

# Treasury Sanctions Russian Cyber Actors for Virtual Currency Theft

September 16, 2020

**Washington** - Today, in a coordinated action with the U.S. Department of Justice and the U.S. Department of Homeland Security, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned two Russian nationals for their involvement in a sophisticated phishing campaign in 2017 and 2018 that targeted customers of two U.S.-based and one foreign-based virtual asset service providers. American citizens and businesses were among the victims of this malicious cyber-enabled activity, which resulted in combined losses of at least \$16.8 million.

"The individuals who administered this scheme defrauded American citizens, businesses, and others by deceiving them and stealing virtual currency from their accounts," said Secretary Steven T. Mnuchin. "The Treasury Department will continue to use our authorities to target cybercriminals and remains committed to the safe and secure use of emerging technologies in the financial sector."

**Danil Potekhin** (Potekhin) and **Dmitrii Karasavidi** (Karasavidi) are being designated pursuant to Executive Order (E.O.) 13694, as amended by E.O. 13757, which targets malicious cyber-enabled activities, including those related to the significant misappropriation of funds or personal identifiers for private financial gain. Potekhin and Karasavidi are also the subjects of an indictment unsealed today by the Department of Justice.

Potekhin created numerous web domains that mimicked those of legitimate virtual currency exchanges. This tactic, known as spoofing, exploits Internet users' trust in known companies and organizations to fraudulently obtain their personal information. When unwitting customers accessed Potekhin's spoofed websites and entered their login information, Potekhin and his accomplices stole their login credentials and gained access to their real accounts. The attackers then employed a variety of methods to exfiltrate their ill-gotten virtual currency: using exchange accounts created using fictitious or stolen identities; circumventing exchanges' internal controls; swapping into different types of virtual currency; moving virtual currency through multiple intermediary addresses; and a market

manipulation scheme in which inexpensive virtual currency was purchased at a fast rate to increase demand and price, then quickly sold for a higher price to glean quick profit. Karasavidi laundered the proceeds of the attacks into an account in his name. He attempted to conceal the nature and source of the funds by transferring them in a layered and sophisticated manner through multiple accounts and multiple virtual currency blockchains. Ultimately, the stolen virtual currency was traced to Karasavidi's account, and millions of dollars in virtual currency and U.S. dollars was seized in a forfeiture action by the United States Secret Service.

Potekhin and Karasavidi's actions underscore the evolving threat that global financial institutions face from cybercriminals, who employ a variety of sophisticated schemes to profit at their victims' expense.


OFAC closely coordinated today's action with the United States Secret Service's San Francisco Field Office and with the U.S. Attorney's Office for the Northern District of California. Treasury is committed to collaborating with law enforcement to respond to evolving threats from malicious actors who exploit virtual currencies and target legitimate virtual asset service providers and their customers.

"Since its inception in 1865 to combat U.S. currency counterfeiting, the Secret Service has remained committed to safeguarding the Nation's financial infrastructure. The Secret Service mission has evolved to combat cyber fraud by tracing and seizing fraudulently obtained virtual currencies. These recent actions highlight the efforts of law enforcement to provide attribution to cybercriminals wherever they may reside," said Special Agent in Charge David Smith, U.S. Secret Service Criminal Investigative Division.

Today's action demonstrates the important role that a robust anti-money laundering and countering the financing of terrorism (AML/CFT) regime plays in deterring cybercrimes. As Potekhin and Karasavidi resorted to complex schemes to circumvent exchanges' compliance controls, they created a trail of evidence that helped investigators to identify them and hold them accountable. Because profit-motivated cybercriminals must launder their misappropriated funds, AML/CFT regimes pose a critical chokepoint in countering and deterring this criminal activity. The United States will continue to lead in AML/CFT regulation and supervision of digital assets to prevent their misuse by illicit actors.

[View identifying information on the individuals designated today.](#)

As a result of today's action, all property and interests in property of the designated persons that are in the possession or control of U.S. persons or within or transiting the United States are blocked, and U.S. persons generally are prohibited from dealing with them.

For additional information regarding illicit activity involving virtual currency, please see the [May 2019 FinCEN advisory](#) .