King & Spalding

Client Alert

Providing Strategic Legal Guidance to the Global Financial Services Industry

FINANCIAL SERVICES

OCTOBER 25, 2021

For more information, contact:

Jeffrey M. Telep
+1 202 626 2390
jtelep@kslaw.com

Christine Savage
+1 202 626 5541
csavage@kslaw.com

J.C. Boggs
+1 202 626 2383
jboggs@kslaw.com

Seth Atkisson
+1 202 626 9257
satkisson@kslaw.com

Adam Harper
+1 202 393 3799
arharper@kslaw.com

Taylor Green
+1 202 626 5601
tgreen@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

OFAC Puts Virtual Currency Industry On Notice

Guidance Demonstrates OFAC's Expectations for Sanctions Compliance by Cryptocurrency Industry

On October 15, 2021, the Office of Foreign Assets Control ("OFAC") of the U.S. Department of the Treasury published Sanctions Compliance Guidance for the Virtual Currency Industry (the "Guidance"). The Guidance puts the cryptocurrency industry on notice concerning OFAC's compliance expectations and comes amid ongoing efforts by the U.S. government to crack down on the use of cryptocurrencies for illicit purposes, including to avoid sanctions.[1]

The Guidance comes complete with an eye-catching color scheme and sleek graphics, clearly aimed at holding the attention of those otherwise unfamiliar with OFAC and its mission. In straightforward language, the Guidance explains the purpose and use of sanctions for the uninitiated, details best practices for sanctions compliance by the virtual currency industry, and gives resources for further study.

The virtual currency industry now has a prominent role in the global economy.[2] While the Biden administration recognizes the benefits of the virtual currency industry, concern has grown over the use of virtual currency for nefarious purposes such as ransomware and money laundering.[3] Furthermore, virtual currency's explosion in popularity has allowed rogue states and devious private actors to gain access to the financial system that they might not otherwise have.[4] As a result, the Financial Crimes Enforcement Network ("FinCEN") and OFAC have released several advisories to provide guidance relevant to the virtual currency industry, including on risks associated with facilitating ransomware payments, cyber security practices, and reporting suspect or blocked transactions.[5]

It is amid such concerns that OFAC has issued the Guidance. The expanded usage of virtual currency has made industry members a critical component in preventing sanctioned persons and countries from exploiting virtual currencies to evade sanctions and undermining U.S. foreign policy and national security interest.

In this environment of heightened awareness of the criminal uses of virtual currency, companies dealing with virtual currency should use the Guidance as a tool to ensure that their compliance program is in line with OFAC's expectations. The Guidance highlights that "**OFAC sanctions compliance obligations apply equally to transactions involving virtual currencies and those involving traditional fiat currencies**." Those dealing with virtual currencies should ensure that their sanctions compliance sufficiently covers the risk involved in their business model.

The Guidance provides substantial background information about U.S. sanctions, OFAC, and OFAC's authorities. Perhaps most importantly, the Guidance provides detailed information about best practices for the virtual currency industry to comply with U.S. sanctions. The Guidance provides the following best practices, which are further described in this alert:

- Management Commitment;
- Risk Assessment;
- Internal Controls;
- Testing/Auditing; and
- Training.

MANAGEMENT COMMITMENT

The Guidance states that management's commitment to a "company's sanctions compliance program is one of the most important factors in determining the program's success." OFAC recommends that virtual currency company management take the following steps to demonstrate their support for their company's compliance programs:

- Review and endorse sanctions compliance policies and procedures;
- Ensure adequate resources — including human capital, expertise, information technology, and other resources — support the compliance function and procedures;
- Delegate sufficient autonomy and authority to the compliance unit; and
- Appoint a dedicated sanctions compliance officer with the requisite technical expertise.

RISK ASSESSMENT

While the Guidance notes that there is no "one-size-fits-all" approach to risk assessments, the Guidance encourages companies in the virtual currency industry to "conduct a routine and, if appropriate, ongoing risk assessments to identify potential sanctions issues the company is likely to encounter." Furthermore, "OFAC encourages members of the virtual currency industry to **evaluate their exposure to OFAC sanctions and take steps to minimize their risks...prior to providing services or products to customers**." A risk assessment allows the company to understand and identify potential areas which may directly or indirectly engage with OFAC sanctioned persons, countries, or regions. According to the Guidance, the results of risk assessments are essential for developing effective policies, procedures, internal controls, and training to mitigate exposure to sanctions risk. The Guidance states that "[a]ppropriately customized risk assessments should reflect a company's customer or client base, products, services, supply chain, counterparties, transactions, and geographic locations, and may also include evaluating whether counterparties and partners have adequate compliance procedures."

