would determine a reasonable sentence to impose under the advisory United States Sentencing Guidelines.

An indictment contains only charges and is not evidence of guilt. The defendants are presumed innocent and are entitled to a fair trial at which the government has the burden of proving guilt beyond a reasonable doubt.

# # # #