2023

Virtual Assets Service Providers Guide to the Prevention of Money Laundering, Terrorist Financing and Proliferation Financing

APPROVED BY THE BOARD OF COMMISSIONERS – 26/1/23
ISSUED BY FINANCIAL SERVICES COMMISSION – 31/1/23
PUBLISHED - 1/2/23
COMMENCEMENT DATE – 1/2/23

Contents

1. Introduction

The BVI Financial Services Commission (the "FSC") has recently expanded its remit to include the supervision of Virtual Asset Service Providers ("VASPs") through the passage of the Virtual Assets Service Providers Act, 2022 (the "Act"). VASPs face unique risks from bad actors who may seek to use VASPs for money laundering ("ML"), terrorist financing ("TF") and proliferation financing ("PF"). These Guidelines have been developed to bring greater awareness of these risks, as well as other risks, including sanctions evasion, illicit financing activities and other financial crimes.

Importantly, these Guidelines also buttress the provisions for compliance with the Anti-Money Laundering Terrorist Financing Code of Practice (the "AMLTFCOP"), the Anti-Money Laundering Regulations ("AML Regulations"), the Regulatory Code (the "RC") and the Financial Services Commission Act (the "FSC Act"). In addition, the updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers published by the Financial Action Task Force (the "FATF") has provided additional clarity of the unique risks impacting VASPs. Therefore, this FATF Guidance has been factored into the development of these Guidelines. All relevant persons including those providing virtual assets services are guided to keep up to date with this and future publications from the FATF that may be relevant to the sector.

Comprehensive AML/CFT compliance by VASPs, and other regulated entities operating in or from within the Virgin Islands ("VI"), also requires reporting and engagement with the FSC and other Competent Authorities including law enforcement agencies. These include the Office of the Governor's Office, Attorney General's Chambers Royal Virgin Islands Police Force (RVIPF), the BVI Financial Investigation Agency (FIA) and the International Tax Authority (ITA)

2. Applicable Persons to Whom these Guidelines Apply

2.1. These Guidelines are relevant for all persons who are operating as VASPs operating in or from within the VI. Any entity wishing to provide virtual asset services in or from within the Virgin Islands is required to be registered by the FSC. VASPs may be registered to operate under the following categories:

- Operate a virtual asset exchange;
- Provide virtual assets custody services; and
- Provide other virtual assets services.

3. Objective

3.1. These Guidelines give clarity on specific AML/CFT obligations for VASPs under BVI law, which includes requirements for robust customer due diligence and enhanced customer due diligence procedures, proper recordkeeping measures, frameworks to fulfil statutory reporting obligations and monitoring and assessment of risks that are present in the use and exchange of virtual assets and in the operations of VASPs themselves. These Guidelines also highlight other critical considerations that VASPs should address to develop and maintain a robust framework that enables strong compliance measures to be effective.

4. AML/CFT/PF Risks and VASPs

4.1. AML/CFT/PF requirements for entities operating in or from within the Virgin Islands are primarily set out in the AMLTFCOP, AML Regulations, Proceeds of Criminal Conduct Act ("PCCA"), Criminal Justice (International Cooperation) Act, 1993, Counter-Terrorism Act, 2021 ("CTA"), Proliferation Financing (Prohibition) Act, 2021 ("PFPA") and the relevant Orders in Council related to terrorism and terrorist financing. Due to the speed in transferring value and the cross-border nature of transactions and other risks, it is important that all VASPs mitigate against the risks of ML, TF, PF, and other illicit activities.

4.2. Section 25 of the Act requires every VASP to take appropriate steps to comply with the provisions of the Act and other enactments relating to ML, TF, and PF. Section 41 of the Act requires VASPs to appoint a Compliance Officer, unless otherwise exempt. The duties of the Compliance Officer include, among other things, the development and implementation of the compliance framework which addresses all areas of operation. The compliance framework must therefore be designed to prevent risks of a VASP being used for ML, TF, PF and other risks. These risks have been documented and reported on by international standard setters and other bodies. Awareness of the risks that exist with the use and exchange of virtual assets as well as operating as VASPs is critical to the development of a resilient compliance framework.

