A comparative dive into virtual asset legislation in South Africa, Mauritius, Namibia and the UK

Niesa Van Staden, Elsabe Kilian and Jacqui-Lyn McIntyre
School of Accounting Sciences, North-West University, Potchefstroom, South Africa

Abstract

Purpose – Virtual assets are considered to be particularly susceptible to money laundering. The Financial Action Task Force has established an international regime to address the money laundering risk associated with virtual assets. This study aims to compare the anti-money laundering regimes in South Africa with those of Mauritius, Namibia and the United Kingdom to identify any gaps and areas for improvement in South Africa's regime for virtual assets service providers.

Design/methodology/approach – A comparative analysis of the anti-money laundering laws for virtual asset service providers in South Africa, Mauritius, Namibia and the United Kingdom was done. A black letter approach was followed by examining the anti-money laundering legislation of said countries with a focus on supervision, licencing, customer due diligence, recordkeeping and suspicious transaction reporting for virtual asset service providers.

Findings – It is recommended that South Africa introduce a distinct law that specifically addresses virtual assets and virtual asset service providers. Also, its range of customer due diligence measures should be broadened to reduce the anonymity of virtual asset holders.

Originality/value – It is essential to regulate virtual asset service providers to mitigate the risk of money laundering associated with these assets. Prior studies have not thoroughly examined the effectiveness of South African legislation in addressing virtual assets and virtual asset service providers.

Keywords Anti-money laundering legislation, Crypto asset, FATF, Mauritius, Namibia, United Kingdom, South Africa, Virtual assets, Virtual asset service providers

Paper type Research paper

1. Introduction

Virtual assets (VAs), cryptocurrencies, non-fungible tokens (NFTs), digital currencies, bitcoin and digital assets are all terms used to describe innovative technology that enables the quick global transfer of digital representation of value. Its appeal lies in its speed, global accessibility and, most significantly, the anonymity it offers to users (FATF, 2019, p. 3). In recent years, VAs have become increasingly prevalent and accessible. Based on information provided in Chainalysis's (2023, p. 12) Geography of Cryptocurrency Report, it can be estimated that nearly

The authors would like to thank the Workwell Research Unit at the North-West University for its support in this project, which was completed under the sub-programme ReTORIC (Research and Teaching in Organised & Integrity Crimes).

Journal of Money Laundering Control
Vol. 28 No. 7, 2025
pp. 50-64
Emerald Publishing Limited
1368-5201
DOI 10.1108/JMLC-10-2024-0170

$5tn in VA value was received globally from July 2022 to June 2023. The report also estimated that the sub-Saharan Africa region received $117.1 bn in VA value, of which South Africa received over $20bn (Chainalysis, 2023, p. 78). Current figures show that 12.4% of the South African population own some form of VA (Chainalysis, 2023, p. 80; Triple A, 2024, p. 4).

However, the rise in the use of VAs has also led to their involvement in illicit activities, such as money laundering (Utkina *et al.*, 2023, p. 350). The 2024 Crypto Crime Report indicates that a total of $24.2 bn in VA value was laundered in 2024 in comparison to $22.2 bn in 2023 (Chainalysis, 2024, p. 24). Schmidt (2021, p. 337) explained the significant risk that VAs pose for use in money laundering, noting that VAs allow for efficient value transfer from one place to another, because these assets can be exchanged without an intermediary and more expansively. Criminals are innovative and exploit the opportunities presented by VAs to "utilize their funds gained from the criminal economy in the legitimate economy" (Schmidt, 2021, p. 337). The Financial Intelligence Centre (FIC) (2023, p. 4) of South Africa highlights various reasons why VAs are used by criminals: its cross-border nature; pseudonymity; ability to be used without face-to-face interaction and the lack of requirement to identify sources of funding.

To prevent money laundering, an anti-money laundering regime must be established. Hence, the Financial Action Task Force (FATF) introduced its 40 Recommendations to effectively combat this form of financial crime (Utkina *et al.*, 2023, p. 359). These Recommendations are seen as the global anti-money laundering standards to which member countries must adhere (FATF, 2021a, p. 1). Due to the money laundering risk associated with VAs, the FATF amended its global anti-money laundering regime to include VAs and virtual asset service providers (VASPs), specifically under Recommendation 15. This Recommendation requires that VASPs be regulated for anti-money laundering purposes and be licenced or registered to ensure compliance with preventative measures such as customer due diligence, recordkeeping and suspicious transaction reporting (FATF, 2021a, p. 4). To take effective action against the risks associated with VAs, the FATF (2024) stresses the need for member countries to implement the applicable Recommendations.

South Africa has been a member of the FATF since 2003 and is therefore required to comply with the Recommendations. However, the country was placed on the FATF grey list in 2023 due to *inter alia* the non-compliance with these Recommendations (Van Wyk, 2023, p. 22). Regarding its non-compliance with Recommendation 15 specifically, South African lawmakers brought VAs under the country's anti-money laundering regime by declaring VAs as a "financial product" in 2022 (FSCA, 2022, p. 3). Although the declaration has improved South Africa's compliance score, the new score still indicates that there are areas for improvement in the country's anti-money laundering framework.

This study aimed to identify such areas for improvement in the South African anti-money laundering framework for VAs and VASPs. The study took the form of a comparative analysis of the anti-money laundering framework of South Africa with that of Mauritius, Namibia and the United Kingdom (UK). These countries were chosen for the comparison because South Africa, Mauritius and Namibia belong to the same Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG, 2018), whereas the UK, with its robust legal framework, is considered a global leader in effectively implementing anti-money laundering measures (FATF, 2018, p. 4). Furthermore, the UK is a suitable comparison due to the similarities in the legal and justice systems of the UK and South Africa (Wille, 1942, p. 124) as both countries' legal systems incorporate English common law (Barratt *et al.*, 2019, p. 2; Courts and Tribunals Judiciary, 2025).

