



*United States Attorney
District of New Jersey*



FOR IMMEDIATE RELEASE
June 12, 2013
www.justice.gov/usao/nj

CONTACT: Rebekah Carmichael
Matthew Reilly
Office of Public Affairs
(973) 645-2888

**EIGHT CHARGED WITH FRAUD, ID THEFT, MONEY LAUNDERING
IN MULTIMILLION-DOLLAR INTERNATIONAL CYBERCRIME SCHEME**

*Organization Allegedly Capitalized on Information Hacked
From More Than a Dozen Global Financial Institutions*

NEWARK, N.J. – Eight alleged members of an international cybercrime, money laundering and identity theft conspiracy are federally charged in New Jersey with a scheme to use information hacked from customer accounts held at more than a dozen banks, brokerage firms, payroll processing companies and government agencies in an attempt to steal at least \$15 million from U.S. customers, New Jersey U.S. Attorney Paul J. Fishman announced.

The eight defendants are charged together in a criminal complaint with conspiracy to commit wire fraud, conspiracy to commit money laundering and conspiracy to commit identity theft. Allegedly, Oleksiy Sharapka, 33, of Kiev, Ukraine, directed the conspiracy with the help of Leonid Yanovitsky, 38, also of Kiev. Oleg Pidtergerya, 49, of Brooklyn, N.Y.; Robert Dubuc, 40, of Malden, Mass.; and Andrey Yarmolitskiy, 41, of Atlanta, managed crews in their respective cities. Richard Gunderson, 46, of Brooklyn, and Lamar Taylor, 37, of Salem, Mass, worked for Pidtergerya and Dubuc, respectively. Ilya Ostapyuk, 31, of Brooklyn, allegedly facilitated the movement of fraud proceeds.

Pidtergerya, Ostapyuk and Dubuc were arrested this morning at their homes by federal agents, and Yarmolitskiy was arrested yesterday, June 11, 2013, as he arrived at John F. Kennedy International Airport on an overseas flight. He is expected to appear on a date to be determined before U.S. Magistrate Judge Cathy L. Waldor in Newark federal court. Pidtergerya and Ostapyuk are to appear before Judge Waldor this afternoon. Dubuc is scheduled for an initial appearance in federal court in Boston. Taylor and Gunderson are being pursued by law enforcement, and Sharapka and Yanovitsky, Ukrainian nationals, remain at large.

“According to the complaint unsealed today, cybercriminals penetrated some of our most trusted financial institutions as part of a global scheme that stole money and identities from people in the United States,” said U.S. Attorney Fishman. “Today’s charges and arrests take out key members of the organization, including leaders of crews in three states that used those stolen identities to “cash out” hacked accounts in a series of internationally coordinated modern-day

bank robberies. We will continue to pursue our investigation into this scheme and our fight against the rising threat of criminals for whom computers are the weapon of choice.”

“The investigation and successful prosecution of suspects involved in organized global fraud directed at electronic payment systems is dependent upon the collaborative efforts of federal law enforcement and private industry to ensure the confidentiality, integrity and availability of these systems as part of our critical financial infrastructure,” said Special Agent in Charge James Mottola of the U.S. Secret Service, Newark Field Office.

“These arrests underscore HSI’s commitment and the joint ongoing efforts across the entire law enforcement spectrum to stop these cybercriminals in their tracks,” said Andrew M. McLees, Special Agent in Charge of Immigration and Customs Enforcement, Homeland Security Investigations (HSI) in Newark. “HSI special agents will use every cutting-edge technological investigative tool at their disposal to dismantle these global criminal enterprises at the source and bring them to justice.”

According to the criminal complaint unsealed today:

Conspiring hackers gained unauthorized access to the computer networks of more than a dozen global financial institutions, including: Aon Hewitt; Automated Data Processing Inc.; Citibank N.A.; E-Trade; Electronic Payments Inc.; Fundtech Holdings LLC, iPayment Inc.; JP Morgan Chase Bank N.A.; Nordstrom Bank; PayPal; TD Ameritrade; U.S. Department of Defense, Defense Finance and Accounting Service; TIAA-CREF; USAA; and Veracity Payment Solutions Inc.

Once inside the victim companies’ computer networks, the defendants and conspirators diverted money from accounts of the companies’ customers to bank accounts and pre-paid debit cards controlled by the defendants. They then implemented a sophisticated “cash out” operation, employing crews of individuals known as “cashers” to withdraw the stolen funds, among other ways, by making ATM withdrawals and fraudulent purchases in New York, Massachusetts, Illinois, Georgia and elsewhere.

As part of the scheme, the defendants stole identities from individuals in the United States, which they used to facilitate the cash out operation, including by transferring money to cards in the names of those stolen identities. They also used some of those identities to file fraudulent tax returns with the IRS seeking refunds.

The defendants and their conspirators laundered the proceeds of the scheme, often through international wire transfer services, to the leaders of the conspiracy overseas.

The government’s ongoing investigation into the organization has so far identified attempts to defraud the victim companies and their customers of more than \$15 million.

If convicted, each of the defendants face a maximum potential penalty of 20 years in prison on the conspiracy to commit wire fraud count, 20 years in prison on the conspiracy to commit money laundering count and 15 years in prison on the conspiracy to commit identity

theft count. The wire fraud and identity theft counts also carry a maximum fine of \$250,000, or twice the gross amount of pecuniary gain or loss resulting from the offenses. The money laundering conspiracy count carries a maximum fine of \$500,000, or twice the value of the monetary instruments involved.

U.S. Attorney Fishman credited the U.S. Secret Service, under the direction of Special Agent in Charge Mottola; HSI, under the direction of Special Agent in Charge McLees; Defense Criminal Investigative Service, under the direction of Special Agent in Charge Jeffery D. Thorpe; and IRS-Criminal Investigation, under the direction of Special Agent in Charge Shantelle P. Kitchen with the ongoing investigation. He also thanked the Department of Homeland Security's Customs and Border Protection for assistance with the Yarmolitskiy arrest.

The government is represented by Assistant U.S. Attorneys Gurbir S. Grewal, of the Computer Hacking and Intellectual Property Section of the U.S. Attorney's Office Economic Crimes Unit, and Barbara Ward of the office's Asset Forfeiture and Money Laundering Unit.

The charges and allegations contained in the complaint are merely accusations, and the defendants are presumed innocent unless and until proven guilty.

This case was brought in coordination with President Barack Obama's Financial Fraud Enforcement Task Force. The task force was established to wage an aggressive, coordinated and proactive effort to investigate and prosecute financial crimes. With more than 20 federal agencies, 94 U.S. Attorneys' offices and state and local partners, it's the broadest coalition of law enforcement, investigatory and regulatory agencies ever assembled to combat fraud. Since its formation, the task force has made great strides in facilitating increased investigation and prosecution of financial crimes; enhancing coordination and cooperation among federal, state and local authorities; addressing discrimination in the lending and financial markets and conducting outreach to the public, victims, financial institutions and other organizations. Over the past three fiscal years, the Justice Department has filed nearly 10,000 financial fraud cases against nearly 15,000 defendants including more than 2,900 mortgage fraud defendants. For more information on the task force, please visit www.stopfraud.gov.