

Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin ‘Mixer’ That Laundered Over \$300 Million

[justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million](https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million)



Press Release

Wednesday, August 18, 2021

For Immediate Release

Office of Public Affairs

An Ohio man pleaded guilty today to a money laundering conspiracy arising from his operation of Helix, a Darknet-based cryptocurrency laundering service.

According to court documents, Larry Dean Harmon, 38, of Akron, admitted that he operated Helix from 2014 to 2017. Helix functioned as a bitcoin “mixer” or “tumbler,” allowing customers, for a fee, to send bitcoin to designated recipients in a manner that was designed to conceal the source or owner of the bitcoin. Helix was linked to and associated with “Grams,” a Darknet search engine also run by Harmon. Harmon advertised Helix to customers on the Darknet to conceal transactions from law enforcement.

“By holding Harmon accountable, the department has disrupted the unlawful money laundering practices of these dangerous criminal enterprises,” said Assistant Attorney General Kenneth A. Polite Jr. of the Justice Department’s Criminal Division. “The Justice Department, together with our law enforcement and regulatory partners, will continue to take enforcement actions to identify and impede those who use illicit means for financial gain, as well as those who use the Darknet to facilitate and obscure their criminal conduct.”

“Darknet markets and the dealers who sell opioids and other illegal drugs on them are a growing scourge,” said Acting U.S. Attorney Channing D. Phillips for the District of Columbia. “They may try to hide their identities and launder millions in sales behind technologies like Helix. But the department and its law enforcement partners will shine a light on their activities, dismantle the infrastructure such criminal marketplaces depend on, and prosecute and convict those responsible.”

“Criminals may think they can mask financial transactions by using services like Helix to conceal the source of illicit funds,” said Assistant Director Calvin A. Shivers of the FBI’s Criminal Investigative Division. “The FBI and our state, local, federal and international law enforcement partners are working together every day in a complex and ever-changing digital environment to protect the American people from sophisticated money launderers and financiers.”

“The Darknet is driven in part by the criminal marketplaces which peddle their nefarious goods and services,” said Chief James C. Lee of the IRS Criminal Investigation. “But these marketplaces thrive in large measure because of the infrastructure that supports them. Harmon profited by facilitating the back-channel support of these marketplaces and helped criminals launder money they received via illicit activities. He then hid those funds from the government. He admitted his role today in these activities and will now be held accountable.”

“Harmon admitted that he conspired with Darknet vendors to launder bitcoin generated through drug trafficking and other illegal activities,” said Assistant Director in Charge Steven M. D’Antuono of the FBI’s Washington Field Office. “Today’s guilty plea demonstrates the FBI’s commitment to infiltrate and shut down the cryptocurrency money-laundering networks that support cyber-criminal enterprises.”

Harmon admitted that Helix partnered with several Darknet markets, including AlphaBay, Evolution, Cloud 9 and others, to provide bitcoin money laundering services for market customers. In total, Helix moved over 350,000 bitcoin – valued at over \$300 million at the time of the transactions – on behalf of customers, with the largest volume coming from Darknet markets. Harmon further admitted that he conspired with Darknet vendors and marketplace administrators to launder such bitcoins generated through illegal drug trafficking offenses on those Darknet marketplaces.

As part of his plea, Harmon also agreed to the forfeiture of more than 4,400 bitcoin, valued at more than \$200 million at today’s prices, and other seized properties that were involved in the money laundering conspiracy. Harmon will be sentenced at a date to be determined and faces a maximum penalty of 20 years in prison, a fine of \$500,000 or twice the value of the property involved in the transaction, a term of supervised release of not more than three years, and mandatory restitution. Chief Judge Beryl Howell of the U.S. District Court for the District of Columbia accepted Harmon’s guilty plea and will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

The IRS-CI Cyber Crimes Unit and the FBI’s Washington Field Office investigated the case, with valuable assistance provided by the Criminal Division’s Office of International Affairs, the U.S. Attorney’s Office for the Northern District of Ohio, the IRS’s Washington, Cincinnati and Oakland Field Offices, the FBI’s Criminal Investigative Division and Cleveland, Newark and San Francisco Field Offices, and the State Department’s Diplomatic Security Service.

The Belize Ministry of the Attorney General and the Belize National Police Department provided essential support for the investigation, coordinated through U.S. Embassy Belmopan. The investigation was coordinated with the Financial Crimes Enforcement Network, which assessed a \$60 million civil monetary penalty against Harmon in a parallel action.

Trial Attorneys S. Riane Harper and C. Alden Pelker of the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) and Assistant U.S. Attorney Christopher B. Brown of the U.S. Attorney's Office for the District of Columbia prosecuted the case. Additional assistance was provided by Trial Attorneys Emily Siedell and Brian Nicholson of the Criminal Division's Office of International Affairs, former CCIPS Trial Attorney W. Joss Nichols and Assistant U.S. Attorney Daniel Riedl of the Northern District of Ohio.

Updated August 18, 2021

Topic

Cybercrime

Press Release Number: 21-782