Currently, only a few studies have comprehensively examined the efficacy of South African laws in dealing with VAs and VASPs compared to other countries. While Beebeejaun and Mahadew (2024) conducted a study on the anti-money laundering legislative framework related to VAs in Mauritius, the study at hand aimed to fill the existing gap in the literature regarding South African law in this context.

The remainder of this article is divided into seven sections: a discussion of the key concepts "VA" and "VASP"; the Recommendations mandated by the FATF for its member countries; the anti-money laundering framework for VAs and VASPs in South Africa; the anti-money laundering framework of Mauritius, Namibia and the UK; a final comparison between the frameworks of South Africa and the selected countries and the conclusion, recommendations and areas for further research.

2. Virtual assets and virtual asset service providers

VAs originated in 2009 amid the global financial crisis as an alternative to fiat currencies (Schmidt, 2021, p. 333). The FATF (2021a, p. 109) defines a VA as "a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes". There are various types of VAs – cryptocurrencies being the most commonly known. In South African law, a VA is referred to as a crypto asset. Aligning with the FATF definition, crypto assets are defined in the Advisory and Intermediary Services Act No. 37 of 2002 as a "digital representation of value" that can be used for payment or investment. The definition further specifies that crypto assets are not issued by a central bank and that they utilise distributed ledger technologies – allowing them to be electronically traded, stored and transferred – as well as cryptography. The FATF definition of VAs is widely adopted, including in Mauritian, Namibian and UK legislation. For the purpose of this study, VA is used as the general term and refers to crypto assets.

VAs have value attributed to them and, as a result, can be used to purchase goods or services, such as tech products, luxury goods or cars. Individuals owning a form of a VA can also use them to make long- or short-term investments. The advanced technology underlying VAs ensures that VA transactions are secure (Marella *et al.*, 2020, p. 260). Due to VA's ability to make it easier, faster and cheaper to transfer value (FATF, 2020 p. 4) it has become involved in decentralised finance (DeFi) which uses blockchain to provide financial services using VAs as the trading product (Ozili, 2022, p.117). However, DeFi also heightens the risk of money laundering, as it offers easy access to criminals; operates without intermediaries and allows transaction parties to remain largely anonymous or pseudonymous (Ozili, 2022, pp. 118–119; Aquilina *et al.*, 2023, p.2). Aquilina *et al.* (2023, p. 3) argued that regulating DeFi is crucial for preventing market failures and safeguarding consumers. The challenge with DeFi arises from its intermediary-less framework, which current anti-money laundering laws do not adequately address (Rettig *et al.*, 2024, p. 1). Emerging trends in VAs underline the importance of establishing and adhering to an anti-money laundering regime that incorporates VAs to ensure user protection.

As mentioned, VAs can be used for payment or investment purposes and can be traded, stored and transferred and VASPs are the vehicles that perform these functions (Broby and Quimbayo, 2021, p.2). The FATF (2021a, p. 109) defines VASPs as legal or natural persons whose main business activities involve exchanging VAs with fiat currencies or other forms of VAs, as well as transferring, safekeeping and providing financial services related to VAs.

South African legislation defines a "crypto asset service provider" [FIC, 2023, p. 2; Financial Markets Act, 2012 (No. 19)] in a manner identical to the FATF's definition of a VASP. Similarly, the definition of a VASP in the Mauritian Virtual Asset and Initial Token Offerings Services Act (2021) (VAITOSA) replicates the FATF definition. In Namibia, the Virtual Assets Act (VAA) No. 10 of 2023 gives a short description of a VASP as a person or an entity whose business activities involve providing VA services. The UK defines a VASP in two parts under regulation 14A(1) of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations (2017) (MLRs):

(1) in circumstances where services involve the exchange of VAs for money or other VAs, the providers are considered "cryptoasset [1] exchange providers"; and

(2) when the services involve safeguarding, holding, storing and transferring VAs, the providers are considered "custodian wallet providers".

For the purpose of this study, VASP is used as the general term and refers to "crypto asset service provider" and "cryptoasset exchange providers" and "custodian wallet providers" when referenced in the context of South African and UK law respectively.

3. The Financial Action Task Force Recommendations

Recommendation 15 is the umbrella Recommendation regarding VASPs. It requires countries to regulate these providers through registration, licencing and monitoring to ensure they are adhering to the set Recommendations (FATF, 2023a, p. 17). In addition to Recommendation 15, VASPs must implement four other Recommendations for the prevention of money laundering. These include Recommendation 10: Customer due diligence; Recommendation 11: Record-keeping; Recommendation 20: Reporting of suspicious transactions and Recommendation 21: Tipping-off and confidentiality. Although there are more Recommendations that VASPs must adhere to, this study focused on the aforementioned, as they are the primary obligations set by the FATF for VASPs.

Recommendation 15 requires member countries to designate a competent authority for the supervision and monitoring of VASPs to ensure compliance (FATF, 2023a, p. 79). In addition to being registered or licenced with an authority (FATF, 2023a, p. 78), VASPs are mandated by the FATF (2021a, p. 43) to be registered or licenced in the jurisdictions where they were established.

The first Recommendation that places an obligation on VASPs is Recommendation 10, which requires these providers to perform ongoing customer due diligence measures. These measures entail obtaining and verifying the identity of customers and beneficial owners. The aim is to ensure that a VASP's business relationship with a customer is in line with its knowledge of the customer (FATF, 2023a, p. 14).

