Treasury Continues Campaign to Combat Ransomware As Part of Whole-of-Government Effort

October 15, 2021

OFAC Issues Sanctions Compliance Guidance for Virtual Currency Industry

FinCEN Issues Report on Ransomware Trends in Bank Secrecy Act Data

WASHINGTON – Building on the first-ever designation of a virtual currency exchange for facilitating transactions for ransomware actors, the U.S. Department of the Treasury announced additional steps today to help the virtual currency industry prevent exploitation by sanctioned persons and other illicit actors. These actions are part of the Biden Administration's focused, integrated effort to counter the ransomware threat. New industry-specific guidance outlines sanctions compliance best practices tailored to the unique risks posed in this dynamic space, while new data from the Financial Crimes Enforcement Network (FinCEN) shows the increasing threat ransomware posed to the U.S financial sector, businesses, and the public during the first half of 2021. Treasury's actions underscore the need for a collaborative approach to counter ransomware attacks, including public-private partnerships and close relationships with international partners. "Ransomware actors are criminals who are enabled by gaps in compliance regimes across the global virtual currency ecosystem," said Deputy Secretary of the Treasury Wally Adeyemo. "Treasury is helping to stop ransomware attacks by making it difficult for criminals to profit from their crimes, but we need partners in the private sector to help prevent this illicit activity."

The private sector plays a key role by implementing appropriate sanctions and anti-money laundering/countering the financing of terrorism (AML/CFT) controls to prevent sanctioned persons and other illicit actors from exploiting virtual currencies and undermining U.S. foreign policy and national security interests. Treasury will continue its engagement with the private sector and other countries to disrupt and hold accountable ransomware actors and their money laundering networks.

Sanctions Compliance Guidance for the Virtual Currency Industry

As ransomware attacks have increased in recent years, so has the number of ransomware payments, which have been typically paid through virtual currency. Today, the Treasury

Department's Office of Foreign Assets Control (OFAC) issued a brochure to promote sanctions compliance in the virtual currency industry.

The growing prevalence of virtual currency as a payment method brings greater exposure to sanctions risks—like the risk that a sanctioned person or a person in a sanctioned jurisdiction might be involved in a virtual currency transaction. Accordingly, the virtual currency industry plays an increasingly critical role in preventing sanctioned persons from exploiting virtual currencies.

OFAC sanctions compliance requirements apply to the virtual currency industry in the same manner as they do to traditional financial institutions, and there are civil and criminal penalties for failing to comply. The guidance issued by OFAC today provides an overview of OFAC sanctions requirements and provides examples of compliance best practices for operators in this space, including technology companies, exchangers, administrators, miners, and wallet providers, as well as more traditional financial institutions that may have exposure to virtual currencies or their service providers. Industry participants should consider incorporating the elements and controls outlined in the brochure into their sanctions compliance programs. If ignored or mishandled, sanctions risks are vulnerabilities that can lead to violations and subsequent enforcement actions, as well as harm U.S. foreign policy and national security interests.

OFAC is publishing this guidance as part of its commitment to engage with the virtual currency industry to promote compliance with sanctions requirements.

Ransomware Trends in Bank Secrecy Act Data

FinCEN is also publishing Ransomware Trends in Bank Secrecy Act data today. The Anti-Money Laundering Act of 2020 (AMLA) mandates that FinCEN publish threat pattern and trend information derived from financial institutions' Suspicious Activity Reports (SARs). This first report issued pursuant to the AMLA focuses on pattern and trend information pertaining to ransomware, in line with FinCEN's issuance of government-wide priorities for AML/CFT policy. FinCEN analysis of ransomware-related SARs filed during the first half of 2021 further establishes that ransomware is a significant threat to the U.S. financial sector, businesses, and the public. FinCEN's analysis of ransomware-related SARs highlights average ransomware payment amounts, prevalent ransomware variants, and prominent ransomware money laundering typologies:

Average Monthly Ransomware Payment Amount: The average amount of reported ransomware transactions per month in 2021 was $102.3 million.
Prevalent Ransomware Variants: FinCEN identified 68 different ransomware variants reported in SAR data for transactions occurring between January 1, 2021 and June 30, 2021. The most commonly reported variants were REvil/Sodinokibi, Conti, DarkSide, Avaddon, and Phobos.

- *Ransomware Money Laundering Typologies:* FinCEN identified several money laundering typologies common among ransomware variants in 2021, including threat actors increasingly requesting payments in Anonymity-Enhanced Cryptocurrencies such as Monero, and avoiding reusing wallet addresses, "chain hopping" and cashing out at centralized exchanges, and using mixing services and decentralized exchanges to convert proceeds.

Click here for OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry.

Click here for FinCEN's Ransomware Trends in Bank Secrecy Act Data.

For More Information on Ransomware

Please visit StopRansomare.gov, a one-stop resource for individuals and organizations of all sizes to reduce their risk of ransomware attacks and improve their cybersecurity resilience. This webpage brings together tools and resources from multiple federal government agencies under one online platform. Learn more about how ransomware works, how to protect yourself, how to report an incident, and how to request technical assistance.

###