WINSTON & STRAWN LLP

BLOG

OFAC's Eye on Virtual Currencies – Cryptocurrency Regulation and Enforcement Updates

NOVEMBER 4, 2021

There is no doubt that United States regulators and government agencies have been paying close attention to the virtual currency industry over the past several years. In the past few months, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issued two publications highlighting its growing focus on the virtual currency industry. Specifically, on September 21, 2021, OFAC updated its Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, and just a few weeks later, on October 15, 2021, issued a brochure on Sanctions Compliance Guidance for the Virtual Currency Industry. The Treasury Department also recently commented on the digital asset space in its 2021 Sanctions Review. The Review discussed the possibility that typical sanctions may not be as effective in combating illegal transactions in the virtual currency space. In order to increase efficacy, the Treasury recognized that it should "invest in deepening its institutional knowledge and capabilities in the evolving digital assets and services space to support the full sanctions lifecycle of activities."

OFAC's September Advisory on Ransomware supersedes its October 2020 Advisory, although the overall guidance is fundamentally the same. Through this Advisory, OFAC confirms it is doubling down on its efforts to counter the rise of ransomware attacks that have become "more focused, sophisticated, costly, and numerous." In fact, OFAC compares the Federal Bureau of Investigation Internet Crime Reports from 2019 and 2020, finding that there was a nearly 21 percent increase in reported ransomware cases and a 225 percent increase in associated losses from 2019 to 2020. The Treasury's Financial Crimes Enforcement Network's (FinCEN) recent Financial Trend Analysis on ransomware relating to Bank Secrecy Act reporting shows a similar trend. The report examined ransomware-related Suspicious Activity Reports (SARs) filed between January 1 and June 30, 2021, which included a total of 635 reports and 458 confirmed transactions that, compiled, total over $590 million in suspected ransom payments, and found a 42% increase from the total ransomware payments identified by FinCEN in all of 2020.

Through its September 2021 Advisory, OFAC reminds companies that they are prohibited from engaging in financial transactions with persons identified on OFAC's Specially Designated Nationals and Blocked Persons (SDN) List and with persons located in sanctioned countries, including Cuba and Iran. OFAC has made clear that ransomware payments made to a sanctioned person or country are considered prohibited financial transactions (even if the victim of the ransomware attack was unaware of the sanctions nexus). OFAC also confirmed in its 2021 Advisory that it will consider a company's self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies, made as soon as possible after discovery of an attack, to be a voluntary self-disclosure and a significant mitigating factor in determining an appropriate enforcement response.

The updated Advisory emphasizes that OFAC is focusing its counter-ransomware strategy on certain virtual currency exchanges, which OFAC described as the "principal means of facilitating ransomware payments and associated money laundering activities." OFAC highlighted this position through its first-of-its-kind designation of virtual currency exchange Suex OTC, S.R.O. after determining its involvement in facilitating illicit transfers for at least eight ransomware groups. OFAC has imposed, and will continue to impose, sanctions on these actors and others who materially assist, sponsor, or provide financial, material, or technological support for these activities.

Similar to the updated Advisory, OFAC's October 15, 2021 Sanctions Compliance Guidance for the Virtual Currency Industry does not necessarily provide any novel information regarding U.S. sanctions compliance; however, it is designed to provide persons operating in the virtual currency sector with a greater understanding of their sanctions compliance obligations. The guide reiterates OFAC's prior guidance in the context of virtual currencies, including OFAC's expectation that a company's program should be risk-based and include management commitment, risk assessments, internal controls, testing/auditing, and training. It also provides useful clarifying information for "blocking" virtual currencies: "[o]nce a US person determines that they hold virtual currency that is required to be blocked pursuant to OFAC's regulations, the US person *must deny all parties* access to that virtual currency." Such blocked virtual currency must be reported to OFAC within 10 business days, and thereafter on an annual basis, so long as the virtual currency remains blocked. The Guidance also provides further "best practices" and advice for the virtual currency space, including information on geolocation, IP monitoring, transaction monitoring and investigation, blockchain analytics, and reporting of potential violations.

KEY TAKEAWAYS:

- Companies, especially those in the financial services industry, should review in detail the updated Advisory and Guidance and incorporate all highlighted best practices in future ransomware planning. This may include considering advanced protection technologies to prevent ransomware attacks in the first place.
- It is critical for companies to have a detailed ransomware response plan that addresses how to detect, mitigate, recover from, and report an attack. Such a plan might include company-specific considerations about any scenarios wherein the company may consider an exception to its no ransomware payments stance and paying a ransom. Companies must weigh the sanctions risk highlighted by OFAC as part of that assessment. In addition, companies involved in facilitating ransomware payments on behalf of victims should consider whether they have regulatory obligations under FinCEN regulations.
- Cryptocurrency exchanges may need to strengthen their Anti-Money Laundering (AML) and Know Your Customer (KYC) compliance programs to avoid the enabling of illicit activities such as allowing sanctioned persons to transact on their platforms. The Guidance reiterates that OFAC's expectations for risk-based sanctions compliance programs are applicable to the virtual currency industry.
- Companies must use information-gathering tools to identify and mitigate sanctions risks (for example, to determine the locations of IP addresses in order to identify any that are in sanctioned jurisdictions or appear on the SDN list). These tools should include basic geolocation and IP blocking, but companies should also consider adopting more advanced blockchain analytic solutions.
- This appears to be just the beginning of the government's attack on ransomware. For example, in recent weeks, the Department of Justice established a Ransomware and Digital Extortion Task Force and launched a one-stop ransomware resource at StopRansomware.gov. Additional OFAC action is expected.

4 Min Read

Authors

Dainia Jabaji

Lara Markarian

Cari Stinebower

Related Locations

Los Angeles | Washington, DC

Related Topics

Cryptocurrency | OFAC | Financial Services | International Trade

Related Capabilities

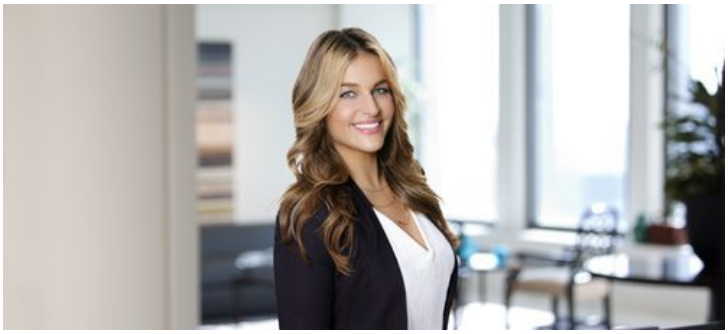
International Trade | Tax | Maritime & Admiralty | Financial Services | Cryptocurrencies, Digital Assets & Blockchain Technology

Related Regions

North America

Related Professionals

Cari Stinebower



Dainia Jabaji

Lara Markarian

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.