

Name: Alert ID: TMML2024031849261 A criminal complaint was unsealed today in federal court in Brooklyn charging Lithuanian national Vytautas Parfionovas with computer intrusion, securities fraud, money laundering, bank fraud and wire fraud, among other offenses. The charged crimes stem from a variety of criminal conduct between 2011 and 2018 in which Parfionovas gained access to U.S.-based computers, including email servers and computers belonging to U.S. financial institutions, in order to steal money from online bank accounts and securities brokerage accounts. Parfionovas was arrested in Ukraine on October 24, 2019, and was extradited to the United States on November 21, 2019. Richard P. Donoghue, United States Attorney for the Eastern District of New York, and William F. Sweeney, Jr., Assistant Director-in-Charge, Federal Bureau of Investigation, New York Field Office (FBI), announced the charges. "As alleged, the defendant and his co-conspirators stole millions of dollars from U.S. victims while sitting behind keyboards thousands of miles away," stated United States Attorney Donoghue. "Cybercriminals are hereby on notice that no amount of distance or subterfuge will protect them, and that we and our law enforcement partners are committed to unmasking, arresting and prosecuting them." Mr. Donoghue thanked the Prosecutor General's Office of Ukraine, the FBI Legal Attaché's Office in Kiev, the Department of Justice's Office of International Affairs and the National Cyber Forensic Training Alliance for their assistance in the investigation and the defendant's extradition. "The world has become a much smaller place with the advent of the internet, and with that shrinking globe, the days of cyber criminals thinking because they're not in our country they can escape justice are over," stated FBI Assistant Director-in-Charge Sweeney. "Our extraordinary partnerships allow the FBI to reach into many of the dark corners where these thieves feel invincible. If you violate our laws, we will make sure you pay the price." As charged in the criminal complaint, starting in January 2011, Parfionovas and his co-conspirators engaged in a long-running scheme to steal money through a variety of computer intrusions. In one part of the scheme, Parfionovas and his co-conspirators allegedly obtained login information for victims' securities brokerage accounts through various methods, including stealing that information from the server of a U.S. securities order management company to which the conspirators gained unauthorized access. The conspirators then used those accounts to steal money and conduct trades to their own benefit. Initially, conspirators accessed the victim brokerage accounts and transferred money from those accounts to other accounts under their control. After financial institutions began to block those unauthorized transfers, Parfionovas and his co-conspirators accessed other victim brokerage accounts without authorization, and placed unauthorized stock trades within those accounts while simultaneously trading profitably in the same stocks from accounts that they controlled. On or about February 22, 2016, Parfionovas explained this aspect of the scheme to a co-conspirator as follows: "I take some fraud logins. Do some s[ ]t with stock . . . sometimes 2-3 in day . . . manipulation is 100%." In this manner, Parfionovas and his co-conspirators realized financial gains while causing losses of more than \$5.5 million. In another part of the scheme, Parfionovas and his co-conspirators allegedly obtained login information for victim email accounts and accessed those accounts without authorization. The conspirators then sent email messages from those accounts to the victims' financial advisers and requested wire transfers from the victims' financial institutions to overseas bank accounts that the conspirators controlled. For example, in or about May 2013, Parfionovas and his co-conspirators obtained \$50,000 from an investment account that belonged to U.S. victims, and Parfionovas directed the transfer of those funds to a series of bank accounts and ultimately to an individual in Kharkov, Ukraine, where Parfionovas was located. To defraud another victim, Parfionovas and his co-conspirators obtained control over a victim's email account and used it to send written instructions—which falsely appeared to have been signed by the victim—to transfer \$225,000 from one of the victim's accounts. If convicted, the defendant faces up to 30 years' imprisonment for the money laundering charge, and a mandatory consecutive two-year sentence for the charge of aggravated identity theft. The charges in the complaint announced today are allegations, and the defendant is presumed innocent unless and until proven guilty. The government's case is being handled by the Office's National Security and Cybercrime Section and the Business and Securities Fraud Section. Assistant United States Attorneys David K. Kessler, Mark E. Bini and Alexander Mindlin are in charge of the prosecution. The Justice Department's Office of International Affairs of the Department's Criminal Division provided significant assistance in securing the defendant's extradition from Ukraine. VYTAUTAS PARFIONOVAS Age: 32 Kiev, Ukraine E.D.N.Y. Docket No.

19-MJ-883