

Man charged in biggest US hacking scheme pleads not guilty (Update 2)

February 17 2015, by David Porter

A Russian citizen pleaded not guilty Tuesday to an 11-count indictment charging him and four others with running what authorities have called the largest criminal computer hacking scheme ever prosecuted in the United States.

Vladimir Drinkman appeared in U.S. District Court in New Jersey shackled and in yellow prison garb for the brief hearing, in which he pleaded not guilty to computer hacking conspiracy, wire fraud conspiracy, several counts of unauthorized computer access and three counts of wire fraud.

The wire fraud and wire fraud conspiracy counts each carries a maximum sentence of 30 years.

Authorities say Drinkman, 34, of Moscow and Syktyvkar, Russia, and four co-conspirators from Russia and Ukraine stole and sold 100 million to 200 million credit and debit card numbers from payment processing companies, retailers and financial institutions between 2005 and 2012. The U.S. attorney's office estimated the total loss to just three of the corporate victims comes to more than \$300 million.

Among the alleged victims were the Nasdaq stock exchange; Dow Jones Inc.; Heartland Payment Systems; JC Penney; 7-Eleven and JetBlue Airways.

Heartland, which has offices in Princeton and is one of the world's

largest credit and debit card payment processing companies, suffered the loss of more than 130 million card numbers leading to losses of about \$200 million, according to the indictment. The co-conspirators allegedly stole more than 950,000 card numbers from Atlanta, Georgia-based Global Payment Systems, one of the world's largest electronic transaction processing companies, creating losses of about \$93 million.

According to the U.S. attorney's office, Drinkman and others would seek vulnerabilities in the networks of corporations that conducted financial transactions and then used computers in New Jersey, California, Illinois, and Pennsylvania and in countries, including the Netherlands, the Bahamas, Latvia and Panama, to stage attacks on the networks.

Federal prosecutors say that once log-in data, card numbers and personal information was stolen it was passed to Dmitriy Smilianets, who allegedly sold it to resellers who in turn sold it to individuals to be encoded onto the magnetic strips of blank plastic cards. The cards were used to withdraw money from ATMs or charge purchases.

According to the indictment, Smilianets charged about \$10 for each stolen U.S. credit card number, \$15 for a Canadian number and \$50 for each European credit card number, with discounts for bulk purchases.

Drinkman was held in Amsterdam after his arrest in 2012 before he was extradited Friday, according to his attorney.

Amsterdam-based attorney Bart Stapert said his client "will finally be able to receive and confront what the government claims is the evidence against him. He looks forward to thoroughly litigating these charges."

Smilianets also is in custody awaiting trial. The other three named in the indictment are fugitives.

© 2015 The Associated Press. All rights reserved.

Citation: Man charged in biggest US hacking scheme pleads not guilty (Update 2) (2015, February 17) retrieved 25 April 2024 from <https://phys.org/news/2015-02-russian-biggest-hacking-scheme-due.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.