4.3. The FATF published Guidance for the Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers in October 2018. FATF also updated Recommendation 15 and the accompanying Interpretive Note to clarify the application of key international standards in relation to persons and entities that use or engage in business with virtual assets ("VAs") and VASP. This Guidance solidifies VASPs within the scope of entities that are required to have AML/CFT measures in place towards combatting global money laundering and terrorist financing. In September 2020, the FATF also supplemented its Guidance with a Report on Red Flag Indicators of Money Laundering and Terrorist Financing (ML/TF) for Virtual Assets to help persons who may engage with or operate a VASP to detect and promptly report suspicious transactions.

4.4. The FATF Guidance for the Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers was updated in October 2021. FATF Recommendations 15 and 16 were updated because of the advancement of new technologies and VA transfers are of particular importance to VASPs. That includes adherence to the FATF Travel Rule where VASPs must collect originator and beneficiary information for transfers of VAs.

4.5. FATF Recommendations 10 and 11 in relation to customer due diligence and recordkeeping respectively, are especially important to ensure that VASPs collect customer due diligence information and maintain full records for all transactions and customers. VASPs should also consider other FATF Recommendations, and in particular, Recommendations 12, 17 and 19 through 22 in the development of their compliance framework.

5. Risks to be Monitored by VASPs

5.1. VASPs may be exposed to ML/TF/PF and other risks through their engagement with other VASPs operating in jurisdictions that lack an effective framework for the supervision of AML/CFT risks. On this basis, VASPs should take all measures to ensure that risk assessments and proper due diligence are carried out in relation to a foreign VASP (VASP operating in or from within a jurisdiction outside the VI) towards assessing risks. In keeping with FATF Recommendation 15 where a foreign VASP (i.e., a non-Virgin Islands VASP) presents a material risk of ML/TF/PF or other material risks, VASPs should decline engaging in business where a foreign VASP cannot evidence stringent AML/CFT measures and controls. Risks in relation to Peer-to-Peer transactions (P2P business) are also present as it permits individuals to interact and transfer value directly. VASPs should be aware of the material risks that may be present with counterparty VASPs (VASPs for which and with whom they engage in transactions) with whom P2P transactions may be carried out or otherwise facilitated and conduct risk assessments and due diligence in relation to P2P transactions.

5.2. The use of mixers, tumblers, privacy coins, decentralized platforms and other digital tools designed to increase anonymity in the sale or trade of virtual assets are methods that have been observed in illicit activities. These methods can expose VASPs to increased risks of being exposed to or used to further the efforts of bad actors. Additionally, new illicit financing typologies continue to emerge that reduce transparency of transactions that are facilitated by VAs as well as fiat currencies being converted to or from VAs. Therefore, VASPs should take caution to ensure that they investigate suspicious activities and patterns that may indicate emergent risks of ML/TF/PF or other illicit financing risks.

5.3. VASPs must be vigilant against being used to effect layering of virtual assets that further obscure possible criminal activities. Typologies1 continue to emerge in relation to VASPs being used to support criminal activities, including human trafficking, smuggling, sale of narcotics, tax evasion and illegal gambling activities. Therefore, VASPs must be diligent in ensuring that their risk assessment frameworks are regularly updated and calibrated to changes in risks.

6. Institutional Risk Assessments

6.1. VASPs are required to assess the risk inherent in their business, taking into consideration relevant factors, i.e., their customers, countries, or geographical areas to which they are exposed, the products, services, or transactions they offer, and the delivery channels used to access customers. An institutional risk assessment should assist an entity or a professional to holistically understand the ML/TF/PF risks to which it or he or she is exposed and identify the areas that should be prioritised to combat ML/TF/PF. For a VASP, particular attention must be paid to the technology and cyber security risk it faces.

