4 Russians, 1 Ukrainian charged in massive hacking

July 25 2013, by Samantha Henry

(AP)—Four Russian nationals and a Ukrainian have been charged with running a sophisticated hacking organization that over seven years penetrated computer networks of more than a dozen major American and international corporations, stealing and selling at least 160 million credit and debit card numbers, resulting in losses of hundreds of millions of dollars.

Indictments were announced Thursday in Newark, where U.S. Attorney Paul Fishman called the case the largest hacking and data breach scheme ever prosecuted in the United States.

Princeton-based Heartland Payment Systems Inc., which processes credit and debit cards for small to mid-sized businesses, was identified as taking the biggest hit in a scheme starting in 2007—the theft of more than 130 million card numbers at a loss of about $200 million.

Atlanta-based Global Payment Systems, another major payment processing company, had nearly 1 million card numbers stolen, with losses of nearly $93 million, prosecutors said.

The indictment did not put a loss figure on the thefts at some other major corporations, including Commidea Ltd., a European provider of electronic payment processing for retailers. The government said hackers in 2008 covertly removed about 30 million card numbers from its computer network.

About 800,000 card numbers were stolen in an attack on the Visa network, but the indictment did not cite any loss figure.

Not all the companies the hackers infected over the years with malicious computer software suffered financial losses. Customer log-in credentials were stolen from Nasdaq and Dow Jones Inc., the indictment said, though prosecutors said Nasdaq's trading platform was not affected.

The indictment said the suspects sent each other instant messages as they took control of the corporate data, telling each other, for instance: "NASDAQ is owned." At least one man told others that he used Google news alerts to learn whether his hacks had been discovered, according to the court filing.

The defendants were identified as Russians Vladimir Drinkman, Aleksander Kalinin, Roman Kotov and Dmitriy Smilianets, and Ukrainian Mikhail Rytikov.

Smilianets is in U.S. custody and is expected to appear in federal court next week. Drinkman is being held in the Netherlands pending extradition, prosecutors said. The other three defendants remained at large.

The prosecution builds on a case that resulted in a 20-year prison sentence in 2010 for Albert Gonzalez of Miami, who often used the screen name "soupnazi" and is identified in the new complaint as an unindicted co-conspirator. Other unindicted co-conspirators were also named.

Prosecutors identified Drinkman and Kalinin as sophisticated hackers who specialized in penetrating the computer networks of multinational corporations, financial institutions and payment processors.

Kotov's specialty was harvesting data from the networks after they had been penetrated, and Rytikov provided anonymous web-hosting services that were used to hack into computer networks and covertly remove data, the indictment said.

Smilianets was the information salesman, the government said.

All five are charged with taking part in a computer hacking conspiracy and conspiracy to commit wire fraud. The four Russian nationals are also charged with multiple counts of unauthorized computer access and wire fraud.

The individuals who purchased the credit and debit card numbers and associated data from the hacking organization resold them through online forums or directly to others known as "cashers," the indictment said. According to the indictment, U.S. credit card numbers sold for about $10 each; Canadian numbers were $15 and European ones $50.

The data was stored on computer servers all over the world, including in New Jersey, Pennsylvania, California, Illinois, Latvia, the Netherlands, Bahamas, Ukraine, Panama and Germany.

The cashers would encode the information onto the magnetic strips of blank plastic cards and cash out the value, by either withdrawing money from ATMs in the case of debit cards, or running up charges and purchasing goods in the case of credit cards.