Department of Justice

FOR IMMEDIATE RELEASE
THURSDAY, JUNE 11, 2020
WWW.JUSTICE.GOV

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

FIFTEEN DEFENDANTS PLEAD GUILTY TO RACKETEERING CONSPIRACY IN INTERNATIONAL CYBER FRAUD SCHEME

Guilty Pleas Include Owner of Romanian Bitcoin Exchange and Hacker Who Also Pleaded Guilty in Separate Phishing Scheme

WASHINGTON – Fifteen defendants have pleaded guilty to-date for their roles in a transnational and multi-million dollar scheme to defraud American victims through online auction fraud.

Four of the guilty pleas took place in the past 24 days before U.S. Magistrate Judge Matthew A. Stinnett of the U.S. District Court for the Eastern District of Kentucky.

Bogdan-Stefan Popescu, 30, of Romania, pleaded guilty on June 11, 2020, to one count of RICO conspiracy. According to plea documents, Popescu operated a car wash in Bucharest, Romania, where he managed coconspirators in the RICO enterprise. From at least December of 2013, Popescu oversaw an operation whereby he knowingly negotiated fraudulently obtained Bitcoin. He did so in many ways. For example, he would sometimes receive cryptocurrency from coconspirators who obtained the funds through online fraud scams, transfer the cryptocurrency to other conspirators such as codefendant Vlad-Călin Nistor. He would then direct that Nistor exchange the cryptocurrency for fiat currency, and deposit the fiat currency into bank accounts held in the names of various employees and family members. According to court documents, in addition to providing money laundering services, Popescu also coordinated the dissemination of tools used to defraud American-based victims, such as the language and photographs for fake advertisements as well as usernames and passwords for IP address anonymizing services. Popescu also assisted members of the RICO conspiracy by connecting them with other members who could provide call center services—that is, who would impersonate eBay customer service representatives over the phone.

Liviu-Sorin Nedelcu, 34, of Romania, pleaded guilty on June 11, 2020, to one count of RICO conspiracy. According to court documents, Nedelcu worked in conjunction with others to post advertisements for goods online. To maintain the appearance of legitimacy, Nedelcu created fictitious entities through which he purported to sell vehicles. Once Nedelcu and his coconspirators convinced victims to purchase falsely advertised goods, they sent the victims invoices for payment that appeared to be from legitimate sellers, such as eBay Motors. Upon

receiving payment, Nedelcu and his coconspirators engaged in a sophisticated money laundering scheme to convert the victim payment into Bitcoin.

Vlad-Călin Nistor, 33, of Romania, pleaded guilty on May 19, 2020, to one count of RICO conspiracy. According to plea documents, Nistor was the founder and owner of the Romania-based Bitcoin exchange Coinflux Services SRL. He exchanged cryptocurrency into local fiat currency on behalf of the Romania-based members of the conspiracy, knowing that the Bitcoin represented the proceeds of illegal activity. According to plea documents for example, Nistor exchanged over $1.8 million worth of Bitcoin for co-defendant Bogdan Popescu.

Beniamin-Filip Ologeanu, 30, of Romania, pleaded guilty on May 19, 2020, to one count of RICO conspiracy. According to court documents, Ologeanu worked in conjunction with others in the conspiracy to post advertisements for goods to auction websites, including eBay, and sales websites, including craigslist. Once Ologeanu or his coconspirators convinced victims to purchase and provide payment for falsely advertised items, Ologeanu reached out to U.S.-based conspirators to convert the victim payment into other forms of payment and transfer part of it to Ologeanu in Bitcoin. Ologeanu also purchased fraud proceeds from other coconspirators, typically in the form of prepaid debit cards, to be laundered by U.S.-based coconspirators.

"Today's modern cybercriminals rely on increasingly sophisticated techniques to defraud victims, often masquerading as legitimate businesses," said Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division. "These guilty pleas demonstrate that the United States will hold accountable foreign and domestic criminal enterprises and their enablers, including crooked bitcoin exchanges that swindle the American public."

"The guilty pleas announced today are a direct result of the extraordinary cooperation and partnership among law enforcement agencies at the local, state, federal, and international levels," said U.S. Attorney Robert M. Duncan Jr. for the Eastern District of Kentucky. "These partnerships helped dismantle a sophisticated organized crime group who preyed upon victims across the United States. I commend the exceptional work conducted by our law enforcement partners and trial team members who worked diligently to hold these defendants accountable."

"Through the use of digital currencies and trans-border organizational strategies, this criminal syndicate believed they were beyond the reach of law enforcement," said Assistant Director Michael D'Ambrosio, U.S. Secret Service, Office of Investigations. "However, as this successful investigation clearly illustrates, with sustained, international cooperation, we can effectively hold cyber criminals accountable for their actions, no matter where they reside. I commend the hard work and perseverance of all those who joined together in this investigation and prosecution. This includes our partners in Europe, as well as those closer to home."

"Today's guilty pleas serve as a reminder that IRS-CI special agents will uncover illegal activity here and abroad, pierce the perceived veil of anonymity provided by cryptocurrencies, and bring those responsible for unlawful acts to justice," said Special Agent in Charge Jonathan Larsen of the IRS-Criminal Investigations (IRS-CI) New York Field Office. "We will continue to push the agency to the forefront of complex cyber investigations and work collaboratively with our law enforcement partners to ensure the United States financial system is protected."

"These are scam artists who hide behind a wall of technology which allows them to prey upon innocent victims throughout the United States," said Kentucky State Police Commissioner Rodney Brewer. "The dismantling of this criminal enterprise was made possible because of the incredible level of cooperation between the law enforcement community here in Kentucky."

According to court documents, the defendants participated in a criminal conspiracy that engaged in a large-scale scheme of online auction fraud. Specifically, Romania-based members of the conspiracy 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. Members of the conspiracy 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.

According to court documents, members of the conspiracy created fictitious online accounts to post these advertisements and communicate with victims, often using the stolen identities of Americans to do so. They also delivered invoices to the victims bearing trademarks of reputable companies in order to make the transaction appear legitimate. Members of the conspiracy also set up call centers, impersonating customer support, to address questions and alleviate concerns over the advertisements.

Once victims were convinced to send payment, the conspiracy participants 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 money launderers.

The 15 defendants who have pleaded guilty in this case have yet to be sentenced. Two other defendants in the case are scheduled for trial starting on Sept. 14, 2020, before the Honorable Robert E. Wier of the U.S. District Court for the Eastern District of Kentucky. Three others are fugitives.

In addition to pleading guilty in this case, on Jan. 13, 2020, Adrian Mitan pleaded guilty in a related money laundering conspiracy, arising from online schemes, including a credit card phishing and brute-force attack scheme, designed to steal money from Americans. According to court documents, Mitan phished for payment 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 payment card information. Mitan then directed American money launderers to create clone payment 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 Criminal Division's Money Laundering and Asset Recovery Section provided significant support and the Criminal Division's Office of International Affairs provided significant support in securing and coordinating the arrests and extraditions from Romania of more than a dozen defendants.

This case is being prosecuted by Senior Trial Attorney Timothy C. Flowers and Senior Counsel Frank H. Lin of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorneys Kathryn M. Anderson and Kenneth R. Taylor of the U.S. Attorney's Office for the Eastern District of Kentucky.

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.

The year 2020 marks the 150th anniversary of the Department of Justice. Learn more about the history of our agency at www.Justice.gov/Celebrating150Years.

# # #

20-536