This Recommendation is crucial for VASPs because one of the defining characteristics of VAs is the anonymity they offer to users. Thus, the Recommendation mandates that countries legally require VASPs to conduct customer due diligence (FATF, 2023a, p. 14). Customer due diligence should also be performed at specific times, including:

- upon the establishment of the business relationship;
- when transactions exceed a certain threshold;
- when there is suspicion of money laundering; and
- when the institution has doubts about the accuracy of data previously obtained.

The threshold amount for individual transactions (referred to in point 2) is USD/EUR 1 000 for VASPs compared to USD/EUR 10 000 for other financial institutions (FATF, 2023a, p. 14).

Recommendation 11 flows from Recommendation 10 by requiring that information obtained through customer due diligence measures are kept for a minimum of five years from the date a business relationship with a customer has ended. For occasional transactions, the information must be kept for a minimum of five years after the transaction has occurred (FATF, 2023a, p. 15). Records of information include documents obtained through customer due diligence measures, account files and business correspondence. VASPs are also required to make these records available to authorities (FATF, 2023a, p. 15).

Recommendation 20 states that VASPs must report any suspicion that funds may be the proceeds of criminal activity, or related to terrorist financing, to their country's financial intelligence unit. Interestingly, Recommendation 21 specifies that directors, officers and employees of a VASP must be protected from criminal or civil liability for breach of any

restriction on disclosure of information imposed on them by contract, such as non-disclosure agreements, when they report a suspicious transaction in good faith. It also states that the individuals responsible for reporting suspicious transactions must be prohibited from disclosing the fact that such a report has been made. Furthermore, the FATF (2021a, p. 43) allows countries to either integrate the regulation of VASPs into their existing anti-money laundering regime or create a new anti-money laundering regime specifically applicable to VASPs.

4. South Africa

Despite the FATF (2021b) crediting the South African legal anti-money laundering framework as being rigorous, significant non-compliance with the Recommendations persists. As a result, the country was placed on the FATF's grey list. Being grey listed has several consequences, including possible damage to the country's reputation and increased due diligence by other countries when conducting cross-border business. This could prompt other countries to take additional measures to better understand South African clients and their sources of income – potentially leading to higher costs of doing business with South Africa, with a detrimental impact on the country's financial stability (National Treasury, 2023, pp. 3–6).

De Koker (2024:621) confirmed that grey listing has a continuing negative impact on the economy of a country. Therefore, to minimise these consequences, South Africa must endeavour to be removed from the grey list as soon as possible. South Africa was initially rated as non-compliant with Recommendation 15 in the FATF's Mutual Evaluation Report in 2021, but was re-rated as partially compliant in a follow-up report by the FATF in 2023 (FATF, 2023b).

In an effort to address non-compliancy, South African lawmakers took steps to incorporate the oversight of VASPs within the country's anti-money laundering framework. The most important step was to integrate legislation pertaining to VAs and VASPs with the overall anti-money laundering regime of the country. Local anti-money laundering legislation includes the Financial Intelligence Centre Act 38 of 2001 (FICA), the Proceeds of Crime Act 76 of 1996 and the Prevention and Combating of Corrupt Activities Act 12 of 2004. The declaration of a VA as a "financial product" brings these assets under the legal regime of South Africa in a twofold manner. Firstly, VAs were brought in under the Financial Advisory and Intermediary Services Act (FIASA) No. 37 of 2002 since "financial products" are defined in section 1 of this Act. Secondly, the first Schedule of the FICA (South Africa's main anti-money laundering legislation) lists the accountable institutions in the country; VASPs are now included in this list making them accountable for adhering to the preventative measures put into place by this Act.

The classification of a VA as a "financial product" further enables the application of Recommendation 15, and because the business activities of VASPs are considered a "financial product", the FIASA categorises VASPs as "financial service providers". Sections 7 and 8 of the FIASA require financial service providers to be licenced with the Financial Sector Conduct Authority. VASPs are, as a result, regulated and supervised by the Financial Sector Conduct Authority, as this authority is responsible for overseeing licenced financial service providers in South Africa (FSCA, 2024).

Schedule 2 of the FICA confirms this status of the Financial Sector Conduct Authority. The Schedule lists supervisory bodies, including the Financial Sector Conduct Authority [still referred to as the "Financial Service Board", which was replaced by the Financial Sector Conduct Authority in 2018 (Krige and Laskov, 2018)]. Section 45(1) of the FICA also states that these supervisory bodies are responsible for supervising and regulating accountable institutions. Thus, under the South African regime, the Financial Sector Conduct

Authority is tasked with supervising and regulating VASPs. Adherence to Recommendation 15 is demonstrated by requiring the registration of VASPs under the FIASA. According to the Financial Intelligence Centre (FIC) (FIC, 2023:7), VASPs that are "established, registered, incorporated or licenced" in South Africa must, at a minimum, register with the FIC. The obligation to register falls upon the VASPs themselves.

The Financial Sector Conduct Authority is the public entity responsible for overseeing the country's financial markets, focusing on improving the integrity and efficiency of financial products and services (National Government of South Africa, 2024a). The FIC, on the other hand, is the public entity tasked with managing financial intelligence to improve the integrity of the financial system as a whole (National Government of South Africa, 2024b).

