United States Attorney
Southern District of New York

FOR IMMEDIATE RELEASE
APRIL 19, 2010

CONTACT: **U.S. ATTORNEY'S OFFICE**
YUSILL SCRIBNER,
JANICE OH
PUBLIC INFORMATION OFFICE
(212) 637-2600

FBI
JIM MARGOLIN, RICHARD KOLKO
PUBLIC INFORMATION OFFICE
(212) 384-2720, 2715

MANHATTAN U.S. ATTORNEY CHARGES BELARUSIAN CREATOR OF INTERNATIONAL IDENTITY THEFT WEBSITE

Dmitry Naskovets Allegedly Ran Online Business That Targeted U.S. and European Financial Institutions And Committed Over 5,000 Frauds. At Request of U.S. Authorities, Naskovets Was Arrested In the Czech Republic On April 15, 2010.

PREET BHARARA, the United States Attorney for the Southern District of New York, and JOSEPH M. DEMAREST, JR., the Assistant Director-in-Charge of the New York Office of the Federal Bureau of Investigation ("FBI"), announced today the unsealing of an Indictment against DMITRY M. NASKOVETS -- creator and operator of CallService.biz, an online business that assisted over 2,000 identity thieves in over 5,000 instances of fraud -- on charges of conspiracy to commit wire fraud, conspiracy to commit credit card fraud, and aggravated identity theft. At the request of the United States, authorities of the Czech Republic on Thursday, April 15, 2010, provisionally arrested NASKOVETS pending his extradition to the United States.

According to the Indictment unsealed today in Manhattan federal court:

In June 2007, NASKOVETS, a Belarusian national, and co-conspirator SERGEY SEMASHKO, also a Belarusian national who is charged by the Belarusians, created CallService.biz (the "Website"), an online business intended to assist identity thieves in exploiting stolen financial information, such as credit card and debit card numbers. The Website was, among other things, designed to counteract security measures put in place by financial institutions. These security measures, for example, require persons seeking to make transfers or withdrawals from accounts, or to conduct other financial transactions to verify by

telephone certain information associated with the account. Businesses that accept online or telephone purchases by credit card have similar security measures. Representatives at such financial institutions and businesses are trained to make sure that persons purporting over the telephone to be account holders appear to fit the account holder's profile. So if an account holder is an American female, the screener is supposed to make sure that the caller speaks English, and does in fact sound like a female.

Through the Website, NASKOVETS and SEMASHKO, in exchange for a fee, provided the services of English- and German-speaking individuals to persons who had stolen account and biographical information to beat the above-described security screening processes. Specifically, those English and German speakers would, among other things, pose as authorized account holders and place telephone calls to financial institutions and other businesses to conduct or confirm fraudulent withdrawals, transactions, or other account activity on behalf of the Website users, who were identity thieves. Using information provided by the identity thieves over the Website, which was hosted on a computer in Lithuania, the fraudulent callers would, among other things, confirm unauthorized withdrawals or transfers from bank accounts, unblock accounts, or change the address or phone number associated with an account so that it could be accessed by the identity thieves.

For example, a request made to the Website could consist of the name of the bank the identity thief wanted to contact, the stolen account information and biographical information the thief had illegally obtained, and instructions from the identity thief as to what to say, or the fraudulent transaction that was to be conducted, during a phone call to the bank. NASKOVETS and his co-conspirators would assign an appropriate individual employed by the Website, namely one who was the same gender and spoke the same language as the authorized account holder. After the requested call was made, NASKOVETS and his co-conspirators would report the results to the the identity thief, who could issue instructions for further telephone calls, if necessary.

The Website posted advertisements for its services on other websites used by identity thieves, including CardingWorld.cc, which was operated by SEMASHKO. The advertisements boasted that the Website had "over 2090 people working with" it and had "done over 5400 confirmation calls" to banks, referencing calls to defeat security screening procedures and confirm or conduct fraudulent transactions, as described above.

* * *

NASKOVETS was provisionally arrested by Czech law enforcement authorities on April 15, 2010, at the request of the United States pursuant to bilateral treaties between the countries. Also on April 15, 2010, in a joint operation, Belarusian law enforcement authorities arrested SEMASHKO in Belarus and Lithuanian law enforcement authorities seized the computers on which the Website and the CardingWorld.cc website were hosted.

In addition, here in New York, the FBI simultaneously seized the Website domain name pursuant to a seizure warrant issued by United States District Judge LEWIS A. KAPLAN, to whom the case is assigned.

On April 15, 2010, Belarusian authorities arrested additional co-conspirators of SEMASHKO for related criminal conduct. The Lithuanian investigation is continuing.

* * *

The Indictment charges NASKOVETS with one count of conspiracy to commit wire fraud, one count of conspiracy to commit access device fraud, and one count of aggravated identity theft. If convicted on all three counts, NASKOVETS faces a maximum sentence of 39 years plus six months in prison.

U.S. Attorney PREET BHARARA said, "Cybercrime poses an increasingly grave threat to American and European financial institutions and their customers. As alleged, Dmitry Naskovets's website was essentially an online bazaar for dangerous identity thieves. His website was especially dangerous because it allegedly was specifically designed to bypass the usual security measures that bank and business customers have come to rely on. Today, we have shut down that business and protected untold thousands of potential victims of identity theft. This Office is committed to pursuing the perpetrators of cybercrimes wherever they may be, and will continue to work with the FBI and our foreign law enforcement partners to bring this new breed of criminals to justice."

FBI Assistant Director-in-Charge JOSEPH M. DEMAREST, JR., stated: "People such as Naskovets believe that simply being outside of the United States gives them the freedom to carry out their criminal activities. The victims of these criminal schemes pay dearly, but online crime affects everyone by reducing the

public's confidence in the Internet and the losses affect all businesses and customers with increased costs. Cyber crime has no boundaries, and the FBI will continue to work with our international partners to pursue these criminals wherever they may try to hide."

Mr. BHARARA praised the FBI for its exceptional work on the investigation, and thanked the Department of Justice's Office of International Affairs; the Belarusian Ministry of Internal Affairs, High Tech Crime Department; the Police Presidium of the Czech Republic; and the Lithuanian Criminal Police Bureau Cybercrime Board for their assistance.

This case is being handled by the Office's Complex Frauds Unit. Assistant United States Attorneys THOMAS G.A. BROWN and MICHAEL FERRARA are in charge of the prosecution.

The charges contained in the Indictment are merely accusations and NASKOVETS is presumed innocent unless and until proven guilty.

10-134 ###