November 17, 2005
WWW.USDOJ.GOV
Department Of Justice
CRM
(202) 514-2007
TDD (202) 514-1888

Six Defendants Plead Guilty in Internet Identity Theft and Credit Card Fraud Conspiracy

Shadowcrew Organization Was Called 'One-Stop Online Marketplace For Identity Theft'

WASHINGTON, D.C. — Six men who administered and operated the "Shadowcrew.com" website one of the largest online centers for trafficking in stolen credit and bank card numbers and identity information pleaded guilty today in federal court, the Department of Justice and U.S. Attorney's office for the District of New Jersey announced today.

The one-stop online marketplace operated by the defendants was taken down in October 2004 by the U.S. Secret Service, closing an illicit business that trafficked in at least 1.5 million stolen credit and bank card numbers that resulted in losses in excess of $4 million.

Andrew Mantovani, 23, of Scottsdale, Ariz.; Kim Taylor, 47, of Arcadia, Calif.; Jeremy Stephens, 31, of Charlotte, N.C.; Brandon Monchamp, 22, of Scottsdale, Ariz.; Omar Dhanani, 22, of Fountain Valley, Calif.; and Jeremy Zielinski, 22, of Longwood, Fla., entered guilty pleas to the lead count of conspiracy before U.S. District Judge William J. Martini. Judge Martini scheduled sentencings in late February and early March.

The defendants admitted their respective roles in the online conspiracy to commit credit and bank card fraud, as well as identification document fraud. Mantovani also pleaded guilty to a second count of unlawful transfer of identification to facilitate criminal conduct. Mantovani admitted his role in illegally obtaining approximately 18 million e-mail accounts with associated personal identifying information.

Both the conspiracy and unlawful transfer counts carry maximum prison sentences of five years and a maximum fine of $250,000. On Wednesday, Wesley Lanning, 22, of Grove City, Ohio, also pleaded guilty before Judge Martini to the conspiracy count, as did Rogerio Rodrigues 22, of Chicago, on Sept. 22.

"These individuals proved in a big way that the Internet can be a dangerous place where consumers can be victimized without warning," said U.S. Attorney Christopher J. Christie. "But as this case also shows, criminals operating in the virtual world of the Internet are not ultimately anonymous. Their crimes can be traced and documented, and they can be tracked down, arrested, prosecuted and sent to prison."

"These guilty pleas illustrate the continued success of investigations such as Operation Firewall in disrupting cyber criminal networks," said David O' Connor, Special Agent in Charge of the

Secret Service's Newark Field Office. "Through the joint efforts of the Secret Service and our partners at the state, local and federal levels, we continue to aggressively investigate and successfully prosecute criminal activity that threatens our country's financial infrastructure."

The Shadowcrew organization and its associated website, www.Shadowcrew.com, was a hub of online identity theft activity, facilitating online trafficking in stolen identity information and documents, as well as stolen credit and debit card numbers. A year-long investigation by the Secret Service led to the arrests of 21 individuals in the United States in October 2004. To date, 12 have pleaded guilty. Additionally, several individuals were arrested in foreign countries.

The indictment charged that the administrators, moderators, vendors and others involved with Shadowcrew conspired to provide stolen credit and bank card numbers and identity documents through the Shadowcrew marketplace. The account numbers and other items were sold by approved vendors who had been granted permission to sell by administrators and moderators of the Shadowcrew site after completing a review process.

During his guilty plea, Mantovani acknowledged his role as co-founder and administrator of the Shadowcrew website. As such, Mantovani had the power to control the direction of the organization as well as the day-to-day management of the website. He admitted using techniques such as phishing and spamming to illegally obtain credit and bank card information, which he then used to make purchases of merchandise online. The illegally obtained goods were then sent to a "drop" or mailing address specifically set up to receive the stolen goods.

Stephens, Taylor, Mantovani, Zielinski, Monchamp and Lanning all acknowledged that Shadowcrew members sent and received payment for illicit merchandise and services via Western Union money transfers and digital currencies such as E-Gold and Web Money. In addition, Mantovani admitted that in September 2004, he illegally acquired via computer, approximately 18 million e-mail accounts with associated usernames, passwords, dates of birth, and other personally identifying information — approximately 60,000 of which included first and last name, gender, address, city, state, country and telephone number.

U.S. Attorney Christie credited Special Agents of the Secret Service in Newark, under the direction of Special Agent in Charge David O'Connor, in Morristown, for their work in developing the case.

The government was represented by Assistant U.S. Attorney Kevin M. O'Dowd of the U.S. Attorney's Office Criminal Division, and Kimberly Kiefer Peretti from the Computer Crime and Intellectual Property Section of the Department of Justice.

05-619

###