U.S. Department of Justice
United States Attorney Northern District of California
11th Floor, Federal Building, 450 Golden Gate Ave, San Francisco, CA 94102 - Tel: (415) 436-7200 - Fax: (415) 436-7234
FOR IMMEDIATE RELEASE

June 4, 2004

The United States Attorney for the Northern District of California announced that Roman Vega, 39 of Ukraine, made his initial appearance in federal court in San Francisco today following his extradition from Cyprus on a 40-count indictment alleging credit card trafficking and wire fraud. Mr. Vega entered a not guilty plea to all charges.

According to the indictment, which was unsealed today, Mr. Vega is alleged to have used Internet chat rooms to traffic in credit card information of thousands of individuals that had been illegally obtained from sources around the world, including credit card processors and merchants. Mr. Vega was also allegedly an operator of a Web site at www.boafactory.com, where stolen and counterfeit credit card account information was allegedly bought and sold.

In particular, the indictment charges Mr. Vega with 20 counts of wire fraud under 18 U.S.C. § 1343 and 20 counts of using of unauthorized access devices (credit cards) with intent to defraud under 18 U.S.C. § 1029(a)(2). The maximum statutory penalty for each count in violation of 18 U.S.C. § 1343 is 20 years imprisonment, a fine of $250,000, plus restitution if appropriate. The maximum statutory penalty for each count in violation of 18 U.S.C. § 1029(a)(2) is 10 years imprisonment, a fine of $250,000, plus restitution if appropriate.

However, any sentence following conviction would be dictated by the Federal Sentencing Guidelines, which take into account a number of factors, and would be imposed in the discretion of the Court. An indictment simply contains allegations against an individual and, as with all defendants, Mr. Vega must be presumed innocent unless and until convicted.

Following the government's motion to detain defendant as a flight risk pending trial, United States Magistrate Judge Joseph C. Spero remanded Mr. Vega into custody pending a detention hearing to be held on Wednesday, June 9 at 9:30 a.m. The defendant is also scheduled to appear for a status conference before United States District Judge Charles R. Breyer on June 9 at 2:15 p.m.

United States Attorney Kevin V. Ryan stated: "This case signifies the Northern District of California's commitment to bring criminal charges against those alleged to be major traffickers of stolen credit card account information. It also should serve as an example to individuals abroad who commit frauds against our country's citizens and institutions that the Department of Justice will vigorously seek their extradition to the United States."

The prosecution is the result of an investigation by the San Francisco Electronic Crimes Task Force, which includes agents from the United States Secret Service and the United States Postal Inspection Service. The United States Embassy in Cyprus and the authorities from Cyprus also substantially assisted in Mr. Vega's extradition. The investigation was overseen by the Computer Hacking and Intellectual Property (CHIP) Unit of the United States Attorney's Office. Assistant United States Attorneys Kyle F. Waldinger and Christopher P. Sonderby are prosecuting the case.

Visa Security Summit

Cardholder Security in the New Electronic Payments Age
Keynote Address
John Philip Coghlan, President and CEO, Visa USA
Mandarin Oriental Hotel, Washington, DC, 5. October, 2005

There is a man named “Boa,” an alias for someone named Roman Vega, originally from the Ukraine. According to authorities, he’s an accomplished fraud artist and credit card scammer. Roman used sophisticated computer systems to produce and sell counterfeit credit cards. At his peak, he was even so brazen as to advertise his services.
Monitoring systems were able to track patterns of unusual activity in Cyprus – where a merchant working with Boa with little transaction volume suddenly showed significant volume.
Today, Boa sits in a California jail, facing charges of wire and credit card fraud in a 40-count federal indictment. His trial is expected to begin in San Francisco soon. With any luck, we may have won this single battle.
It’s an example of how we can use INNOVATION, in this case, through TECHNOLOGY, to outsmart a criminal and put an end to a costly fraud ring.
You’ve already seen this technology at work. Many of you have received a phone call at home asking if you made a purchase in a city you've never been in or at a store you don’t recognize. It happened to me in New York the other day. One of my Visa cards that I don’t use very often was declined as I tried to purchase a pair of shoes. So I smiled and was actually pleased when my card was declined, knowing that the safeguards were working. The technology is enormously sophisticated. Well beyond my simple situation. Unusual spending patterns, or tangential linkages to other fraud events are detected through “hybrid networks” technology that we call, simply, “Advanced Authorization.”

