FiveBy

ADVISORY

Treasury Sanctions Review Flags Virtual Currency Risks

The Treasury Department's long-awaited sanctions review offered few specifics into how the Biden administration's sanctions regime is going to change. The brief document provides general insight into OFAC's approach toward designations, namely stepping away from maximum pressure campaigns and improving coordination with government and private-sector stakeholders, such as foreign allies and partners. However, the review does specifically highlight the sanctions compliance risks of virtual currencies, which appears to be a priority for the administration in light new guidance for the virtual currency industry published this month.

The short review document outlines the steps to modernize sanctions: linking designations to clear government policy objectives that fit into a broader government strategy; using analytic resources to ensure that the designations are the right tool to pursue broader US policy objectives; assessing and mitigating possible consequences that can impact individuals and entities outside the intended targets; multilateral coordination with allies and partners, as well as government stakeholders; and making sanctions easily enforceable and reversable when possible.

- Treasury did specifically flag digital currencies, alternative payment platforms, and other tech tools that allow malign actors to obscure cross-border transactions by operating outside the dollar-dominated global financial system, curtailing the efficacy of US sanctions. In addition, new technologies would also allow adversaries to develop payment systems that would diminish the dollar's role as the world's reserve currency.

Deputy Treasury Secretary Wally Adeyemo in a recent online event hosted by the Center for a New American Security, acknowledged that most transactions in the virtual currency space are legitimate and highlighted the importance of targeting crypto exchanges that are "fundamentally in the business of furthering" cyber-criminal activity. The recent Treasury designation of SUEX exchange highlighted that analysis of known transactions shows that more than 40 percent of the company's activities are associated with illicit actors and that SUEX has facilitated financial transfers linked to at least eight ransomware variants.

- Although US firms are required to deny all blocked parties access to virtual currencies, they are not obligated to convert the blocked virtual funds into fiat currencies, nor are they required to hold these currencies in an interest-bearing account. OFAC emphasizes that any company active in the virtual currency space should make cybersecurity a priority and ensure effective sanctions compliance tools that use all available information to mitigate the risk of sanctioned individuals who seek to exploit virtual currencies gaining access to the US financial system.

- OFAC's list of best practices for the virtual currency industry matches the best practices the agency recommends for all US persons and entities: a risk-based approach that will depend on the type of business, its size and sophistication, the products and services it offers, the customers and counterparties with whom it transacts, and the geographic locations it serves. Sanctions list and geographic screening should be the minimum measures taken by firms active in the virtual currencies space.

INFO@FIVEBY.COM
206-800-1700
FIVEBY.COM

In late 2020, OFAC reached a settlement agreement with technology company BitGo, that offers non-custodial secure digital wallet management services, for 183 apparent violations of multiple sanctions programs. BitGo tracked its users' IP addresses during the time the violations occurred but did not use the IP information for sanctions compliance purposes to detect possible risky jurisdictions. FiveBy experts can help identify jurisdictional risks by examining IP address data, as well as perform periodic analysis of firms' ecosystems to ensure any inadvertent violations are identified and reported.

OFAC also advises that the use of geolocation tools and IP address blocking technologies, such as Chainalysis, can help prevent IP addresses in sanctioned or embargoed jurisdictions from accessing virtual currencies. Analytic tools can also help identify IP misattribution by screening IP addresses against known virtual private network (VPN) IP addresses and identifying suspicious and shared logins. In addition, an examination of email addresses or invoices can help identify customers or counterparties in sanctioned or risky jurisdictions. FiveBy's regional and linguistic experts and data analysts can also help evaluate information contained in email addresses and other identifying data provided by customers and counterparties to determine their possible connections to sanctioned entities or jurisdictions and identify possible violations or risky transactions.