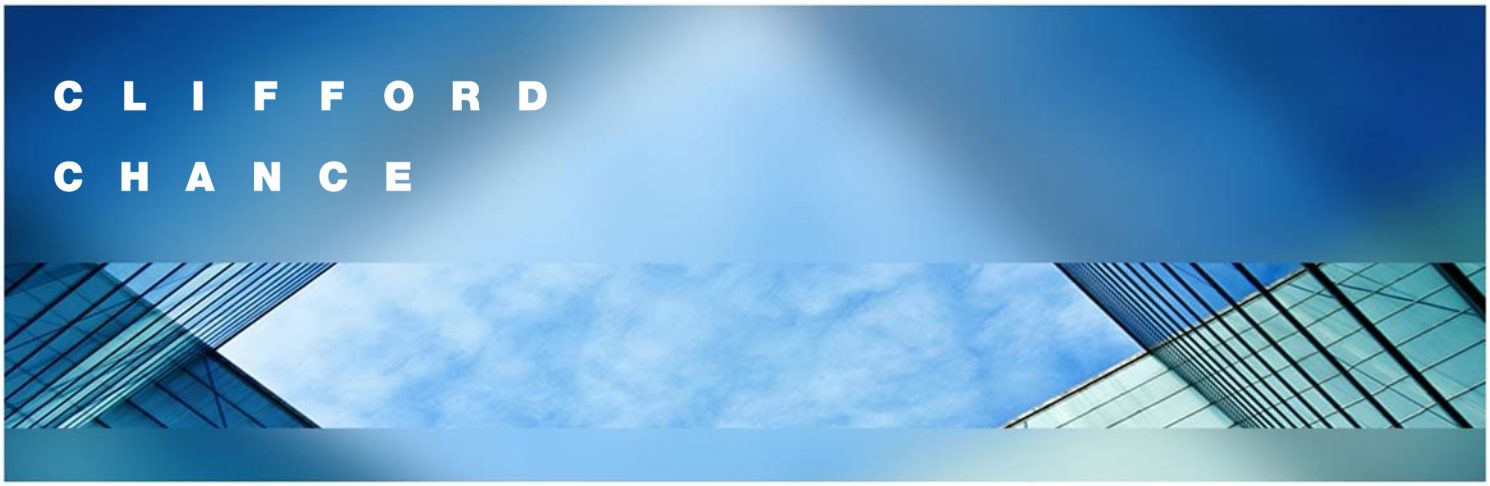

OFAC URGES THE VIRTUAL CURRENCY INDUSTRY TO GET REAL ABOUT SANCTIONS COMPLIANCE

The United States Treasury Department's Office of Foreign Assets Control ("**OFAC**") has further increased the pressure on crypto-currency service providers to ensure they maintain adequate OFAC compliance controls. In very clear language, OFAC advised the virtual currency industry that it is holding them to the same compliance standards and expectations as the fiat currency industry, which has had many years to develop their compliance framework. This will require virtual currency market participants to quickly up their compliance game at the threat of enforcement action.

On October 15, 2021, OFAC issued *Sanctions Compliance Guidance for the Virtual Currency Industry* (the "**Guidance**"), available at https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf. The Guidance follows a series of enforcement actions against participants in the virtual currency industry that fell short of the compliance standards OFAC historically has imposed in the fiat currency sector. The Guidance helpfully provides virtual currency exchanges, wallet providers, administrators, technology companies and financial institutions that process digital currency transactions with a detailed road map of OFAC's compliance expectations.

In March 2018, OFAC published FAQ 560 warning that OFAC compliance requirements apply to virtual currency transactions, including to non-US parties to the extent their virtual currency transactions involve US persons, the US financial system or other US elements. The Guidance advises crypto-currency service providers to adopt a risk-based OFAC sanctions compliance program ("**SCP**") to identify and mitigate the primary sanctions risks confronting their business. The Guidance cites *OFAC's Framework for OFAC Compliance Commitments* (the "**Framework**"), which OFAC published in May 2019 at https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf.

As first noted by OFAC in the Framework (and re-stated in the Guidance), the core elements of an effective risk-based SCP include: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training. The Guidance notes that a risk-based SCP should take into account a variety of factors, including the type of business involved, its size and sophistication, products and services offered, customers and counterparties and geographic locations served. The Guidance also

emphasizes, citing recent enforcement actions against two companies in the virtual currency industry, that information collected for business or security purposes should also be utilized for OFAC compliance purposes.

The Guidance includes specific recommendations for controls that companies operating in the virtual currency industry should incorporate into their risk-based SCP. These include:

- Geolocation and IP blocking controls to prevent individuals in OFAC sanctioned countries from accessing online platforms and other services. OFAC also noted that there are tools available that can identify "*IP misattribution*", including IP addresses that are associated with virtual privacy networks and "*improbable logins*."
- Robust know-your-customer procedures to identify customers that are OFAC sanctions targets or are at increased risk of exposing the company to activity involving OFAC sanctions targets (*i.e.,* higher risk customers).
- Transaction screening controls that include screening virtual currency transactions against the virtual currency addresses included on OFAC's List of Specially Designated Nationals.
- Conducting look-back reviews of suspicious transactions to identify potential links between particular virtual currency addresses and the addresses listed by OFAC (*i.e.,* unlisted addresses that have transacted with listed addresses or review of wallets that contain listed addresses).

The Biden Administration has assigned a high priority to combatting ransomware, cyber-based sanctions evasion and cyber-crime generally, and seemingly is looking to the virtual currency market participants as the gatekeepers to the crypto-currency ransom payments in the same way banks historically have been held accountable for processing violative payments. OFAC accordingly has intensified its attention to these threats along with other US government authorities. In the months ahead, we expect additional cyber-related OFAC enforcement actions and SDN designations, such as the September 2021 designation of the SUEX Exchange (*see* https://home.treasury.gov/news/press-releases/jy0364).

Cyber service providers accordingly should ensure they have conducted an appropriate risk assessment and then assessed their existing compliance capabilities to adequately manage those risks, while confirming that they address the core elements of the OFAC Framework as well as the specific controls identified in the Guidance. Under its Enforcement Guidelines, OFAC considers the existence, nature and adequacy of a SCP when determining the appropriate enforcement response to an apparent violation, meaning that the lack of an effective SCP can provoke a harsher enforcement response to apparent sanctions violations.

CLIFFORD CHANCE

CONTACTS

David DiBari
Partner

T +1 202 912 5098
E david.dibari
@cliffordchance.com

Steven Gatti
Partner

T +1 202 912 5095
E steven.gatti
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

George Kleinfeld
Partner

T +1 202 912 5126
E george.kleinfeld
@cliffordchance.com

Philip Angeloff
Counsel

T +1 202 912 5111
E philip.angeloff
@cliffordchance.com

Jamal El-Hindi
Counsel

T +1 202 912 5167
E jamal.elhindi
@cliffordchance.com

John-Patrick Powers
Counsel

T +1 202 912 5048
E john-patrick.powers
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 2001 K Street NW, Washington, DC 20006-1001, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.