VASPs as Regulated Entities: Building a Compliant AML Ecosystem

December-2, 2025

Virtual Asset Service Providers (VASPs) are entities that facilitate the transfer, safekeeping, administration or exchange of digital/virtual assets and fiat currencies. Although relatively new in the financial world, VASPs play a crucial role in the digital economy and are subject to ongoing regulatory updates. The virtual asset landscape is continuously evolving, with new asset types and services. Some examples of virtual assets (VAs) handled by VASPs include cryptocurrencies like Bitcoin and Ethereum, stablecoins such as USDT and USDC and privacy-enhanced coins like Monero and Zcash.

Among these, stablecoins are increasingly being misused in illicit financial activities due to their price stability, fast settlement capability and global reach, making them a growing area of concern for AML/CFT regulators. Criminals using stablecoins leverage anonymity enhancing tools and dormant VASP accounts for layering. Stablecoins held in unhosted wallets could be used for purchase of goods without being converted into fiat currencies and without any form of regulation. Mass adoption of stablecoins could therefore increase financial crime risks, particularly where FATF (Financial Action Task Force) standards for VASPs are unevenly applied.

With the growing use of virtual assets, the risk of money laundering and terrorist financing activities has increased due to the speed, global reach, and pseudonymous nature of the virtual asset transactions. Virtual asset ecosystems allow the movement of value across borders without regulated financial entities, which creates opportunities for concealing the source of funds. Criminal actors may exploit this sector by using anonymising tools such as tumblers, mixers, or privacy-enhancing features to limit transaction traceability. Although blockchain records transactions publicly, the use of pseudonymous wallet addresses can make it difficult to clearly associate activity with identifiable individuals. This highlights the importance of an effective and compliant AML framework for VASPs, to ensure they have strong controls to identify customers, monitor transactions, detect high-risk behaviour, and report suspicious activity in line with regulatory expectations.

Following are some components of a compliant AML Framework for VASPs:

- Customer Due Diligence- Proper customer due diligence to identify and verify customer and beneficial owners' information using reliable documents before starting a relationship.

- Transaction Monitoring- Transaction monitoring to identify suspicious or irregular activities, focusing on customer behaviour, transaction trends and threshold limits on an ongoing basis.
- Training- Training for all employees on AML/CFT concepts as part of their training curriculum.
- Record Keeping- Maintain records of originator and beneficiary information for at least five years as per FATF guidelines to ensure traceability of virtual asset transfers and support regulatory investigations.
- Risk-Based Approach (RBA): VASPs should assess ML/TF risks associated with their customers, transactions, services, and business models and adapt their controls and resources accordingly.

The AML framework also plays a crucial role in handling cross-border virtual asset transfers. The FATF recommends that VASPs implement the “Travel Rule,” which obligates them to collect and securely transmit originator and beneficiary information during transfers to another VASP or financial institution. This prevents anonymity from being used to obscure the ownership and source of virtual asset flows across borders. The Travel Rule further supports international cooperation by requiring supervisors, law enforcement and financial intelligence units to exchange relevant information swiftly when VASPs operate across multiple jurisdictions.

Given the anonymous nature of transactions in VASPs, a robust transaction monitoring system can ensure mitigation of the growing ML/TF risks. By following the regulatory guidelines, keeping systems updated, training, and reporting promptly, VASPs can maintain compliance and protect their business. A comprehensive Anti-Money Laundering framework and a robust system for Virtual Asset Service Providers is essential to ensure compliance, transparency, and regulatory alignment in the virtual asset ecosystem. It is not only a regulatory requirement but a fundamental safeguard for the integrity of their business.

Quantum Data Engines™

Quantum Data Engines is a reg-tech company that helps financial institutions detect, manage, and report financial crime more effectively and efficiently.

For more details write to: connect@qde.ai