As VASPs are classified as "accountable institutions" under the FICA, it holds them responsible for adhering to the preventive measures established by the Act, in alignment with FATF Recommendations. Section 20A of the FICA places the requirement on VASPs to perform customer due diligence measures. These measures must be carried out before establishing a business relationship with a client or before conducting any transaction with a customer. Customer due diligence must also be performed when there are doubts about customer due diligence information obtained previously and when there is suspicion of money laundering, as stipulated in section 21D of the FICA. Section 21 further mandates VASPs to obtain and verify the identity of customers. If an individual is acting on behalf of someone else, VASPs are required to establish and verify the identity of both parties, as well as whether the individual has the authority to act on behalf of the other person.

In addition to verifying identities, section 21A of the FICA mandates that VASPs obtain information about the nature and intended purpose of the business relationship with the client, together with the sources of the client's funds. Section 21C obligates VASPs to obtain and verify beneficial ownership in cases where the customer is not a natural person. Furthermore, section 21C indicates that VASPs must perform ongoing due diligence.

Recommendation 11, which concerns the keeping of customer due diligence records, is imposed on VASPs by section 22 of the FICA. According to this section, VASPs are required to keep records of their business relationship with clients, whether longstanding or a once-off transaction. The section lists the information that must be recorded, which includes: the identity of the client and all parties in instances where an individual is acting on behalf of someone else, as well as the approval given in such circumstances; information on the manner in which client identities were obtained and verified; details of the nature of the business transaction; the amount of the transaction; and the parties and accounts involved in the transaction. Section 23 of the FICA specifies that records must be kept for a minimum of five years from the termination of the business relationship or the conclusion of the transaction, in line with Recommendation 11.

Recommendation 20 stipulates that VASPs must report suspicious transactions. Accordingly, the FICA places a duty on accountable institutions to report cash transactions above the prescribed amount (currently R50 000) to the Financial Intelligence Centre under section 28. Section 29 of the FICA further requires anyone who carries on, manages, or is employed by a business to report any knowledge or suspicion of transactions that have occurred or will occur involving unlawful activities. Such reports must be directed to the FIC and include the prescribed particulars, together with the grounds for the knowledge or suspicion of unlawful activities.

Finally, section 29(3) of the FICA prohibits the person responsible for the report from tipping off the parties involved. Furthermore, sections 37 and 38 of the FICA apply Recommendation 21 by releasing the person making the report from any restriction on disclosing information and protecting the person from any civil or criminal liability or action.

5. Other international anti-money laundering regimes

5.1 Mauritius

The anti-money laundering regime of Mauritius consists of The Financial Intelligence and Anti-Money Laundering Act (2002) (FIAMLA). In 2021, the country enacted the VAITOSA to specifically address the regulation of VAs and VASPs; hence, this Act was selected for comparison in this study. While the VAITOSA has a section dedicated to VASPs, it makes provision for issuers of initial token offerings, as well as for the supervision and registration or licencing requirements of VASPs. The VAITOSA designates the Financial Commission, established under Mauritius' Financial Services Act (2007) No. 14 (section 2), as responsible for the regulation and supervision of VASPs (section 5).

Section 7 of the VAITOSA addresses the licencing of VASPs and requires anyone conducting the business activities of a VASP in or from Mauritius to be in possession of a VASP licence. The registration of VASPs is encompassed in the FIAMLA which stipulates that VASPs must be registered with the Financial Intelligence Unit, and the obligation to register falls upon these providers (section 14C).

Section 19 of the VAITOSA sets out the requirements for customer due diligence regarding VASPs. The act specifies a detailed list of customer due diligence measures that VASPs must carry out, emphasising the information that these providers are mandated to collect from originators and beneficial owners. Although section 19 requires VASPs to hold the customer due diligence information obtained, it does not specify how long such information must be held. The only requirement made in this section is that the information be available immediately upon the request of authorities. Conversely, the FIAMLA stipulates a specific period of seven years for these records to be kept.

The VAITOSA does not impose a duty of reporting suspicious transactions on any person involved in the business of a VASP, as per FATF Recommendation 20. Section 18 of the VAITOSA only places a responsibility on VASPs to identify, detect, prevent, monitor, restrict or suspend, but no obligation to report. In contrast, the FIAMLA obligates VASPs to report suspicious transactions (section 14) and prohibits alerting the parties involved [section 16(1)] as per Recommendation 21. Section 16 protects VASPs when disclosing confidential information, stating that no proceedings shall be initiated against VASPs, and no liability will be incurred upon them in such cases.

5.2 Namibia

Namibia, similar to Mauritius, has established a specific anti-money laundering regime for VAs through the enactment of the VAA. The country has incorporated VAs into its existing anti-money laundering regime by listing VASPs as an accountable institution under the Financial Intelligence Amendment Act (2023) (FIAA) No. 6. For comparative purposes in this study, the focus is placed on the VAA.

Sections 5 and 7 of the VAA, respectively, make provision for the regulation and licencing of VASPs per Recommendation 15. Section 5 determines that the Minister is responsible for appointing an entity as the Regulatory Authority for VASPs, which is currently the Bank of Namibia (Ministry of Finance and Public Enterprises, 2023).

Section 7, based on Recommendation 15, requires any VASP that is incorporated or registered in Namibia to obtain a licence, with the responsibility of applying for such a licence resting on the VASP. The FIAA, on the other hand, determines that the Bank of Namibia must register VASPs with the Financial Intelligence Centre (section 35). The customer due diligence stipulation is set out in section 18 of the VAA, which mandates VASPs to obtain the required originator information, which is established in the Rules by the Regulatory Authority. As such, the VAA elaborates on the customer due diligence measures

applicable to VASPs with the aim to mitigate the anonymity risk of VAs. Section 18 also determines that information obtained must be kept in such a manner that it is immediately available to the Regulatory Authority.

