



Department of Justice

FOR IMMEDIATE RELEASE
THURSDAY, FEBRUARY 7, 2019
WWW.JUSTICE.GOV

CRM
(202) 514-2007
TTY (866) 544-5309

**UNITED STATES AND INTERNATIONAL LAW ENFORCEMENT DISMANTLE
ONLINE ORGANIZED CRIME RING OPERATING OUT OF ROMANIA THAT
VICTIMIZED THOUSANDS OF U.S. RESIDENTS**

Twelve Foreign Nationals Extradited to the United States

WASHINGTON – According to court documents unsealed today, 20 people, including 16 foreign nationals, have been charged for their roles in an international organized crime group that defrauded American victims through online auction fraud causing millions of dollars in losses.

Assistant Attorney General Brian A. Benczkowski of the Justice Department’s Criminal Division, U.S. Attorney Robert M. Duncan, Jr. of the Eastern District of Kentucky, Director Randolph D. Alles of the U.S. Secret Service (USSS), Commissioner Richard W. Sanders of the Kentucky State Police, Chief of Police Lawrence Weathers of the Lexington Police Department, Chief Don Fort of IRS Criminal Investigation and Inspector in Charge Tommy Coke of the U.S. Postal Inspection Service Pittsburgh Division made the announcement.

“The defendants allegedly orchestrated a highly organized and sophisticated scheme to steal money from unsuspecting victims in America and then launder their funds using cryptocurrency,” said Assistant Attorney General Benczkowski. “As the charges and arrests announced today demonstrate, the Criminal Division and our law enforcement partners will vigorously pursue cybercriminals who defraud the American public, regardless of where those criminals may reside.”

“This prosecution stems from a multi-year investigation initiated in Kentucky led by the U.S. Secret Service, in cooperation with several local, state, federal, and international law enforcement partners,” said U.S. Attorney Duncan. “Cooperation of this kind is essential, if we are to be effective in disrupting organized cybercrime, which costs victims from across the United States millions of dollars and has become an increasingly prevalent means for criminals to prey on the public. I commend the exceptional work done by our law enforcement partners, and we are proud to join this cooperative effort to combat cyber fraud schemes.”

“Today’s announcement demonstrates the success of the collaborative efforts of our worldwide network of law enforcement partners. It sends a powerful message and demonstrates the transnational investigative capabilities of the Secret Service,” said Secret Service Director

Randolph “Tex” Alles. “This is a shared win for law enforcement across the globe. I would like to thank the more than a dozen law enforcement agencies worldwide who helped us investigate this case, each played a vital role in its success.”

On July 5, 2018, a federal grand jury in Lexington, Kentucky returned a 24-count indictment charging 15 foreign nationals with RICO conspiracy, wire fraud conspiracy, money laundering conspiracy, and aggravated identity theft. Those charged include Andrei-Cătălin Stoica, 28, of Romania; Victor-Aurel Grama, 29, of Romania; Liviu-Sorin Nedelcu, 33, of Romania; Ionuț Ciobanu, 28, of Romania; Marius-Dorin Cernat, 35, of Romania; Alexandru Ion, 30, of Romania; Ștefan-Alexandru Păiuși, 33, of Romania; Eugen-Alin Badea, 34, of Romania; Cristișor Olteanu, 31, of Romania; Adrian Mitan, 34, of Romania; Bogdan-Ștefan Popescu, 29, of Romania; Florin Arvat, 24, of Romania; Alin-Ionuț Dobrică, 26, of Romania; Vlad-Călin Nistor, 31, of Romania, and Rossen Iossifov, 51, of Bulgaria. On Feb. 6, a federal grand jury in Lexington returned an 11-count indictment charging an additional foreign national and four Americans for their roles in the criminal enterprise. Those charged include Benjamin-Filip Ologeanu, 29, of Alexandria, Romania; Austin Edward Nedved, 27, of Northborough, Massachusetts; Dimitrius Antoine Brown, 37, of Macon, Georgia and Rashawd Lamar Tulloch, 30, of Newnan, Georgia. Andrew Gilbert Ybarra II, 25, of Patterson, California, was also charged with conspiracy to commit money laundering. In all, 15 Romanian nationals and one Bulgarian national were charged in these two indictments. Of these, 12 have been extradited to the United States and are awaiting trials, which are currently set for June 18, 2019 and Aug. 7, 2019.

The indictment alleges that these defendants participated in a criminal conspiracy primarily located in Alexandria, Romania that engaged in a large-scale scheme of online auction fraud. Specifically, Romania-based members of the conspiracy and their associates posted false advertisements to popular online auction and sales websites—such as Craigslist and eBay—for high-cost goods (typically vehicles) that did not actually exist. According to the indictment, these members would convince American victims to send money for the advertised goods by crafting persuasive narratives, for example, by impersonating a military member who needed to sell the advertised item before deployment. The members of the conspiracy are alleged to have created fictitious online accounts to post these advertisements and communicate with victims, often using the stolen identities of Americans to do so. They are alleged to have delivered invoices to the victims bearing trademarks of reputable companies in order to make the transactions appear legitimate. Once victims were convinced to send payment, the indictment alleges that the conspiracy engaged in a complicated money laundering scheme wherein domestic associates would accept victim funds, convert these funds to cryptocurrency, and transfer proceeds in the form of cryptocurrency to foreign-based associates. The indictment alleges that these foreign-based money launderers include Vlad-Călin Nistor, who owns Coinflux Services SRL, and Rossen Iossifov, who owns R G Coins. According to the indictment, Nistor and Iossifov exchanged cryptocurrency into local fiat currency on behalf of the Romania-based members of the conspiracy, knowing that they were exchanging bitcoin that represented the proceeds of fraud.