6.2. An important part of the risk assessment is to identify the level of risks posed by each relevant factor and develop a risk rating. VASPs must be able to identify the areas that pose higher risks and apply enhanced measures accordingly.

6.3. Records of the VASP's institutional risk assessment must be maintained and made available to the FSC and all other competent authorities. Such records will include the findings, recommendations and steps taken to implement any recommendations. It is expected that the personnel at the highest level of a VASP (i.e., directors/senior management) will consider and execute the findings of the institutional risk assessment.

7. Matters for Considerations

7.1. Recordkeeping and Transaction Monitoring by VASPs

7.1.1. Section 22 of the Act and Part IV of the AMLTFCOP require VASPs to maintain records that are sufficient to show and explain transactions and fiscal positions, as well as ensure that all customer due diligence records are obtained and maintained. VASPs must also ensure that records are maintained in a manner that allows for retrieval without undue delay as set out by regulation 11 of the AML Regulations.

[1] VASPs should pay attention to typology reports issued by domestic authorities and other international bodies such as FATF, IMF, FSB, Basel etc. For example, FATF Report on Virtual Assets Reg Flag Indicators of Money Laundering and Terrorist Financing.

7.2. Customer Due Diligence

7.2.1. Part III of the AMLTFCOP provides the detailed requirements for undertaking customer due diligence ("CDD"). CDD relates to forestalling and preventing the activity of ML, TF, and PF. VASPs are considered to have business relationships with persons who execute transactions on an ongoing basis or otherwise maintain an account. In such circumstances, VASPs are required to carry out CDD to identify and verify the applicant for business or customer. Similar identity verification is required in the case of one-off transactions.

7.2.2. In addition to carrying out CDD measures when one sets up a business relationship with a customer or carries out an occasional transaction, CDD should also be carried out if the VASP:

- suspects ML, TF or PF;
- determined that the relationship presents a higher-than-normal risk; and
- has any doubt about any information provided by the customer for identification or verification purposes.

7.2.3. To effectively carry out the act of CDD, a VASP must:

- have systems to identify those persons who cannot produce standard documents;
- take account of the greater potential for money laundering in higher risk cases, specifically in respect of politically exposed persons[2];
- not deal with persons or entities if due diligence cannot be executed, or the results are not satisfactory; and
- have a system for keeping customer information up to date.

[2] Politically exposed persons (PEPs) are persons (foreign and domestic) who are, or have been, entrusted with prominent public functions (Heads of state or government, politicians, senior government officials, judicial or military officials, senior executives of statutory bodies, senior political party officials) or who hold prominent functions within an international organisation (senior managers and members of the Board).

7.3. Applying CDD Measures

7.3.1. The extent to which CDD measures are applied may vary, to the extent permitted or required by law, based on the ML/TF/PF risk identified or associated with the business relationship or a one-off transaction. This means that the amount or type of information obtained, or the extent to which this information is verified, must be increased where the risk associated with the business relationship or transaction is higher. It may also be simplified where the risk associated with the business relationship or transaction is lower. It should, however, be noted that applying and adopting simplified CDD measures is not acceptable whenever there is a suspicion of ML or TF or PF, or where specific higher-risk scenarios apply. Additionally, the AMLTFCOP allows VASPs and other relevant entities to utilise technological mechanisms to effect CDD and record keeping. VASPs must be able to demonstrate to the FSC that any technological means are consistent with the requirements to undertake CDD and primarily with respect to identifying and verifying applicants for business and customers, including beneficial owners. Any technological development must neither hinder the exchange of information with the FSC, other competent authorities and law enforcement agencies.