It is worth noting that Recommendations 20 and 21 are not outlined directly within the VAA itself, but rather included within the requirements of the FIAA. Thus, these two Recommendations are complied with in the FIAA. The obligation to report suspicious transactions is stated in section 33, the prohibition of disclosing such a report in section 46 and the protection of such a person from providing any evidence in court, criminal action and civil liability in section 45.

5.3 United Kingdom

The UK, unlike Mauritius and Namibia, but similar to South Africa, does not have its own VA act. Staples and Asolo (2024) found that VAs are still largely unregulated in the UK. The UK government is, however, in the process of bringing VAs under their anti-money laundering regime but does not aim to develop a standalone VA regime; their intention is to regulate VAs under the already established regime (FCA, 2024; HM Treasury, 2023, p. 15).

VASPs are obligated to adhere to the UK anti-money laundering regime, specifically the MLRs. Under section 8 of the MLRs, VASPs are classified as a "relevant person" and must apply these regulations accordingly.

Section 7 of the MLRs determines that the Financial Conduct Authority is the supervisory authority for VASPs. Sections 56 and 56A require VASPs to be registered with this authority to be permitted to conduct their business. While it is the Financial Conduct Authority's responsibility to register VASPs, no particulars are prescribed in the Act for VASPs regarding registration. Under the UK anti-money laundering laws, VASPs are also not required to apply for a licence.

Section 27 encompasses the customer due diligence measures, as per Recommendation 11. Customer due diligence must be performed when a business relationship is being established, when there is suspicion of money laundering, and when there is doubt regarding previously acquired identification information. This section elaborates on specific instances in which VASPs must perform customer due diligence measures. Circumstances include: when the transaction amounts to EUR 15 000 or more, when a machine with automated processes exchanges VAs for money and vice versa and when a VA transfer is equal to or more than EUR 1 000. Section 64A lists additional information that VASPs are mandated to obtain.

In section 40, the MLRs provide for Recommendation 11, prescribing the retention of records for a period of five years from the end of the business relationship or once the transaction has been completed. In addition, section 40(5) lists circumstances in which a retention period longer than five years may apply.

As with Mauritius and Namibia, the requirements of Recommendations 20 and 21 are set out in a separate piece of legislation, namely, the Proceeds of Crime Act (2002). Section 330 of this Act obligates VASPs to report suspicious transactions, whereas section 333A prohibits a person disclosing a suspicious transaction from tipping off the parties involved. Section 338 provides protection from any civil liability for making a suspicious transaction report, and section 339ZF protects a person from liability for breaching confidentiality obligations related to such reports.

6. Comparison

This section compares the South African legislative framework on VAs with that of Mauritius, Namibia and the UK. The anti-money laundering regimes of these three countries

provide a valuable paradigm to gain insight into the South African regime. Both Mauritius and Namibia were previously non-compliant with Recommendation 15 (ESAAMLG, 2022a, pp. 4–5; ESAAMLG, 2022b, p. 160), but have since been re-rated as compliant following the establishment of their respective VA acts. Mauritius was furthermore swiftly removed from the FATF grey list on 21 October 2021. Regarding the UK, FATF assessments have determined that they are largely compliant with Recommendation 15.

Similarities between the four countries include their application of not only FATF Recommendation 15, but also 10, 11, 20 and 21. Recommendation 15, which stipulates that VASPs must be supervised by an appropriate authority and be subject to licencing or registration requirements, is implemented by the following entities: The Financial Sector Conduct Authority in South Africa, the Financial Services Commission in Mauritius, the Bank of Namibia and the Financial Conduct Authority in the UK.

Although all four countries have licencing or registration requirements, some differences are notable. South Africa, Mauritius and Namibia require VASPs to obtain a licence from their respective supervisory authorities. The UK, however, does not impose a licensing requirement on VASPs. The registration of VASPs is required by all four countries, but the responsibility differs: South Africa and Mauritius place the onus on the VASPs themselves, whereas Namibia and the UK require registration through their respective supervisory authorities. In addition, South Africa, like Mauritius and Namibia, has minimum requirements for VASP registration with their supervisory authority, whereas, in the UK, VASPs must register with the Financial Intelligence Unit.

As per Recommendation 10, customer due diligence measures are essential for VAs due to their inherent anonymity. Legislation in all four countries stipulates that customer due diligence measures be performed. However, South Africa's FICA regulations are more extensive compared to those of the other three countries. In addition to obtaining and verifying the identity of the customer, beneficial owner and other third parties to the transaction, and having ongoing due diligence requirements in place, South African legislation also dictates that the purpose, nature and sources of financing must be obtained and understood. Conversely, the anti-money laundering legislation of Mauritius, Namibia and the UK details additional information that VASPs must obtain from clients, beneficial owners and other parties involved in transactions, to identify the individuals. Given the unique nature of VAs in comparison to other financial products, it is pertinent to propose the implementation of additional customer due diligence measures that are tailored to the specific characteristics and features of VAs.

Based on the above comparison, the study recommends that South Africa, although having extensive customer due diligence requirements, should expand their existing anti-money laundering regime in relation to VASPs, to include additional information when conducting customer due diligence, given the higher risk of money laundering associated with the anonymous nature of VAs. Expanding on the information VASPs must obtain from VA holders will assist in reducing the risk that VA holders are holding accounts and conducting transactions anonymously. The FATF Recommendations require VASPs to conduct customer due diligence for single transactions exceeding a threshold amount of USD/EUR 1 000. Mauritius and the UK have established this threshold amount in their laws, whereas South Africa and Namibia require VASPs to conduct customer due diligence for every transaction, making the process more stringent.

