Virtually Consistent

OFAC Guidance for the Virtual Currency Industry

NOVEMBER 2021

AUTHORS:

Christopher Sidler
202.740.1307
csidler@thinkbrg.com

Debra Bonosconi
202.480.2756
dbonosconi@thinkbrg.com

Valtteri Tamminen
202.480.2772
vtamminen@thinkbrg.com

Dominic Zagara
212.782.1419
dzagara@thinkbrg.com

INTELLIGENCE THAT WORKS

BRG

On October 15, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) issued its first sanctions compliance guidance for the virtual currency industry.[1] The guidance highlights the Treasury Department's increased focus on virtual currencies and ransomware, both of which had been highlighted in the Financial Crimes Enforcement Network's (FinCEN) *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities* in June.[2] Both OFAC and FinCEN published ransomware advisories in October 2020, and OFAC sanctioned its first virtual currency exchange in September 2021 for facilitating ransomware payments.[3]

In this article, we discuss these focus areas and key takeaways for firms with virtual currency exposure based on OFAC's guidance.

Key takeaways

- **Consistency is key.** Though the document focuses on virtual currency–related sanctions compliance insights, OFAC reminds readers that sanctions requirements related to virtual currencies are the same as those on fiat currencies. OFAC refers to its earlier insights from the foundational 2009 Enforcement Guidelines and 2019 Framework for OFAC Sanctions Compliance Commitments.[4]
- **Stronger together.** OFAC's guidance has clarified that all virtual currency industry players have a role in preventing terrorism and other threats to national security. The covered entities include financial institutions, technology companies, exchanges, administrators, miners, wallet providers, and users.
- **Root cause remediation.** As the virtual currency industry evolves, there will be lessons learned by OFAC and the covered institutions. OFAC has made it clear that companies with virtual currency exposure should remediate the root causes of sanctions violations, and they should implement controls proactively to address weaknesses and prevent future violations.
- **Geolocation and IP blocking.** Firms with virtual currency exposure should prohibit users located in sanctioned jurisdictions from accessing their accounts. Strategies to do this may use, for example, geolocation tools to identify where users are located and IP blocking for sanctioned jurisdictions. OFAC stresses that all available information should be screened or otherwise incorporated into a sanctions compliance program.
- **VPN-ternal controls.** Firms with virtual currency exposure should be aware that specially designated nationals (SDNs) and users in sanctioned jurisdictions can use virtual private networks (VPNs) to hide their true locations and identities. OFAC has included updated guidance and expectations for covered institutions from Know Your Customer (KYC) (e.g., collecting IP addresses at onboarding) and screening perspectives (e.g., screening IP addresses against SDN sanctions lists).

---

1 OFAC, *Sanctions Compliance Guidance for the Virtual Currency Industry* (October 10, 2021). https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf

2 FinCEN, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities* (June 30, 2021). https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf

3 US Department of the Treasury, "Treasury Takes Robust Actions to Counter Ransomware," press release (September 21, 2021). https://home.treasury.gov/news/press-releases/jy0364

4 OFAC, *Economic sanctions enforcement guidelines, final* (November 9, 2009). https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20091109; and US Department of the Treasury, *A Framework for OFAC Compliance Commitments* (May 2, 2019). https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf

What firms should do

OFAC organized its virtual currency guidance using the same approach that it provided in its framework for OFAC compliance commitments: the five "essential components."[5] These components are key to understanding how OFAC views an effective sanctions compliance program and informs the office's enforcement response in the event that it becomes aware of an apparent violation.

1. **Management commitment.** Senior management should commit to supporting the compliance program and providing the resources that it needs to operate effectively. This includes:
   - Reviewing, approving, and endorsing the firm's compliance policies and procedures.
   - Appointing a dedicated sanctions compliance officer with the requisite technical expertise and sufficient autonomy and authority.
   - Ensuring that the program has adequate resources, including personnel, expertise, and technology.
2. **Risk assessment.** The risk-based approach is fundamental to an effective program. Risk assessments should identify areas in which a firm may engage with OFAC-sanctioned persons or geographies, considering the specific products and services that are offered. Companies with virtual currency exposure should identify these risks and implement the corresponding controls. For example, a risk assessment that includes understanding who is accessing a company's platform can help to determine appropriate screening standards for its products and services.

   Companies with established sanctions programs should include an evaluation of the compliance programs of new partners and counterparties in their risk assessment. The pseudonymous nature of virtual currencies underscores the need to mitigate counterparty risk, as the 2021 BitPay settlement with OFAC demonstrates.[6] These risks are even more heightened when dealing with anonymity enhanced cryptocurrencies (AECs), also known as "privacy coins," such as Monero or Zcash.

5 US Department of the Treasury, *A Framework for OFAC Compliance Commitments* (May 2, 2019). https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf

6 US Department of the Treasury, *OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions* (February 18, 2021). https://home.treasury.gov/system/files/126/20210218_bp.pdf

3. **Internal controls.** OFAC emphasized the need for risk-based internal controls around virtual currency addresses and reporting requirements.
    - Virtual currency addresses added to the SDN list must be blocked, but these designations can bring collateral risks. Association with a sanctioned address, such as another address on the same wallet, can pose added risk of dealing with a blocked person.
    - As with fiat currencies, initial blocked property reports for virtual currencies must be filed within ten days, and then annually in September. However, OFAC clarified that there is no need to convert blocked virtual currencies into fiat, nor to hold them in interest-bearing accounts.
    - Firms also should have processes in place to design and implement compensating controls in the event they identify a compliance failure or apparent violation. OFAC highlights this feature as key, noting that such remedial measures may be considered as mitigating factors when it determines an appropriate enforcement response.
4. **Testing and auditing.** As virtual currency transactions present unique risks, new methods of testing will need to be developed and implemented. As systems and other technical internal controls are developed to mitigate these risks, lessons will be learned by third-line audit functions. The sanctions testing and audit functions should incorporate reviewing technical internal controls, including sanctions list screening, geographic keyword screening, and IP blocking, which OFAC has flagged as best practices for the virtual currency industry. Although the testing of screening systems usually occurs at least annually, more frequent testing may be needed given the dynamic nature of virtual currencies.

   OFAC's guidance underlines the importance of remediating root causes, the process of addressing underlying failures that gave rise to the breach, and demonstrating the enhancement of controls to prevent similar recurrences.
5. **Training.** OFAC reiterates from its compliance framework that firms should provide job-specific training informed by factors such as the firm's size and risk profile. Specific to the virtual currency industry, OFAC recommends the training account for the frequent changes to sanctions programs, as well as new technologies in the virtual currency space.

   In our experience, training also should cover concepts such as the additional compliance risks of AECs compared to other virtual currencies.

Conclusion

While OFAC's new guidance contains numerous sanctions risk and compliance insights specific to the virtual currency industry, it echoes guidance and practices that the agency has recommended for years. Virtual currencies present new and novel risks, and appropriate controls will have to be developed and tested to sufficiently mitigate these risks. While the technology and methods may be novel and continue to evolve, the expectation that firms maintain effective sanctions compliance programs remains fundamental to the compliance effort.

About BRG

Berkeley Research Group, LLC (BRG) is a global consulting firm that helps leading organizations advance in three key areas: disputes and investigations, corporate finance, and performance improvement and advisory. Headquartered in California with offices around the world, we are an integrated group of experts, industry leaders, academics, data scientists, and professionals working beyond borders and disciplines. We harness our collective expertise to deliver the inspired insights and practical strategies our clients need to stay ahead of what's next. Visit thinkbrg.com for more information.

THINKBRG.COM