7.4. Simplified CDD Measures

7.4.1. Where a VASP determines that a customer poses a significantly low risk and having regard to the money laundering, terrorist financing and proliferation financing risks identified by a Virgin Islands' national risk assessment, or a risk assessment conducted by a competent authority, law enforcement agency or any other authority with responsibility relating to money laundering, terrorist financing and proliferation financing in the Virgin Islands, simplified CDD measures may be applied. In cases where a VASP determines that simplified CDD measures may be applied, the following actions may be taken:

a) fewer elements of customer identification data may be obtained (production of one form of ID instead of two, for example);
b) less robust identity verification procedures may be employed;
c) collection of specific information or the carrying out of specific measures to understand the purpose and intended nature of the business relationship may not be required (the purpose and nature of the business relationship may be inferred from the type of transactions or business relationship established);
d) the identity of the customer and the beneficial owner(s) may be verified after the establishment of the business relationship;
e) in the case of an existing business relationship, the frequency of customer identification updates may be reduced; and
f) the degree and extent of ongoing monitoring and scrutiny of transactions may be reduced based on a reasonable monetary threshold.

7.5. Enhanced CDD Measures (ECDD)

7.5.1. ECDD refers to the additional steps an entity is required to undertake to limit or manage the risk posed by a customer who poses a higher level of risk. This will be the case in relation, for instance, to a politically exposed person, to a person from a jurisdiction that is considered to pose a high ML/TF risk or a person who trades in products that are of a complex nature. In cases where a VASP determines that ECDD measures may be applied, the following actions may be taken:

a) additional identifying information from a wider variety or more robust sources should be obtained and corroborated and the information used to inform the individual customer's risk profile;
b) additional searches (e.g., verifiable adverse internet searches) should be carried out to better inform the individual customer's risk profile;
c) where appropriate, further verification procedures should be undertaken on the customer or beneficial owner to better understand the risk that the customer or beneficial owner may pose to the VASP;
d) the source of funds and wealth involved in the transaction or business relationship should be verified to satisfy the VASP that they do not constitute the proceeds of crime;
e) the information provided with regard to the destination of funds and the reasons for the transaction should be evaluated; and
f) additional information about the purpose and intended nature of the transaction or the business relationship should be sought and verified.

7.5.2. VASPs should also consider the following specific higher-risk factors, which may also trigger the need to conduct ECDD:

(a) The ability of customers to:
    (i) operate more than one account with the VASP; and
    (ii) operate accounts on behalf of third parties.
(b) The customer:
    (i) is involved in virtual asset mining operations (either directly or indirectly through relationships with third parties) that take place in a high-risk jurisdiction, relate to higher-risk VAs (such as privacy coins) or where its organisation gives rise to higher risk;
    (ii) uses VPN, TOR, encrypted, anonymous or randomly generated email or a temporary email service;
    (iii) requests an exchange to or from cash, privacy coins or anonymous electronic money;
    (iv) sends VAs to a newly created address;
    (v) persistently avoids thresholds through smaller transactions;
    (vi) sends or receives VAs to/from peer-to-peer exchanges, or funds/withdraws money without using the platform's other features; and
    (vii) exploits technological glitches or failures to his advantage.

(c) The VA comes from, or is associated with, the darknet or other illegal/high-risk sources, such as an unregulated exchange, or is associated with market abuse, ransomware, hacking, fraud, Ponzi schemes, or sanctioned bitcoin addresses.

7.5.3. Where a VASP is unable to verify the identity of an individual, it should not enter a business relationship or execute a one-off transaction with that individual. If the business relationship already exists, the VASP should terminate the business relationship. In all circumstances, the VASP should consider filing a suspicious transaction report with the FIA in relation to the customer or individual.

7.6. Ongoing CDD and Transaction Monitoring

7.6.1. Once a business relationship is established, the VASP has an obligation to ensure that CDD measures are carried out on an ongoing basis. Such measures are required to determine whether executed transactions are consistent with the VASP's information about the customer and the nature and purpose of the business relationship, wherever appropriate. These ongoing CDD measures should allow VASPs to identify changes in customer profiles (for example, their behaviour, use of products and the amount of money involved), and to keep them up to date, which may require the application of enhanced CDD measures.