INTERNAL CONTROLS

After a company conducts its risk assessment, the Guidance recommends that they implement internal controls to address the risks identified in the risk assessment. The Guidance states that the internal controls implemented by companies in

the virtual currency industry will depend on the company, but that an effective compliance program "will enable a company to conduct sufficient due diligence on customers, business partners, and transactions and identify 'red flags,'" which are indicators that illicit activities or breakdowns in compliance procedures may be occurring. The Guidance recommends the following internal controls tools, as appropriate:

- Geolocation tools and IP address blocking controls to "identify and prevent IP addresses that originate in sanctioned jurisdictions from accessing a company's website and services for activity that is prohibited by OFAC's regulations, and not authorized or exempt";
- Know Your Customer ("KYC") Procedures to obtain information about customers during onboarding and throughout the lifecycle of the customer relationship and use such information to conduct due diligence sufficient to mitigate potential sanctions-related risk;
- Transaction monitoring and investigation software to "identify transactions involving virtual currency addresses or other identifying information (*e.g.*, originator, beneficiary, originating and beneficiary exchanges, and underlying transactional data) associated with sanctioned individuals and entities";
- Implementing remedial measures to address discovered weaknesses in the company's compliance program;
- Sanctions screening of customer information against U.S. sanctions lists;
- Monitoring OFAC enforcement actions for the types of remedial measures that were required and may be useful for the company's compliance program; and
- Screening transactions for red flags that may indicate potential sanctions risks such as when customers provide inaccurate identification information or are hesitant to provide identification information.

TESTING AND AUDITING

The Guidance advises that testing a sanctions compliance program is the best means to determine whether it is effective. The Guidance notes that the size and sophistication of a company will determine the types of testing and auditing the company should perform, but the Guidance also states "[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 and what aspects need to be updated, enhanced, or recalibrated to account for a changing risk assessment or sanctions environment."

TRAINING

While the Guidance acknowledges that the training a company offers will be based on its size and sophistication, the Guidance states that "training should be provided to all appropriate employees, including compliance, management, and customer service personnel, and should be conducted on a periodic basis, and, at a minimum, annually." According to the Guidance, well-developed sanctions compliance training will provide "job-specific knowledge based on need, communicate the sanctions compliance responsibilities for each employee, and hold employees accountable for meeting training requirements through the use of assessments."

ADDITIONAL RESOURCES

Beyond the best practices overview provided by the Guidance, the document also includes a list of additional resources, guidance, and information from OFAC regarding virtual currencies. The Guidance points readers to OFAC's frequently asked questions ("FAQs") addressing the following topics:

- Definitions of digital currency, digital currency wallet, digital currency address, and virtual currency for purposes of OFAC's regulations;
- Understanding if OFAC compliance obligations are the same regardless of whether the transaction is in digital currency or traditional fiat;
- OFAC existing authorities to sanction those who use digital currencies for illicit purpose;
- OFAC process to identify digital currency information on SDN list;
- Structure of digital currency address on SDN list;
- Searching digital currency addresses on OFAC's sanctions List Search tool;
- Guidance to blocking virtual currency;
- Communicating with customers regarding blocked access to their digital currency;
- Venezuela FAQ regarding "Petro" or "Petro Gold";
- Venezuela FAQ regarding "Bolivar Fuerte"; and
- Venezuela FAQ discussing the ability to perform transactions in Venezuela's digital currency on or after March 19, 2018.

CONCLUSION

The U.S. government has demonstrated a strong determination to address illicit activities in which cryptocurrencies often play a large role, including ransomware attacks. U.S. government action to address its concerns about cryptocurrencies, including attention to the virtual currency industry from OFAC, will continue moving quickly and expanding. One senior White House official was recently reported as stating that "[t]he Biden administration is only beginning to ramp up regulatory scrutiny around cryptocurrencies."[6]

As part of addressing increased U.S. government scrutiny of the virtual currency industry, companies in the industry should review the recommendations in the Guidance, use the Guidance to assess their sanctions risks, and implement an appropriate sanctions compliance program.

[1] *See e.g.*, OFAC's recent sanctioning of virtual currency exchange SUEX OTC, S.R.O. (a.k.a. "SUCCESSFUL EXCHANGE"), available at: https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210921.
[2] *See* Office of Foreign Assets Control, Sanctions Compliance Guidance for the Virtual Currency Industry, 1 (Oct. 2021), available at: https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.
[3] *See* U.S. Department of Justice, Attorney General's Cyber Digital Task Force, *Cryptocurrency: Enforcement Framework*, 15 (Oct. 2020), available at: https://www.justice.gov/archives/ag/page/file/1326061/download.
[4] *See* Dylan Tokar, *Biden Administration Embarking on 'Aggressive' Tack for Cryptocurrency, White House Official Says*, WSJ (Oct. 12, 2021), available at: https://www.wsj.com/articles/biden-administration-embarking-on-aggressive-tack-for-cryptocurrency-white-house-official-says-11634077058.
[5] *See* U.S. Office of Foreign Assets Control, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Sept. 21, 2021), available at: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf; *see also* Financial Crimes Enforcement Network, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments,* #FIN-2020-A006 (Oct. 1, 2021) available at: https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.
[6] *Supra* n.4.