Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack

Press Release

Monday, March 2, 2020

For Immediate Release
Office of Public Affairs

Forfeiture Complaint Details Over $250 Million Stolen by North Korean Actors

Two Chinese nationals were charged with laundering over $100 million worth of cryptocurrency from a hack of a cryptocurrency exchange. The funds were stolen by North Korean actors in 2018, as detailed in the civil forfeiture complaint also unsealed today.

In the two-count indictment unsealed today in the District of Columbia, 田寅寅 aka Tian Yinyin, and 李家东 aka Li Jiadong, were charged with money laundering conspiracy and operating an unlicensed money transmitting business.

“These defendants allegedly laundered over a hundred million dollars worth of stolen cryptocurrency to obscure transactions for the benefit of actors based in North Korea,” said Assistant Attorney General Brian A. Benczkowski of the Justice Department’s Criminal Division. “Today's actions underscore that the Department will pierce the veil of anonymity provided by cryptocurrencies to hold criminals accountable, no matter where they are located.”

“Today, we are publicly exposing a criminal network’s valuable support to North Korea’s cyber heist program and seizing the fruits of its crimes,” said Assistant Attorney General John C. Demers of the Justice Department’s National Security Division. “This case exemplifies the commitment of the United States

government to work with foreign partners and the worldwide financial services industry to disrupt this blended threat."

"The hacking of virtual currency exchanges and related money laundering for the benefit of North Korean actors poses a grave threat to the security and integrity of the global financial system," said U.S. Attorney Timothy J. Shea of the District of Columbia. "These charges should serve as a reminder that law enforcement, through its partnerships and collaboration, will uncover illegal activity here and abroad, and charge those responsible for unlawful acts and seize illicit funds even when in the form of virtual currency."

"North Korea continues to attack the growing worldwide ecosystem of virtual currency as a means to bypass the sanctions imposed on it by the United States and the United Nations Security Council. IRS-CI is committed to combatting the means and methods used by foreign and domestic adversaries to finance operations and activities that pose a threat to U.S. national security," said Internal Revenue Service-Criminal Investigation (IRS-CI) Chief Don Fort. "We will continue to push our agency to the forefront of complex cyber investigations and work collaboratively with our law enforcement partners to ensure these nefarious criminals are stopped and that the integrity of the United States financial system is preserved."

"The FBI will continue to actively work with our domestic and international law enforcement partners to identify and mitigate illicit movement of currency," said Assistant Director Calvin Shivers of the FBI's Criminal Investigative Division. "Today's indictment and sanctions send a strong message that the United States will not relent in holding accountable bad actors attempting to evade sanctions and undermine our financial system."

"This case shows how important robust partnerships across the U.S. Government are in disrupting criminal actors," said Acting Assistant Director Robert Wells of the FBI's Counterintelligence Division.

"This indictment shows what can be accomplished when international law enforcement agencies work together to uncover complex cross-border crimes," said Acting Executive Associate Director Alysa Erichs of U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI). "HSI is committed to upholding the rule of law and investigating those that would steal cryptocurrency for their illicit purposes."

According to the pleadings, in 2018, North Korean co-conspirators hacked into a virtual currency exchange and stole nearly $250 million worth of virtual currency. The funds were then laundered through hundreds of automated cryptocurrency transactions aimed at preventing law enforcement from tracing the funds. The North Korean co-conspirators circumvented multiple virtual currency exchanges' know-your-customer controls by submitting doctored photographs and falsified identification documentation. A portion of the laundered funds was used to pay for infrastructure used in North Korean hacking campaigns against the financial industry.

The pleadings further allege that between December 2017 and April 2019, Yinyin and Jiadong laundered over $100 million worth of virtual currency, which primarily came from virtual currency exchange hacks. The defendants operated through independent as well as linked accounts and provided virtual currency

transmission services for a fee for customers. The defendants conducted business in the United States but at no time registered with the Financial Crimes Enforcement Network (FinCEN).

The pleadings further allege that the North Korean co-conspirators are tied to the theft of approximately $48.5 million worth of virtual currency from a South Korea-based virtual currency exchange in November 2019. As with the prior campaign, the North Korean co-conspirators are alleged to have laundered the stolen funds through hundreds of automated transactions and submitted doctored photographs and falsified identification documentation. The pleadings identify how the North Korean co-conspirators used infrastructure in North Korea as part of this campaign.

The civil forfeiture complaint specifically names 113 virtual currency accounts and addresses that were used by the defendants and unnamed co-conspirators to launder funds. The forfeiture complaint seeks to recover the funds, a portion of which has already been seized.

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

Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) also imposed sanctions on Yinyin, Liadong, and numerous cryptocurrency addresses related to their involvement in activities facilitating North Korean sanctions evasion based on their services and support for malicious cyber enabled activities linked to North Korean actors.

The investigation was led by the IRS-CI, the FBI, and HSI. The Korean National Police of the Republic of Korea provided assistance and coordinated with their parallel investigation.

The cases are being handled by Trial Attorney C. Alden Pelker of the Criminal Division's Computer Crime and Intellectual Property Section, Trial Attorney David Recker of the National Security Division's Counterintelligence and Export Control Section, and Assistant U.S. Attorneys Zia Faruqui and Christopher B. Brown, Paralegal Specialists Brian Rickers, and Legal Assistant Jessica McCormick of the U.S. Attorney's Office for the District of Columbia. Additional assistance has been provided by former Assistant U.S. Attorney Youli Lee.

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.

Updated July 22, 2022

Topics

Export Control

Cybercrime

Financial Fraud

Press Release Number: 20-255