7.6.2. An essential component in identifying transactions that are potentially suspicious is transaction monitoring. Transactions that do not fit the behaviour expected from a customer's profile or that deviate from the usual pattern of transactions may be potentially suspicious. Monitoring should, therefore, be carried out on a continuous basis.

7.6.3. Transaction monitoring systems may be manual or automated based on the volume of transactions processed by a VASP on a regular basis. However, where automated systems are used, VASPs should understand their operating rules, verify their integrity on a regular basis and check that they take account of the identified ML/TF/PF risks.

7.6.4. The level of transaction monitoring should be based on a VASP's institutional risk assessment and individual customer risk profiles, with enhanced monitoring being executed in higher-risk situations. The adequacy of a VASP's monitoring system, and the criteria used to determine the level of monitoring to be implemented, should be reviewed regularly to ensure that they are in line with the VASP's AML/CFT risk programme.

7.6.5. Transactions performed or initiated by an outsourced party must also be subject to regular monitoring under the same conditions as transactions of the VASP itself. Such monitoring should be conducted under the VASP's control by the VASP itself, or in collaboration with a third party, based on appropriate agreement complying with the requirements of the AMLTFCOP.

7.6.6. VASPs should consider creating thresholds in relation to VAs, whether based on an equivalent monetary value or other thresholds based on a risk-based approach, to determine which activities will be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the established risk levels. Criteria and parameters used for customer segmentation and for the allocation of a risk level for each customer group should be transparent and clearly documented. Additionally, VASPs should properly document, retain and communicate to the relevant personnel, including senior management and front-line staff, the results of their monitoring, as well as any queries raised and resolved. VASPs must also undertake relevant training.

8. VA Transfers and Travel Rule

8.1. The FATF review of risk trends impacting businesses that included VA and VASPs resulted in the publication of the Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers. In their work, the FATF brought VASPs under the umbrella of FATF Recommendation 15 on New Technologies.

8.2. The FATF's work also led to amendments to Recommendation 16 to include VASPs and the introduction of the so-called FATF Travel Rule, where VASPs are required to share originator and beneficiary information in the exchange of virtual assets. It is important to note that the Travel Rule is in line with existing due diligence requirements for VA transfers. As such and required by Part VA of the AMLTFCOP, VASPs are expected to adhere to AML/CFT requirements that are in place for VA transfers. VASP should pay particular attention to the definition of obliged entities and the need to ensure compliance with whom it does transactions.

8.3. VASPs are guided to note the risks that bad actors would seek to exploit VASPs and VAs to obscure the source of criminal proceeds towards furthering criminal activities. Therefore, VASPs are required to assess ML and TF risks posed by counterparty VASPs. This requires VASPs to conduct due diligence and risk assessments in relation to counterparty VASPs. Given the speed and scale of transactions involving virtual assets, it is vital that VASPs develop and implement robust systems that allow for compliance with the Travel Rule, as well as mitigate against the threat of ML, TF, and PF.

VASPs are guided to ensure that they keep abreast of future developments and publications by the FATF.

9. Targeted Financial Sanctions and Sanction Screening

9.1. VASPs must ensure that their compliance framework allows for effective ongoing CDD and transaction monitoring to detect and prevent ML, TF, and PF. This Ongoing CDD and transaction monitoring must also allow for immediate sanctions screening. Consequently, it is expected that VAPS should be able to screen its client base within 24 hours and identify any designated persons and take appropriate measures in keeping with the requirements including freezing and reporting. VASPs must also ensure that they have mechanisms in place to promptly act on new sanctions. Such mechanisms could include subscription to the UK Office of Financial Sanctions Implementation (OFSI) website for the most up to date sanctions list to ensure that customers, clients, or applicants for businesses are not designated persons. Additionally, VASPs must have mechanisms in place to regularly keep up-to-date with updates to the BVI sanctions regime, which can be found here. Where a VASP has detected a customer or assets of someone that has been the subject of a sanction, they are required to take freezing actions, prohibit transactions and report to BVI Competent Authorities (Governor's Office, FSC and FIA) without delay.