All four countries comply with the FATF's Recommendation 11, which determines that records must be retained for at least five years. Notably, Mauritius mandates a minimum retention period of seven years, whereas Namibia and the UK permit an extension period. It

is proposed that South Africa considers allowing for an extension period in situations where information may be required beyond the initial five-year period.

As per Recommendation 20, all four countries require VASPs to report suspicious transactions if criminal activity is suspected, specifically money laundering. The FATF Recommendations do not specify the particulars that must be reported; however, each country has its own prescribed information that must be reported. In all four countries' legislation, per Recommendation 21, prohibits individuals from disclosing to (or tipping off) the parties that a suspicious transaction report is being made. The four countries implemented the confidentiality of Recommendation 21, with minor differences. A person making such a report is protected from both criminal and civil liability under the laws of South Africa, Mauritius and Namibia. However, the UK only provides protection from civil liability. In addition, all four countries protect individuals who disclose information that is in breach of confidentiality.

The anti-money laundering act of South Africa, the FICA, encompasses all the requirements for making a suspicious transaction report under a single piece of legislation. In contrast, the requirements for making a suspicious transaction report under Mauritian, Namibian and UK law are dispersed over their respective anti-money laundering laws. By including all anti-money laundering measures under a single act, as South Africa has done, the legislation becomes more accessible to the applicable entities.

Table 1 provides a brief overview of the comparative analysis of the implementation of Recommendations 10, 11, 15, 20 and 21, applicable to VASPs in the respective anti-money laundering laws of South Africa, Mauritius, Namibia and the UK.

7. Conclusion and recommendation

VAs pose a material risk for money laundering, prompting the FATF to adapt their globally applied Recommendations to accommodate the challenges presented by VAs and VASPs. Countries such as South Africa, Mauritius, Namibia and the UK have adapted their anti-money laundering regime to align with the FATF Recommendations.

The study compared the South African legislative framework on VAs with those of Mauritius, Namibia and the UK and discussed the noteworthy differences and similarities. The study suggests that South African lawmakers explore the idea of creating a dedicated act for VAs to streamline the process for VASPs to obtain all necessary preventive measures from a single source. This approach can draw inspiration from, and build upon, the frameworks of Mauritius and Namibia. In contrast to Mauritius and Namibia, which dispersed the requirement between various anti-money laundering legislation and regulations, South Africa can encompass all preventive measures relating to VASPs in one act. In addition, South African law could benefit from, firstly, incorporating a more comprehensive list of customer due diligence information that VASPs need to obtain and, secondly, including an extension period for the keeping of records.

One aspect that was not explored in this study is the part of Recommendation 15 that requires countries to establish sanctions for VASPs that fail to comply with the national anti-money laundering framework. The FATF, in their follow-up report on South Africa's compliance with the 40 Recommendations, found the country to be non-compliant with this part of Recommendation 15 (FATF, 2023a:23). Given the inadequacy of the South African anti-money laundering framework in imposing sanctions on VASPs, further research is needed to determine which sanctions South African lawmakers can incorporate into the country's anti-money laundering framework to enhance compliance with FATF Recommendations.

Table 1. Comparison of the anti-money laundering law applicable to VASPs

Legislation reference	South Africa	Mauritius	Namibia	UK
Main anti-money laundering law applicable to VASPs	The FICA	The VAITOSA	The VAA	The MLRs
Supervisor	The Financial Sector Conduct Authority	The commission which refers to the Financial Service Commission	The Bank of Namibia	The Financial Conduct Authority
licencing of VASPs	Licences are issued by the Financial Sector Conduct Authority	VASPs from or in Mauritius must apply for a licence Licences are issued by the Financial Service Commission	VASPs incorporated or registered in Namibia must apply for a licence. Licences are issued by the Bank of Namibia	No licensing is required by UK legislation
Registration of VASPs	Responsibility for registering falls upon VASPs established, registered, incorporated or licensed in South Africa Must be registered with the Financial Intelligence Centre	Responsibility for registering falls upon VASPs. Must be registered with the Financial Intelligence Unit	Responsibility for registration falls upon the bank of Namibia. Must be registered with the Financial Intelligence Centre	Responsibility for registration falls upon the Financial Conduct Authority Must be registered with the Financial Conduct Authority
Customer due diligence measures	Required to perform customer due diligence	Required to perform customer due diligence, with additional prescribed measures for VASPs	Required to perform customer due diligence, with additional prescribed measures for VASPs	Required to perform customer due diligence, with additional prescribed measures for VASPs
Period of record keeping	Minimum of five years	Minimum of seven years	Minimum of five years, with extension period	Minimum of five years, with extension period
Reporting of suspicious transactions	Suspicious transactions must be reported	Suspicious transactions must be reported	Suspicious transactions must be reported	Suspicious transactions must be reported
Protection from criminal and civil liability for any breach of restriction on information disclosed	Protection against criminal or civil liability	Protection against criminal or civil liability	Protection against criminal or civil liability	Protection against civil liability
Prohibition from disclosing (tipping off) a report of suspicious transaction being made	Prohibited from tipping off	Prohibited from tipping off	Prohibited from tipping off	Prohibited from tipping off

Source(s): Table created by authors

Countries such as Mauritius, Namibia and the UK have implemented sanctions within their anti-money laundering legislation concerning VASPs, with the FATF rating these countries as largely compliant in their establishment of sanctions (ESAAMLG, 2022a, p. 4; ESAAMLG, 2022b, p. 160; FATF, 2022, p. 4). Sanctions play an important role in the fight against money laundering, highlighting the need for South Africa to enhance its rating. Conducting further research to strengthen South Africa's anti-money laundering framework for VASPs, drawing from the practices of the aforementioned countries, could assist in achieving an improved re-rating.

