Thursday, October 28, 2021

Recently, the Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Treasury Department, released a report on ransomware trends stating that during the first half of 2021, 68 different ransomware variants extracted approximately $600 million from victims across the country. FinCEN identified Bitcoin as the most common ransomware-related payment method in reported transactions and noted that ransomware incidents requesting Monero (XMR) – what FinCEN refers to as an anonymity-enhanced cryptocurrency – are increasing as hackers seek to reduce the transparency and traceability of such transactions.
Given this environment, the White House and Treasury Department have sought to counter the ransomware threat by taking a number of actions, including holding a virtual two-day multinational summit on ransomware, conducting classified threat briefings for critical infrastructure executives, and establishing some expected cybersecurity thresholds for critical infrastructure providers. Compounding these efforts, the Treasury Department is leveraging existing Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) controls that already apply to fiat currency and enforcing them more deliberately toward virtual currency to combat ransomware attacks.

Two days after the White House issued its October 13, 2021 Fact Sheet detailing these anti-ransomware efforts, the Treasury Department’s Office of Foreign Assets Control (OFAC) issued its “Sanctions Compliance Guidance for the Virtual Currency Industry” (“Guidance”).

In the new Guidance, OFAC noted that the virtual currency industry, which includes technology companies, exchanges, miners, wallet providers, service providers and users, plays an increasingly critical role in preventing sanctioned persons from using virtual currencies to evade sanctions and harm national security, and that OFAC sanctions apply equally to entities in the virtual currency industry and traditional financial institutions. OFAC also reiterated that members of the virtual currency industry are responsible for ensuring that they do not engage, directly or indirectly, in transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade- or investment-related transactions. This means that once an entity determines it holds a virtual currency on behalf of a sanctioned person or entity, country, region, or government, such as by administering to a sanctioned person’s digital wallet, that entity must block access to that currency (i.e., deny all parties access to that virtual currency, comply with OFAC regulations related to the holding of and reporting of blocked assets and implement necessary controls). (See Treasury Department FAQ No. 646).[1]

OFAC’s Guidance summarizes these sanctions requirements and offers examples of best practices in how to bolster a sanctions compliance program that could help participants in the virtual currency industry avoid potential violations and enforcement actions. Last month, OFAC sanctioned SUEX OTC, S.R.O., a Russia-based virtual currency exchange, for allegedly facilitating transactions involving illicit proceeds from at least eight ransomware variants.

Although OFAC sanctions do not require that companies maintain an OFAC compliance program (in contrast to AML regulations), the Guidance makes clear that OFAC will consider a company’s implementation of a risk-based OFAC compliance program (and remedial measures taken in response to an apparent violation) when determining its enforcement response. That is important because OFAC sanctions apply with strict liability – so the only way to mitigate potential penalties, even where the violation is entirely inadvertent, is to implement compliance measures.

As outlined in the Guidance, OFAC recommends that an adequate sanctions compliance program should include management commitment, risk assessment, internal controls, testing and auditing, and training. [For further OFAC guidance on compliance measures, please see the Treasury Department’s “A Framework for OFAC]
Compliance Commitments”. OFACs recommendations include the following:

Management Commitment: Management can demonstrate commitment by reviewing and endorsing sanctions compliance policies and procedures, ensuring adequate resources support the compliance function and delegating sufficient autonomy to the compliance unit, as well as considering compliance early in the development process as opposed to after months after launch.

Risk Assessment: Best-practice risk assessment involves a routine (and, for some companies, ongoing) review of all of a company's touchpoints to foreign jurisdictions or persons, and may also include evaluating the compliance procedures of partners and counterparties.

Internal Controls: Companies should implement controls to identify, interdict, escalate, report (as appropriate), and maintain records for transactions or activities prohibited by OFAC-administered sanctions. This means conducting due diligence on customers, partners and transactions to identify red flags. OFAC recommends several specific controls, including:

- Geolocation and IP address blocking controls, which can prevent access by persons in sanctioned jurisdictions. Notably, the guidance suggests the use of analytics tools to prevent IP misattribution via a VPN, a common tool used to circumvent geographic restrictions.

- Know Your Customer (KYC) procedures, which involve gathering identity-verifying information such as date of birth, bank information, and government identification and documents.

- Transaction monitoring and investigation software, which can identify, flag and block transactions with persons or entities on OFAC's sanctions lists, including by referring to OFAC's list of known virtual currency addresses of sanctioned persons.

- Sanctions screening tools, which compare customer information against sanctions lists to discover potential links to sanctioned persons, and may also involve risk-based re-screening to account for updated customer information and changes to sanctions lists and regulatory requirements.

- Monitoring for red flags, which includes, among other things, new users providing incomplete KYC information (and non-responsiveness following a prompt for more information), attempts to access a virtual currency from an IP address or VPN connected to a sanctioned jurisdiction, attempts to transact with a virtual currency address associated with a sanctioned person or jurisdiction, and any behavior that indicates money laundering.

Testing and Auditing: OFAC’s Guidance notes that “[c]ompanies that incorporate a comprehensive, independent, and objective testing or audit function within their sanctions compliance program are equipped to ensure that they are aware of how their programs are performing.” Reviewing the functionality of implemented internal controls can help determine what aspects need to be updated, enhanced, or recalibrated.
Training: The Guidance recommends that compliance training be conducted annually at a minimum, communicate the sanctions compliance responsibilities for each employee, and hold employees accountable for meeting training requirements through the use of assessments.

Given the current threat environment and the high-profile ransomware attacks that have struck critical infrastructure providers in the past year, the Administration has made it a priority to combat ransomware attacks. By enforcing sanctions against companies and providers in the virtual currency industry (as well as traditional financial institutions that may have exposure to virtual currencies), the Treasury Department may hope to undercut the means by which ransomware attackers collect their ransoms, i.e., by blocking sanctioned criminals from accessing virtual funds. These enforcement efforts are consistent with the current regulatory environment, where government agencies are aggressively regulating the cryptocurrency industry using existing legal frameworks. Thus, virtual currency entities should reexamine and continually update existing sanctions compliance programs, and stay attuned to AML risks.

FOOTNOTES

[1] Beyond virtual currencies, such controls would also presumably include transactions involving digital tokens, such as non-fungible tokens (NFTs). This interpretation is echoed in a related Treasury Department FAQ (No. 559), which states that “virtual currency” is “a digital representation of value that functions as (i) a medium of exchange; (ii) a unit of account; and/or (iii) a store of value; and is neither issued nor guaranteed by any jurisdiction.”

© 2021 Proskauer Rose LLP.

National Law Review, Volume XI, Number 301