10. Filing of Suspicious Activity/Transaction Reports

10.1. VASPs must ensure that their compliance framework includes mechanisms, polices, procedures and internal controls to promptly report suspicious activities internally and report suspicious transactions to the FIA. VASPs must ensure that any mechanism accounts for, amongst other things, attempted activity, transaction, or customer relationship that the VASP has refused.

10.2. VASPs' internal controls must detail how an employee should report a suspicious activity and to whom. An internal SAR log should be maintained and should indicate, amongst other things, the date the suspicious activity took place, the date the report was made, the circumstances surrounding the activity and the outcome of the investigation.

10.3. Accordingly, VASPs are required to appoint a qualified individual as its Money Laundering Reporting Officer ("MLRO") to file suspicious activity reports ("SARs"). VASPs are guided to note that section 17(1) of the AMLTFCoP requires the MLRO to make a report to the FIA of every suspicious transaction or customer. This report must be made in a form that ensures compliance with section 55 of the AMLTFCOP. Therefore, VASPs are guided to adhere to requirements of reporting SARs and STRs as a means of minimising risk including operational and reputational risks.

10.4. Once a SAR/STR has been filed with the FIA, VASPs should take swift action to mitigate the risk of being abused by that customer for criminal purposes. This may mean reassessing the risk entailed in the business relationship and escalating the relationship to management. VASPs should also be mindful that if it or an employee knows or suspects that an ML/TF/PF investigation is happening or about to take place, it is an offence to disclose information to anyone else, which is likely to prejudice that investigation. Equally, if the VASP knows or suspects that a disclosure of suspicion has been or is being made, it is an offence to leak information that could prejudice any investigation conducted. This extends beyond ML investigations to disclosures which would prejudice a confiscation investigation. Interfering with documents and other materials relevant to an investigation is also an offence. VASPs must therefore ensure that all staff are appropriately trained and understand their legal obligations in relation to tipping off.

10.5. Some examples of suspicious patterns or behaviour include the following (this should be read in conjunction with any other examples included in the AMLTFCOP, other documents issued by the FIA or relevant competent authority in the VI or other international standard setters such as FATF):

a) Persistently avoids thresholds through smaller transactions;
b) Sends or receives VAs to/from peer-to-peer exchanges or funds/withdraws money without using the platform's other features;
c) Uses anonymising techniques for VA transfers, including the use of privacy wallets, mixers and tumblers and other methods that enhance anonymity;
d) Use of multiple wallets and/or P2P platform-associated wallets;
e) Engages in churning-like transactions (excessively frequent buying and selling of VAs);
f) The VA comes from, or is associated with, the darknet or other illegal/high-risk sources, such as an unregulated exchange, or is associated with market abuse, ransomware, hacking, fraud, Ponzi schemes, or sanctioned bitcoin addresses;
g) Use of domain name registrars (DNS) that suppress or otherwise redact the owners of domain names to access VASP platforms; and
h) Exploits technological glitches or failures to their advantage.

10.6. There may be other emerging practices that are indicative of suspicious patterns or behaviour. The FATF Report – Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing should also be considered by VASPs in the development of their risk assessment frameworks. As such, VASPs are to remain vigilant and review publications of typologies of risks in relation to virtual assets and operators of VASPs. VASPs should also pay particular attention to their specific circumstances and customers to be able to identify suspicious factors which may present themselves or be unique to the VASP, its services or its clients.