Note

1. Whilst South Africa, Mauritius and Namibia uses two words for crypto assets, the UK writes it as one word: cryptoassets.

References

Advisory and Intermediary Services Act (2002), No. 37/2002.

Aquilina, M., Frost, J. and Schrimpf, A. (2023), "Decentralised finance (DeFi): a functional approach", doi; 10.2139/ssrn.4325095.

Barratt, A., van Coller, H., Govindjee, A., de Freitas, S., Iya, P.F., Kruuse, H., Pillay, K., Du Preez, M., Singh, P.P., Tshingana, L. and Meintjes-Van der Walt, L. (2019), *Introduction to South African Law*, (3rd ed.), Pearson South Africa (Pty) Ltd, Cape Town.

Beebeejaun, A. and Mahadew, B. (2024), "Virtual assets and the prevention of money laundering: a critical and comparative analysis of the laws of Mauritius, Japan and South Africa", *Journal of Money Laundering Control*, Vol. 27 No. 4, pp. 790-802, doi: 10.1108/JMLC-05-2023-0091.

Broby, D. and Quimbayo, C. (2021), "The regulation of initial coin offerings, virtual assets and virtual asset service providers", *SSRN Electronic Journal*, doi: 10.2139/ssrn.3946331.

Chainalysis (2023), "The 2023 geography of cryptocurrency report", available at: https://go.chainalysis.com/geography-of-cryptocurrency-2023.html (accessed 15 September 2024).

Chainalysis (2024), "The 2024 crypto crime report", available at: https://go.chainalysis.com/crypto-crime-2024.html (accessed: 15 September 2024).

Courts and Tribunals Judiciary (2025), "The justice system and the constitution", available at: www.judiciary.uk/about-the-judiciary/our-justice-system/jud-acc-ind/justice-sys-and-constitution/#:~:text=The%20United%20Kingdom%20has%20three,in%20a%20written%20constitutional%20instrument (accessed 15 February 2025).

De Koker, L. (2024), "Editorial: FATF greylisting: time to revisit the approach", *Journal of Money Laundering Control*, Vol. 27 No. 4, pp. 621-624, doi: 10.1108/JMLC-07-2024-206.

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) (2018), "Who we are", available at: www.esaamlg.org/index.php/about (accessed 14 September 2024).

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) (2022a), "Anti-money laundering and counter-terrorist financing measures – Mauritius, 5th enhanced follow-up report and technical compliance Re-Rating", available at: www.fatf-gafi.org/en/publications/Mutualevaluations/FUR-Mauritius-2023.html (accessed 14 September 2024).

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) (2022b), "Anti-money laundering and counter-terrorist financing measures – Namibia, second round mutual evaluation report", available at: www.fatf-gafi.org/en/publications/Mutualevaluations/mer-namibia-2023.html (accessed 14 September 2024).

FATF (2020), "Easy guide to FATF standards and methodology", available at: www.fatf-gafi.org/content/dam/fatf-gafi/brochures/FATF-Booklet_VA.pdf (accessed 15 February 2025).

FATF (2021a), "Updated guidance for a risk-based approach to virtual assets and virtual assets service providers", available at: www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (accessed 1 July 2024).

FATF (2021b), "South Africa", available at: www.fatf-gafi-org/publications/mutualevaluations/documents/mer-south-africa-2021.htmlwww.fatf-gafi.org/en/countries/detail/South-Africa.html#:~:text=The%20Mutual%20Evaluation%20Report%20of,compliance%20with%20the%20FATF%20Recommendations (accessed 17 August 2024).

FATF (2022), "Anti-Money laundering and Counter-Terrorist financing measures – United Kingdom 1st regular follow-up report", FATF, Paris, available at: www.fatf-gafi.org/publications/mutualevaluations/documents/fur-united-kingdom2022.html (accessed 1 July 2024).

FATF (2023a), "International standards on combatting money laundering and the financing of terrorism and proliferation", available at: www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html (accessed 1 July 2024).

FATF (2023b), "Anti-money laundering and counter-terrorist financing measures – South Africa, 2nd enhanced follow-up report", available at: www.fatf-gafi.org/en/publications/Mutualevaluations/south-africa-fur-2023.html (accessed 1 July 2024).

FATF (2024), "Virtual assets", available at: www.fatf-gafi.org/en/topics/virtual-assets.html (accessed 1 July 2024).

Financial Action Task Force (FATF) (2018), "Anti-money laundering and counter-terrorist financing measures – United Kingdom, fourth round mutual evaluation report", available at: www.fatf-gafi.org/content/dam/fatf-gafi/mer/MER-United-Kingdom-2018.pdf.coredownload.inline.pdf (accessed 14 September 2024).

Financial Action Task Force (FATF) (2019), "Easy guide to FATF standards and methodology", available at: www.fatf-gafi.org/content/dam/fatf-gafi/brochures/FATF-Booklet_VA.pdf (accessed 3 August 2024).

Financial Advisory and Intermediary Services Act (2002), No. 37/2002.

Financial Conduct Authority (FCA) (2024), "Cryptoassets: AML/CTF regime", available at: www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime#section-scope-of-cryptoasset-services (accessed 17 August 2024).

Financial Intelligence Amendment Act (2023), No. 6/2023.

Financial Intelligence and Anti-Money Laundering Act (2002).