Some of the fraud schemes alleged in the indictments include:

- Nedelcu persuaded victims to send money for the advertised goods by creating fictitious but legitimate sounding entities through which he purported to sell vehicles. For example, he used email address, foiaol2015@gmail.com, belonging to Aol Autos, to communicate with victims by email with subject lines like, “America Online Autos Financial Department [Order # 099106592090].” The email would contain messages appearing to be legitimate invoices for payment for the advertised item purported to be sold.
- Ciobanu and his coconspirators used the email address judithlane82@gmail.com to communicate with victims about the sale of vehicles, signing the emails as “Sgt. Judith Lane,” and created a Facebook profile for Judith Lane, who was depicted as a member of the Air Force. Ciobanu, acting as “Judith Lane,” also posted two Facebook advertisements for the sale of automobiles.
- Cernat and his coconspirators sent victims invoices that appeared to be from eBay Motors and provided an eBay Motors Support Department phone number and email address of ebay@processing-secure.com. These invoices provided instructions for payment and included reassuring language for secure transactions, such as, “Through OneVanilla Prepaid Visa services we can guarantee you 100 percent protection and insurance in this transaction. eBay Payments will secure the payment until the buyer receives, inspects, and accepts the item. Or, if it will be the case, eBay will refund the payment to the buyer.”
- Păiuși also convinced victims to send money for the advertised goods by sending them invoices for payment that appeared legitimate. ... [One such] invoice appeared to be sent from “eBay™ Buyer Protection,” provided the victim with an email address for questions, described the seller as a “certified eBay™ third-party seller,” and explained that the buyer will be refunded if he or she refuses the merchandise.
- The coconspirators then communicated with the victims via email, often signing their emails by posing as a member of the military, like “Sgt. Logan Burdick.” Other emails purported to be from the online auction company, like eBay. The emails often communicated convincing information about the item being sold and the reason payment was required before shipping or viewing the item.

Adrian Mitan, who was charged in the July 5, 2018 indictment, was also charged in a separate indictment unsealed today with money laundering offenses arising from a credit card phishing and brute-force attack scheme, likewise designed to steal money from Americans. The indictment explains that phishing is an attempt to acquire personal information by masquerading as a trustworthy entity through electronic communications, and brute force is a cryptological trial-and-error methodology used to obtain information such as personal identification numbers for credit cards. Mitan allegedly phished for credit/debit card information of U.S. customers, hacked into the electronic systems of American businesses, and then conducted a brute force attack on their point-of-sale systems for the purpose of stealing the remaining credit/debit card information. According to the indictment, Mitan then directed American money launderers to create “dummy” credit/debit cards with the stolen information, which were used to extract

money from the customers' accounts. These fraudulent proceeds were then returned to Mitan in the form of bitcoin.

The investigation was conducted by the U.S. Secret Service, Kentucky State Police, Lexington Police Department, IRS Criminal Investigation and U.S. Postal Inspection Service, and supported by the Justice Department's Organized Crime Drug Enforcement Task Forces (OCDETF) and the International Organized Crime Intelligence and Operations Center (IOC-2). Assistance was provided by the Romanian National Police (Service for Combating Cybercrime) and the Romanian Directorate for Investigating Organized Crime and Terrorism (Agency for Prosecuting Organized Crime). The Justice Department's Office of International Affairs provided significant support with the defendants' extradition. This case is being prosecuted by Assistant U.S. Attorneys Kathryn M. Anderson and Kenneth R. Taylor of the Eastern District of Kentucky and Senior Trial Attorney Timothy Flowers and Senior Counsel Frank Lin of the Criminal Division's Computer Crime and Intellectual Property Section with assistance from the Criminal Division's Money Laundering and Asset Recovery Section.

Individuals believing they may be victims of the advanced fee and online auction fraud or brute-force attack schemes described herein are encouraged to visit the following website to obtain more information: <https://justice.gov/usao-edky/information-victims-large-cases>. Tips to avoid becoming a victim of online auction fraud can be found [here](#) on the U.S. Secret Service's website.

For the RICO conspiracy and wire fraud conspiracy charges, each defendant faces up to 20 years in prison, a fine of \$250,000, and three years of supervised release. The same penalties apply to the money laundering conspiracy charges, except that the fine may be up to \$500,000. Additionally, if convicted of identity theft, Brown faces a term of 15 years in prison, a fine of \$250,000, and three years of supervised release, and if convicted of aggravated identity theft, those charged face a mandatory-minimum sentence of two years in prison, to be served consecutive to any term of imprisonment ordered for the other counts of conviction. However, any sentence following a conviction would be imposed by the Court, after its consideration of the U.S. Sentencing Guidelines and the federal statutes.

The charges in the indictment are merely allegations, and the defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

###

19-89

DO NOT REPLY TO THIS MESSAGE. IF YOU HAVE QUESTIONS, PLEASE USE THE CONTACTS IN THE MESSAGE OR CALL THE OFFICE OF PUBLIC AFFAIRS AT 202-514-2007.