11. Other Risk Indictors or Factors Impacting Risk of ML/TF/PF

11.1. Privacy and Anonymity

11.1.1. Features and characteristics of VAs lend themselves to a higher ML/TF/PF risk. Therefore, VASPs should be aware that several types of virtual assets that may be held in custody or alternatively, used in transactions may be associated with privacy-enhancing features. Which potentially obfuscates transactions or activities and inhibits a VASP's ability to implement CDD requirements and other effective measures to prevent ML, TF, PF, and related activities. Examples of these privacy-enhancing features are as follows:

11.1.2. Anonymity Enhanced Technology, Transaction and Features such Anonymity Enhanced Currencies (AEC), Mixers or tumblers, privacy wallets and clustered wallets;

- Obfuscated ledger technology;
- Un-hosted wallets;
- Privacy coins;
- Internet Protocol (IP) anonymizers;
- Stealth addresses;
- Non-interactive zero-knowledge proofs; and
- VAs held or used in a transaction is associated with escrow services.

11.1.3. The speed inherent in the exchange and transfer of VAs also allows for funds to be moved swiftly within countries and internationally. This speed facilitates a range of financial activities, from money or value transfer services to securities, commodities, or derivatives-related activity, among others. Additionally, VAs also allow for non-face-to-face business relationships. Therefore, VASPs are advised to apply risk-based assessments of their customers and for transactions based on risk factors, which may include the type of business being conducted, as well as the value and/or volume of transactions being executed. Ideally, VASPs should consider embedding blockchain analytics and other means of monitoring and risk-assessing transactions and identifying transaction patterns to mitigate against ML, TF, and PF risks, particularly where the risk is significant, or the volume of transactions is substantial. VASPs should also employ systems that can identify proximal risks, which may include dusting, blacklisted addresses, and other suspicious activities. The VASP should also be able to provide such information upon demand to relevant competent authorities immediately.

11.2. Cross Border Nature

11.2.1. VASPs', by their nature of operations, are widely interconnected to other parties, including other VASPs and traditional financial institutions. The breadth of their operations to multiple parties and multiple jurisdictions may give rise to increased ML, TF, and PF risks. Therefore, VASPs will need to ensure that they are able to effectively apply all AML/CTF processes in the jurisdictions in which they operate and compensate for any additional risks introduced by the cross-border nature of a transaction on a risk basis. Such measures should be documented and available to Competent Authorities upon request.

11.3. Decentralised Nature of VASPs Business Models

11.3.1. VASPs platforms may be established as centralized or decentralized (or a hybrid where there are bridging applications being used by a VASP). Where a VASP is fully or significantly decentralised, there is typically no central server or service provider that has overall responsibility for identifying users, monitoring transactions, reporting suspicious activity, and acting as a contact point for law enforcement. Consequently, individuals and transactions may not be subject to risk assessment and mitigation processes equivalent to those required by AML/CTF regulation. Where VASPs deal with funds originating from decentralised systems, risk-based mitigation measures, such as blockchain analytics, should be applied. The VASP must be able to demonstrate that the risk posed by doing business with these entities are fully mitigated.

11.3.2. Also, where the VASP or the proposed VASP itself operates in a decentralised manner there will be implications for how supervision will be undertaken and whether and on what basis approval will be granted. VASPs should note that issues such as these have been identified by FATF in various reviews and VASPs are urged to account for these FATF reviews when undertaking activities including risk assessment of itself, other VASPs for which it does business, other third-party service providers and clients/customers. The FSC as supervisor of VASPs is unlikely to approve any VASP unable to mitigate its risk or provide clear indication of who will be responsible for the VASP including the central persons responsible for activities on a decentralised exchanged. Approval will be withheld in all cases where this cannot be proven.

11.4. Nature of the Blockchain: Acceptability, Immutability and Convertibility

11.4.1. VAs have experienced increasing acceptability as a form of payment during the last decade. This broad acceptance, coupled with the fluidity of which persons may exchange VAs for other VAs, fiat currency, or a combination of both, presents increased difficulty in tracing some transactions. Transactions executed using VAs are recorded on relevant blockchains (though some transactions may occur using federated sidechains). Based on the inherent recording characteristics of blockchain technology, transactions may be immutable (i.e., unalterable). The use of VAs allows for blockchain analytics to be employed with other tools to mitigate against emerging risks.

