New Crypto Compliance rules – what Directive 9 means for CASPs

By Sameer Kumandan, MD of SearchWorks

With South Africa tightening its grip on crypto regulations, Crypto Asset Service Providers (CASPs) must act now to avoid compliance failures. As of April 30, 2025, Directive 9 will introduce stricter requirements for tracking and reporting crypto asset transactions. A key component of this is the 'travel rule,' which mandates that client details accompany domestic and cross-border crypto transfers. This information includes the originator's full name, identity or passport number, date and place of birth, residential address (if "readily available"), and wallet address for transactions over R5000.

South Africa's greylisting by the Financial Action Task Force (FATF) has triggered a wave of stricter compliance regulations. Directive 9 is a direct response, placing responsibility on CASPs to ensure crypto transactions are not linked to money laundering, terrorism financing, or other illicit financial activities. This includes the 'ordering CASP' (the CASP where the sender of the crypto assets has their account), the 'recipient CASP' (the CASP that receives the crypto assets from the ordering CASP on behalf of the customer) and any intermediary CASP (a CASP that transmits and receives crypto assets on behalf of an ordering CASP or a recipient CASP or another intermediary CASP).

Why CASPs must take note

Crypto assets were officially declared financial products by South Africa's Financial Sector Conduct Authority (FSCA) in October 2022 and CASPs were included in South African regulatory frameworks as accountable institutions in December 2022. As such, these service providers must comply with the Financial Intelligence Centre Act (FICA) regulations to ensure that they stay on the right side of the law.

CASPs now have a responsibility to do customer due diligence and verify a customer's identity before processing transactions. This is especially important because crypto assets enable the quick and seamless transfer of funds across borders, which makes it harder to determine who is behind the transactions and, thus, means that they can easily be used for criminal activities.

If CASPs want to avoid financial penalties and possible reputational damage, they should put robust governance and compliance measures in place, like real time checks against global watchlists, live customer verifications video calls and advanced biometric verification (challenging the user to blink, smile, or perform specific movements during the scanning process). But once a customer is verified, the work isn't over.

CASPS must also monitor transactions regularly; looking for unusual patterns and behaviours that could be linked to illicit activities. These requirements demand that CASPs maintain more detailed and extensive records of client transactions and implement comprehensive risk assessment frameworks to evaluate client risk during onboarding and beyond. For example, external factors such as geopolitical developments could mean that individuals or groups turn to crypto to finance illegal activity because it is harder to trace than if these transactions were done using traditional banking systems. As part of their risk assessment framework, CASPs need to have a clear understanding of when to reject or suspend a cross-border crypto asset transfer and what follow-up action will be taken when this happens.

While this directive has been welcomed by many, some have voiced concerns that the travel rule presents significant privacy governance challenges. POPIA restricts the transfer of personal information outside South Africa but given the global nature of crypto transactions, the travel rule dictates that personal data may have to be transmitted to entities in countries that do not have stringent privacy safeguards in place. Additionally, POPIA stipulates that only the data necessary for completing the transaction itself should be collected and processed and the travel rule could conflict with this.

As more and more measures are put in place to ensure that the crypto world operates within well-regulated frameworks, CASPs and other financial institutions need all the help they can get to stay ahead of changing compliance obligations and reduce operational risk.

VOCA, powered by SearchWorks, was built to comply with FICA, AML, CFT, FATF, and POPIA regulations, meaning it is the ideal tool to ensure that your compliance with the travel rule doesn’t conflict with any other legislation. This automated compliance platform is designed to help businesses meet governance requirements efficiently by integrating real-time identity verifications, risk assessments, and transaction monitoring to prevent fraud, money laundering, and regulatory breaches.

One of the exciting new additions to VOCA’s capabilities is the ongoing monitoring feature, which tracks client profiles daily and will send alerts of any changes that could indicate a compliance risk. And VOCA’s automated reporting ensures that any suspicious activity is tracked and documented as required by regulators.

The implementation of Directive 9 marks a critical shift in South Africa's regulatory framework for CASPs. With non-compliance now carrying the risk of administrative sanctions under the FIC Act, CASPs must take immediate steps to align with these obligations.

Ends.