SANCTIONS COMPLIANCE IN THE WORLD OF CRYPTOCURRENCY

AN ASSET CLASS RIDDLED WITH FRAUD, RISKS AND SCAMS

Authored by : Priyanka Kapoor – PCB Byrne

Virtual currencies have not only arrived but have become a major player in the global economy. The meteoric rise in their importance and the inherent material risks are not lost on the regulators. Cryptoassets by design facilitate the anonymous or pseudonymous conduct of international commercial transactions, making them the target of choice by sanctioned actors and cybercriminals to channel and hide the source of their financial transactions, evade sanctions and launder money. In the post-pandemic world, with the shift to remote working, ransomware attacks have exploded in volume and criminals have come to rely on digital currencies to force victims to pay millions of dollars to regain access to their own files and to prevent leaks of stolen data.

Deficient customer screening compliance programmes in peer-to-peer marketplaces or over-the-counter traders operating on exchanges have only added to the attractiveness of the digital wild west. Given that the virtual currency is decentralised, government agencies across the world have struggled to tame the underregulated world of cryptocurrency and its use for nefarious activities.

Due diligence has forever been the bedrock of sanctions compliance. A risk-based assessment followed by internal policies and procedures specific to the industry and market risks aid in the identification and screening of sanctioned customers and counterparties. But the anonymity or pseudonymity offered by cryptocurrency makes sanctions significantly more difficult to comply with and enforce.

Recent trends indicate that the regulators have opted for an all-in approach wherein irrespective of whether a transaction in question involves fiat or digital currency, the compliance obligations remain the same, sending a clear message to the cryptocurrency players that they will be expected to comply with the sanctions regime in the same way as other industries.

Businesses that allow digital currency payments or those that are involved in the digital currency market or sector (including banks) need to consider how to implement appropriate risk-based compliance measures that address the specific vulnerabilities of digital currency. Due diligence and controls to determine whether digital currency has been tainted by sanctionable or criminal cyber activity may be necessary for certain transactions or businesses. In the current climate of the global pandemic, businesses of any size that utilise the internet (even if only for e-mail), may face an increasing risk of ransomware attacks, which raise cyber-related sanctions compliance concerns. Those involved in the digital currency sector, including companies that facilitate or engage in online

commerce or process transactions using digital currencies, may be more likely to face malicious cyber-enabled attacks, incurring increased sanctions compliance risks.

The US has been at the forefront of establishing a cyber-focused economic sanctions regime. The U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") has introduced a variety of sanctions targeting malicious cyber-related activities, under OFAC's "Cyber-Related Sanctions Program", as well as Executive Order (EO) 14024, Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation, issued on 15 April 2021. On October 15, 2021, OFAC issued "Sanctions Compliance Guidance for the Virtual Currency Industry" (the "Guidance").

The Guidance is an important step in meeting the need for a robust sanctions compliance program and increases the scrutiny of digital currency transactions. A risk-based compliance programme has the potential to mean the difference between private caution and a public penalty, with far-reaching consequences for the investors. However, the recommended best practices do not differ from the existing guidance for compliance programs. At best, they set out the expectations of OFAC.

In March 2021 HMRC, the UK regulating body, released a manual outlining the tax consequences of different types of crypto-asset transactions. [1] Meanwhile, the Treasury is also reviewing evidence from consultation on how to regulate crypto-assets.

Risk-Based Compliance Program

A risk-based compliance program is tailored to the specific company and / or end user, and typically considers the types of products and services offered, the markets and geographic locations served, the company's size and sophistication and the types of intermediaries and customers. It also includes the established best practices for KYC checks.

In addition, a robust compliance program for players in the digital currency industry should ideally incorporate:

- Screening information to detect activity involving sanctioned jurisdictions. Location information acquired with the use of geolocation and IP blocking tools (including IP misattribution screening) can identify parties operating in sanctioned jurisdictions;
- use of blockchain analytics services can help mitigate risks associated with dealing with sanctions-listed addresses and avoid potential sanctions violations;
- adopting a compliance culture that promotes voluntarily self-disclosing any violations and carrying out an internal investigation to understand the reason for the violation, leading to implantation of new internal controls to address the identified weakness and avoid future violations;
- formulating a list of potential red flags that help address risks associated with the factors considered in the risk-based approach, like deficient KYC checks resulting in incomplete client information or a transaction with a VPN or digital currency address linked to a sanctioned person or jurisdiction. This will encourage a compliance culture and empower employees to raise an alarm in a timely manner;
- To the extent that some industry players do not fall within the realm of regulated financial institutions, requiring them to comply with anti-money laundering regulatory requirements and incorporating robust KYC procedures; and
- Voluntary self-disclosure to the relevant regulator, if the company becomes aware that it has engaged in an unauthorised transaction or dealt with a sanctioned person or jurisdiction.

Essential components of a sanctions compliance programme:[2]

The key issues every business (especially those in financial services) should consider when evaluating a virtual currency industry player are centred on the fundamentals of any compliance program, namely: management commitment, risk assessment, internal controls, testing and training. Enquiries may include:

- whether the virtual currency industry player has established an integrated compliance culture throughout the organisation;
- whether the management is actively involved with the compliance and risk mitigation and has established incentives to incorporate compliance objectives;
- whether the policies and procedures are aligned with the business' operating model, products and markets it caters to;
- whether there is an internal protocol for periodic compliance monitoring and testing to identify potential weaknesses; and
- whether the crypto asset firm, for example, is registered with a regulator (if applicable).

Looking ahead

Law enforcement and regulators are focused on arresting the misuse of cryptoassets for nefarious activities, without placing unnecessary limits on the technology itself. Sanctions regimes face the challenge of attempting to address some of the most complicated compliance issues without a "one size fits all" solution for mitigating these sanctions-related risks. For market players in the virtual currency industry, therefore, a combination of a risk-based approach and a voluntary self-disclosure of potential

1 https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual

2 Fig: https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf