EXPERT CRYPTOCURRENCIES

DETECTING HIDDEN RISKS

KATARZYNA SAGANOWSKA, RISK AND COMPLIANCE DIRECTOR AT TMF GROUP, EXPLAINS EXPLAINS THE RISK FOR BUSINESS ORGANIZATIONS WHEN DEALING WITH CRYPTOCURRENCIES.

Cryptocurrencies have introduced new financial possibilities in all jurisdictions around the world. However for a long time, the uncertainty of the blooming regulatory landscape surrounding cryptocurrencies is only increasing, and the ambiguity of the local obligations arising from national legal regimes continues. For companies operating in this space it is critical to understand their compliance obligations, and how they can detect and address the risks that they face. The same goes for companies who have clients involved in cryptocurrencies: they need to understand and monitor their risk exposure as well, as the opportunities and benefits linked to cryptocurrencies have been accompanied by new risks, while regulatory blind spots were immediately used by criminals for money laundering.

providers who wish to embed best practices into their business as usual. In principle, the so-called risk-based approach requires companies to deploy compliance measures to risks that their customers present.

To establish that risk, an individual risk assessment should be performed. It involves collecting and verifying information about clients as well as building their risk profiles to form future compliance decisions.

In particular, companies linked to cryptocurrencies should consider the anonymity and speed of cryptocurrency transactions, and how those factors might inform a risk assessment. With that in mind, a comprehensive approach to cryptocurrency compliance should include rigorous onboarding rules. In a nutshell, it is a proper identity verification.

While such schemes might share characteristics with conventional money laundering crimes, they are also taking an advantage of the increased anonymity and transaction speeds linked to the technology itself. For example, a client may attempt to move illegal crypto assets through different 'layers' of multiple transactions, cycling illegal money through fiat currencies and cryptocurrencies. Money launderers may make large numbers of small cryptocurrency transactions involving third parties—the so-called "money mules"—to conduct transactions on their behalf to avoid identity verification measures.

Criminals may also steal crypto wallets containing virtual assets (e.g. NFTs). If a wallet operates independently of a crypto service provider or exchanges it may be very difficult to track and verify its actual lawful ownership. Such stolen crypto assets may be exchanged with privacy coins and subsequently used in transactions on the Darknet.

but also identify any instances of suspicious behavior.

On the other hand, transaction monitoring solutions for compliance in the cryptocurrency domain can also increase cybersecurity by monitoring and preventing fraudulent transactions or addressing risks related to tracing parties on the sanction lists.

INTERNAL TRAINING PROGRAMS

Firms dealing with cryptocurrencies should also seek to implement internal training programs to ensure that their compliance employees remain familiar with the latest AML/CFT best practices, the latest criminal methodologies, and incoming regulations to safeguard them from being involved in illegal activities.

> Cryptocurrency service providers and companies who have clients involved in the cryptocurrency area must ensure that every stakeholder in their compliance solution system understands their role and responsibilities.

From a practical perspective, there are a few key best practices for entrepreneurs to ensure good cryptocurrency compliance.

COMPREHENSIVE RISK ASSESSMENT

Companies dealing with clients who use cryptocurrencies need to perform a Comprehensive Risk Assessment while entering into new client relationships.

The guidance of taking a risk-based approach to AML/CFT compliance (Anti-Money Laundering/Combating the Financing of Terrorism) should be extended to cryptocurrency service

The risk assessment is an ongoing process, not a one-and-done task, and therefore companies must revisit their risk assessments throughout business relationships to ensure that they remain accurate.

TYPOLOGIES OF CRIME

Companies must also have a good understanding of the typologies of crime, as well as the detection of red flags and prevention.

The controls framework the company implements should be based on a proper and close understanding of criminal typologies and allow to detect the red flags.

TRANSACTION MONITORING

Companies must implement systems to trace the flow of cryptocurrency assets which focuses on verifying whether the transactions by a specific business are legal or have any associations with financial crimes. The monitoring should verify not only the transaction data

Cryptocurrency service providers and companies who have clients involved in the cryptocurrency area must ensure that every stakeholder in their compliance solution system understands their role and responsibilities, therefore companies should seek to ensure that their relationship with the relevant financial regulators and authorities remains strong to apply most recent guidelines and in case the risk is materialized to facilitate the swift remediation of compliance alerts.