August 26, 2004
DoJ Nabs 103 in Online Crime Sweep
By Roy Mark
WASHINGTON -- More than a hundred individuals have been arrested and charged this summer in a federal computer and Internet-related crime sweep known as Operation Web Snare, U.S. Attorney General John Ashcroft said today.
The operation was launched on June 1 and concluded today with several arrests. In all, Ashcroft said, approximately 350 individuals were targeted for major forms of online economic crime and other cybercrimes, resulting in 103 arrests and 53 convictions.
"Operation Web Snare is the largest and most successful collaborative law enforcement operation ever conducted to prosecute online fraud, stop identity theft and prevent other computer-related crimes," Ashcroft said.
Thursday's announcement marked the second consecutive day Ashcroft held a media briefing to tout the Department of Justice's (DoJ) online anti-crime efforts. Wednesday, he said search warrants had been issued in the DOJ's first criminal probe of copyright theft on peer-to-peer (P2P) networks.
Ashcroft said Thursday the summer-long investigations revealed the "continuing internationalization of Internet fraud."
Of the 30 case summaries presented to the media, many of them previously reported, six involved foreign nationals or U.S. citizens originally from Morocco, Pakistan, China, Korea, Romania and Nigeria.

In one of the most recent cases, the U.S. Attorney's Office in Los Angeles charged Jie Dong last week in the largest PayPal and eBay fraud scheme to date. The DoJ considers Dong, who has subsequently fled the country and is at large, a "skilled Internet fraudster"; he allegedly stole more than $800,000 from unwitting victims. The DoJ claims Dong conducted more than 5,000 fraudulent sales to eBay customers in just four months.

In another case, Jay R. Echouafni, CEO of Massachusetts-based Orbit Communications, was indicted Wednesday along with five other individuals on multiple charges of conspiracy and causing damage to protected computers. According to the DoJ, Echouafni and a business partner launched "relentless" Denial-of-Service attacks on Orbit's competitors.

Using the services of computer hackers in Arizona, Louisiana, Ohio and the United Kingdom, the DoJ claims the attacks caused more than $2 million in damage to competitors in revenue and costs associated with responding to the attacks. Echouafni, a U.S. citizen of Moroccan origin, has subsequently fled the United States and is the target of what the FBI characterizes an "international manhunt."

Also on the run is Calin Mateias, an alleged Romanian computer hacker who was charged earlier this month with conspiring to steal more than $10 million in computer equipment from Ingram Micro in Santa Ana, Calif. The indictment claims Mateias, a Bucharest resident, hacked into Ingram's online ordering system and placed fraudulent orders for computers and related equipment.

The DoJ says Mateias then had the equipment sent to dozens of addresses throughout the United States as part of an Internet fraud scheme. Mateias's U.S. co-defendants would in turn allegedly either sell the equipment and send the proceeds to Mateias or repackage the equipment and send it to Romania.

In a case where the DoJ successfully extradited a Cyprus citizen, Roman Vega of the Ukraine is facing a 40-count indictment alleging credit card trafficking and wire fraud. The DoJ claims Vega used Internet chat rooms to gather thousands of individuals' credit card information, which had been illegally obtained from sources around the world, including credit card processors and merchants. The DoJ also alleges Vega operated a Web site where stolen and counterfeit credit card account information was bought and sold.

"Operation Web Snare ... shows that America's justice community is seeking to anticipate, out-think and adapt to new trends in Internet crime," Ashcroft said.

<Quelle: www.internetnews.com>