Financial Intelligence Centre (FIC) (2023), "Public compliance communication 57: guidance on the definition regarding crypto asset service providers in terms of schedule 1 of the financial intelligence Centre act", available at: www.fic.gov.za/wp-content/uploads/2023/09/2023.07-PCC-PCC-57-CASPs.pdf (accessed 1 July 2024).

Financial Markets Act (2012), No. 19/2012.

Financial Sector Conduct Authority (FSCA) (2022), "Financial advisory and intermediary services act, 2002: declaration of a cryptoasset as a financial product under the financial advisory and intermediary services act (notice 1350), general notices, 47334", p.3.

Financial Sector Conduct Authority (2024), "About us", available at: www.fsca.co.za/Pages/About-Us.aspx#:~:text=The%20FSCA%20is%20the%20market,and%20administrators%2C%20and%20market%20infrastructures (accessed 5 July 2024).

Financial Services Act (2007), No. 14/2007.

HM Treasury (2023), "Future financial services regulatory regime for cryptoassets", available at: https://assets.publishing.service.gov.uk/media/653bd1a180884d0013f71cca/Future_financial_services_regulatory_regime_for_cryptoassets_RESPONSE.pdf (accessed 3 July 2024).

Krige, S. and Laskov, H. (2018), "Bye bye FSB, hello FSCA", available at: www.werksmans.com/legal-updates-and-opinions/bye-bye-fsb-hello-fsca/#:~:text=As%20of%201%20April%202018,to%20know%20about%20this%20development (accessed 5 July 2024).

Marella, V., Upreti, B., Merikivi, J. and Tuunainen, V.K. (2020), "Understanding the creation of trust in cryptocurrencies: the case of bitcoin", *Electronic Markets*, Vol. 30 No. 2, pp. 259-271, doi: 10.1007/s12525-019-00392-5.

Ministry of Finance and Public Enterprises (2023), "Virtual assets act, 2023: designation of regulatory authority in terms of section 5 of virtual assets act, 2023 (notice 219), government gazette, 8148", p.2.

Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations (2017).

National Government of South Africa (2024a), "Financial sector conduct authority (FSCA)", available at: https://nationalgovernment.co.za/units/view/98/financial-sector-conduct-authority-fsca (accessed 18 August 2024).

National Government of South Africa (2024b), "Financial intelligence Centre (FIC)", available at: https://nationalgovernment.co.za/units/view/227/financial-intelligence-centre-fic (accessed 18 August 2024).

National Treasury (2023), "Fact sheet: what does FATF greylisting mean for a country?", available at: www.treasury.gov.za/comm_media/press/2023/2023022501%20FATF%20Grey%20Listing%20Fact%20Sheet.pdf (accessed 18 August 2024).

Ozili, P.K. (2022), "Decentralized finance research and developments around the world", *Journal of Banking and Financial Technology*, Vol. 6 No. 2, pp. 117-133, doi: 10.1007/s42786-022-00044-x.

Proceeds of Crime Act (2002), No. 1/2002.

Rettig, R., Mosier, M. and Gilman, K. (2024), "Genuine DeFi as critical infrastructure: a conceptual framework for combating illicit finance activity in decentralized finance", doi: 10.2139/ssrn.4607332.

Schmidt, A. (2021), "Virtual assets: compelling a new anti-money laundering and counter-terrorism financing regulatory model", *International Journal of Law and Information Technology*, Vol. 29 No. 4, pp. 332-363, doi: 10.1093/ijlit/eaac001.

Staples, P. and Asolo, P. (2024), "What's next for UK cryptoassets regulation?", available at: www.grantthornton.co.uk/insights/whats-next-for-uk-cryptoassets-regulation/#:~:text=For%20now%2C%20cryptoassets%20are%20largely,definition%20of%20'specified%20investments (accessed 17 August 2024).

Triple, A. (2024), "The state of global cryptocurrency ownership in 2024", available at: www.triple-a.io/cryptocurrency-ownership-data (accessed 15 September 2024).

Utkina, M., Samsin, R. and Pochtovyi, M. (2023), "Financial intelligence (monitoring) of the transactions with virtual assets: new legislation and best practices of foreign countries", *Journal of Money Laundering Control*, Vol. 26 No. 2, pp. 349-360, doi: 10.1108/JMLC-12-2021-0136.

Van Wyk, J. (2023), "South Africa's imminent greylisting: 'sword of damocles' or a wake-up call for our economy?", *TAXtalk*, Vol. 2023 No. 98, pp. 22-26, doi: 10.10520/ejc-taxtalk-v2023-n98-a10.

Virtual Asset and Initial Token Offerings Services Act (2021), No. 21/2021.

Wille, G. (1942), "Comparison of English and South African law", *South African Law Journal*, Vol. 59, pp. 124-137.

Further reading

Bar Council of India (2025), "Legal system and profession in the United Kingdom", available at: www.barcouncilofindia.org/info/legal-system-and-profession-in-the-united-kingdom#:~:text=The%20constitutional%20law%20of%20the,near%20the%20Inns%20of%20Court (accessed 15 Feburary 2025).

Financial Services and Markets Act (2000), (Financial Promotion) Order 2005.

Van Coller, A. (2023), "These are not the decisions you are looking for–the courts' duty to follow binding precedent", *Southern African Public Law*, Vol. 38 No. 1, pp. 1-22, doi: 10.25159/2522-6800/13164.

Virtual Assets Act No (2023), No. 10/2023.

Corresponding author
Jacqui-Lyn McIntyre can be contacted at: Jacqui.Mcintyre@nwu.ac.za