BIZCOMMUNITY

Is SA's one-size-fits-all approach to crypto risk management sufficient to combat terrorism?

By Angela Itzikowitz and Aslam Moosajee

16 Sep 2022

Recently, the Prudential Authority, acting in terms of the Banks Act, 1990, issued a guidance note (G10/2022) to inform banks and bank controlling companies of practices related to the effective implementation of adequate anti-money laundering and counter-financing of terrorism controls relating to crypto assets and crypto asset service providers.

Image source: welcomia – 123RF.com

The Prudential Authority is aware that certain banks in South Africa have previously decided to terminate their relationship with crypto asset service providers and/or have discontinued the provision of banking services to crypto asset service providers by closing their accounts.

In an implicit criticism of such actions by certain banks, the guidance note emphasises that risk assessment does not necessarily mean that banks should seek to avoid any risk entirely by, for example, closing the accounts of crypto asset service providers or by refusing to open an account for them.

The guidance note highlights that the decision to close accounts or not to offer banking services should be made only after careful due diligence and consideration. By virtue of this, if a bank gives notice of its intention to close an account of a customer simply on the basis that the customer is a crypto asset service provider, the enforcement of the bank's right to terminate may be challenged on the basis that it is contrary to public policy and should not be countenanced.

Risk management processes

Inasmuch as the Financial Intelligence Centre Act, 2001 adopts a risk-based approach to regulation, banks are required to have in place comprehensive policies and risk-management processes as well as procedures to combat money laundering, terrorist financing and proliferation financing. These policies and processes must be documented and updated on a regular basis and training on money laundering and terrorist financing must be provided on an ongoing basis.

Risk assessment in terms of such policies would enable banks to understand the direct and/or indirect exposure to risks that a crypto asset service provider may present. Banks need to assess what elements are driving or reducing money laundering, terrorist and proliferation financing. In this regard, banks have to consider the type of clients, their transactional activity, cross-border flow of funds and a client's association with crypto-related activities.

The risk management and compliance programmes of banks need to be tailored and cater to varying levels of risk that a crypto asset service provider poses. Appropriate risk assessment involves a consideration of various factors, including:

- the type of services, products, transactions involved;
- customer risk;
- geographical factors; and
- the type of crypto assets involved or exchanged.

Regulators launch hub for fintech innovation

7 Apr 2020

Due diligence

When a crypto asset service provider seeks to establish and maintain a relationship with a bank, the bank should, as part of its due diligence, ascertain if the crypto asset service provider has documented and implemented appropriate money laundering, terrorist and proliferation financing risk management policies, procedures, systems and controls that the bank follows in respect of its own activities and product offerings. Where higher risks present themselves, an enhanced due diligence should be undertaken. A "one size fits all" approach in dealing with crypto asset service providers may result in inadequate risk understanding and risk measures. The Prudential Authority has noted that this approach goes against the spirit and practice of a risk-based approach.

Risks associated with crypto asset service providers constantly change and this requires banks to conduct regular risk assessments and amend their risk profiles and risk management programmes to deal with new risks that might arise. Banks need relevant and requisite technical expertise to adequately assess the risks stemming from crypto assets and crypto asset service providers.

Reporting suspicious activity

If the transactional activity of a crypto asset service provider is not in line with the initial profile the bank has of its customer, it should consider filing a suspicious or unusual activity report with the Financial Intelligence Centre (FIC). Banks must ensure that they employ appropriate detection and monitoring mechanisms to mitigate against any risks of money laundering or terrorist financing that may be introduced through crypto assets or crypto asset service providers.

Banks must ensure that they maintain adequate records in respect of all customer transactions for a minimum period of seven years or for a period of seven years from the date of submission of a suspicious or unusual transaction report to the FIC.

In due course, crypto asset service providers will become accountable institutions and will have to comply with all the obligations imposed on accountable institutions and that may give banks some added comfort, at least as to the underlying clients of the crypto asset service providers. Until then, given that the legislation is risk-based and not rule-based, the banks should revisit their risk appetite for crypto asset clients and effect the necessary changes to their policies and compliance manual.

The Protection of Constitutional Democracy Against Terrorist and Related Activities Bill (the Bill)
Parliament's police committee recently heard public submissions on the Bill. The draft law is designed to align South Africa with international instruments that were adopted to provide for:

- offences related to terrorist training and the joining or establishment of terrorist organisations;
- offences related to foreign travel for the purposes of committing an offence outside South Africa for the benefit of or at the direction of or in association with a terrorist group;
- offences related to the possession and distribution of material containing unlawful terrorism related content;
- the authorisation of the Director of Public Prosecutions to be obtained in respect of the investigation and prosecution of certain offences;
- the issuing of warrants for the search and cordoning off of vehicles, persons and premises;
- a direction requiring the disclosure of a decryption key and the effect of a direction to disclose a decryption key; and
- the removal of or making inaccessible material containing unlawful terrorism-related content.

Income tax and VAT implications of crypto mining

Joon Chong 3 Aug 2022

This Bill has been introduced to address shortcomings identified by the global anti-terrorism and anti-money laundering standards body, the Financial Action Task Force (FATF). FATF has given South Africa until February 2023 to remedy shortcomings that were identified by it in 2021 and if not remedied, could result in the country being grey-listed. A grey listing could have an impact on the economy as it could increase costs and risks associated with investments.

Concerns

Concerns have been raised about the proposed new Section 3A that would be introduced into our law, if the Bill is enacted in its current form, this section will prohibit the publication of terrorism-related content. It has been suggested that this new section will result in ordinary people being criminalised for publishing critical content about the South African Government and its policies.

The Bill proposes that someone who is found guilty of the publication of terrorism-related content could face a fine of up to R100 million or imprisonment of up to 30 years. It also allows the National Director of Public Prosecutions to apply without notice to the affected party, to a judge in chambers for various orders, including the freezing of an accused person's property.

The Bill also intends to prohibit a person from relying on a duty of secrecy or confidentiality in order to escape reporting the presence of a person suspected of committing or intending to commit a terrorist-related offence, but this does not apply to legal professional privilege between an attorney and client for communications made for the purposes of legal advice or pending litigation.

Academics and journalists who are arrested for being in possession of terrorist-related content, may raise as a defence that the possession was for carrying out the work as a journalist or for research purposes. This was introduced following an earlier round of public consultations in regard to the Bill. Some argue that this provision should be extended to allow for organisations and individuals involved in work to prevent radical thinking or extreme behaviour such as religious organisations and religious leaders that in good faith engage in research and education of their congregations to counter radical thinking or extreme behaviour.

In a recently published statement by National Treasury, it appears that it is working towards the Bill to be enacted by November 2022 and if so, hopefully this will go some way to avoid a grey-listing for South Africa.

ABOUT THE AUTHOR

Angela Itzikowitz - Executive, Banking and Finance; Aslam Mbosajee - Executive, Dispute Resolution - for ENSafrica