12. Employee Screenings

12.1. VASPs must ensure that they screen their employees in accordance with section 49 of the AMLTFCOP. To safeguard against ML/TF/PF and other risks, measures must also be in place to assess the competence and probity of employees at the time of recruitment and intermittently thereafter. These assessments of employees must include background checks as well as an assessment of integrity, skills, knowledge, and expertise to ably carry out their functions. Additional assessments and screening of employees must also be carried out where there is an anticipated change in their role or functions towards mitigating operational and compliance risks. This is of particular importance where the employee is responsible for the implementation of or monitoring of AML/CFT controls, which may occur directly in relation to the compliance function or indirectly in relation to other functions.

12.2. VASPs must also ensure that the screening of employees is proportionate to the ML/TF/PF risks to which that employee may be exposed to, regardless of the level of seniority of any employee. In addition, systems must be established to address potential conflicts of interest for staff with AML/CFT responsibilities. VASPs must also be aware of their responsibility to report employee misconduct to the FSC, and where relevant, any other competent authority.

13. Powers of the FSC

13.1. The FSC's powers include the ability to inspect a regulated entity or any other entity that falls under the supervisory remit of the FSC. Inspections may occur without notice and include a review of compliance against AML/CFT laws, as well as other regulatory requirements. Where a VASP may be operating in or from within the VI but has not been registered, the remit of the FSC extends to such entities so far as it relates to the ability to take enforcement action for an unauthorised business. The FSC's powers also include its ability to take enforcement action for non-compliance with financial services legislation, including AML/CFT legislation, against a VASP, its directors, shareholders, and senior officers.

14. Information Exchange

14.1. Information exchange between VASP and other financial institutions, as well as regulatory and law enforcement authorities, is an important part of a VI's strategy for combating ML/TF/PF and should also form part of the VASP's ongoing controls. Where authorities are armed with suspicion or evidence of a person's link or suspected link to ML, TF, or PF, they should be able to share that information with the VASPs so that the latter can better engage its processes in dealing with such a person. Conversely, VASPs should also be able to share general information about the type and nature of suspicious activities that may be linked to ML, TF or PF with other financial institutions and government agencies, including the regulator, subject to the requirements to ensure that there is no tipping off related to a filing of a SAR. This can only help to strengthen the VASP sector and insulate it from abuse and misuse for ML, TF, and PF purposes.

14.2. There are various types of information that can be shared between regulatory and law enforcement agencies and VASPs. Such information may include:

- ML/TF/PF risk assessments;
- General feedback on suspicious transaction reports and other relevant reports;
- Typologies of how money launderers or terrorist financiers have misused VASPs;
- Targeted unclassified intelligence which, subject to appropriate safeguards such as confidentiality agreements, may be shared with VASPs, either collectively or individually; and
- Sanctions lists issued through the Governor's Office and published by the FSC and FIA that include countries, persons, or organisations whose assets or transactions should be frozen pursuant to targeted financial sanctions.

14.3. Domestic cooperation and information exchange between VASPs and the FSC (as the supervisor of the VASP sector), among law enforcement and intelligence agencies, and between the FIA and FSC is extremely important in the effective monitoring and/or supervision of the VASP sector.

14.4. Cross-border information sharing between authorities and the VASP sector with their international counterparts are also vitally important given the multi-jurisdictional reach of many VASPs. VASPs must ensure that they fully comply with the CDD and records keeping required, as well as all other requirements of the AMLTFCOP and AML Regulations, ensuring that the VI is able to meet its international obligations, including those relating to beneficial ownership.

15. Overarching Requirement for Compliance

15.1. All VASPs must remain vigilant in relation to evolving ML, TF, and PF threats, as well as other threats that can negatively impact their operations. To mitigate against these threats and risks, VASPs must be diligent in the application of AML/CFT/PF measures. These measures must be holistic and integrate prudent governance and modern risk management strategies with a robust compliance framework. VASPs must remain agile and embed systems to allow for continual improvement in the efficiency and effectiveness of compliance.