CONSULTATION DOCUMENT

APPLICATION OF ANTI-MONEY LAUNDERING AND COUNTERING THE FUNDING OF TERRORISM OBLIGATIONS TO THE VIRTUAL FINANCIAL ASSETS SECTOR

Issued: 31 October 2018
Closing Date: 23 November 2018
The Virtual Financial Assets Act is set to come into force on 1 November 2018. The said Act provides for VFA Agents, issuers and licence holders to be considered as subject persons in terms of the Prevention of Money Laundering and Funding of Terrorism Regulations (“PMLFTR”). Furthermore, the said Regulations are in the process of being amended so as to explicitly bring the activities of VFA Agents, issuers and licence holders within the ambit of the PMLFTR.

Being conscious that issuers and licence holders may not be very familiar with the anti-money laundering and counteracting the funding of terrorism (“AML/CFT”) obligations arising from the PMLFTR and that Virtual Financial Assets activities present particular risks and challenges, the Financial Intelligence Analysis Unit (“FIAU”) has decided to provide VFA Agents, issuers and licence holders with sector-specific guidance on how they can meet their AML/CFT obligations. This document, which was prepared together with the Institute of Financial Service Providers and with the input of the Malta Financial Services Authority, sets out the proposals of the FIAU in this regard. Whilst it is acknowledged that this document is not final, it already sets out how the FIAU considers that VFA agents, issuers and licence holders can meet their AML/CFT obligations.

Prospective VFA Agents, issuers, licence holders and interested parties are therefore invited to consider the proposals contained in this document and provide the FIAU with any feedback they may have. The consultation period ends on 23 November 2018 and anyone wishing to submit feedback can do so by email on the following email address – legal@fiumalta.org.

The FIAU wishes to draw the attention of prospective VFA Agents, issuers and licence holders that simultaneously with this consultation exercise, it has also issued a revised version of its Implementing Procedures – Part I for consultation. The Implementing Procedures – Part I is the general part of the implementing procedures issued by the FIAU and is applicable to all subject person, including to VFA Agents, issuers and licence holders. To be able to appreciate any sector-specific Implementing Procedures issued by the FIAU, such as those intended for the VFA Sector, it is necessary to read the same together with the Implementing Procedures - Part I.

Prospective VFA Agents, issuers and licence holders are therefore invited to also consider the proposals made in relation to the FIAU’s Implementing Procedures – Part I and participate in the relative consultation exercise.
Introduction

1. Background

The evolving financial services landscape has been heavily influenced by virtual financial assets ("VFAs"), which operate outside the traditional financial system. A VFA is defined as ‘any form of digital medium recorrdation that is used as a digital medium of exchange, unit of account or store of value and that is not (a) electronic money; (b) a financial instrument; or (c) a virtual token\(^1\). Thus, a VFA is a medium of exchange that allows for value to be held and exchanged in an electronic, non-physical manner, is not a FIAT currency but may be exchanged for real and/or virtual goods and services, and allows for peer-to-peer transfers.

VFAs can be “centralized”, i.e. they are issued and controlled by a single company or entity, or “decentralized”, i.e. there is no central authority that creates or manages them but, rather, these functions are carried out collectively by a network of selected VFA users who are not subject to any form of regulation (e.g.: Bitcoin).

In addition, VFAs can be “convertible” or “non-convertible”, depending on whether they can be exchanged for fiat currency or otherwise. Given that they allow greater levels of anonymity, or in some cases complete anonymity, when compared to traditional non-cash payment methods, both types of VFAs are vulnerable to abuse for ML/FT purposes.

In the light of these developments, the European Union has extended the scope of its anti-money laundering/countering the funding of terrorism ("AML/CFT") regime to parts of this area as well. In terms of Directive (EU) 2018/843\(^2\) (more commonly referred to as the 5\(^{th}\) AMLD) persons providing services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies, as well as persons engaged in exchange services between virtual currencies and fiat currencies, are to be considered as obliged entities and are to have AML/CFT obligations.

Although Member States, including Malta, have until 10 January 2020 to transpose the 5\(^{th}\) AMLD into national law, Malta has recognised the heightened risks associated with VFAs and has taken the initiative to anticipate this framework by immediately bringing all VFA service providers within the scope of its domestic AML/CFT framework. To this end, VFA Agents, Issuers and Licence Holders, as defined in Article 2(2) of the Virtual Financial Assets Act ("VFAA"), are considered as ‘subject persons’ in terms of the Prevention of Money Laundering and Funding of Terrorism Regulations\(^3\) ("PMLFTR").

2. About these Implementing Procedures

The purpose of these Sector-Specific Implementing Procedures is to introduce the VFA sector to AML/CFT obligations and provide guidance specifically on how VFA Agents, Issuers and Licence Holders (collectively referred to as “VFA Operators”) are to implement the AML/CFT obligations

---

\(^1\) Article 2(2) of the Virtual Financial Assets Act [Cap. 590 of the Laws of Malta].


\(^3\) Subsidiary Legislation 373.01.
arising from the Prevention of Money Laundering Act⁴ ("PMLA"), the PMLFTR and any Implementing Procedures issued by the FIAU. They also aim to assist VFA Operators in better understanding particular money laundering and financing of terrorism ("ML/FT") risks that they may face due to the nature of VFAs, and related products, services and activities.

These Implementing Procedures are structured as follows:

- Part A – applies to VFA Operators;
- Part B – applies to VFA Agents;
- Part C – applies to VFA Issuers;
- Part D – applies to VFA Licence Holders.

These Sector-Specific Implementing Procedures complement the Implementing Procedures – Part I and are to be read in conjunction therewith. It is important to note that, unless otherwise stated, the omission of any reference in this document to particular AML/CFT obligations is not to be considered as tantamount to the inapplicability of the same to VFA Operators. Moreover, in so far as the Implementing Procedures – Part I are not in conflict with these Sector-Specific Implementing Procedures, they are still applicable to VFA Operators. In case of any such conflicts, these Sector-Specific Implementing Procedures are to prevail over the relevant provisions of the Implementing Procedures – Part I.

---

⁴ Cap. 373 of the Laws of Malta.
Part A: General Section applicable to Virtual Financial Assets Agents, Issuers, and Licence Holders

1. ML/FT Risks associated with VFAs

The Financial Intelligence Analysis Unit ("FIAU") considers that transactions made in or using VFAs represent a higher risk of ML/FT than transactions conducted using traditional non-cash payment methods (e.g.: debit cards, bank transfers etc.) or through regulated payment service providers. This is particularly true in the current environment where international standards for the regulation of VFAs and related service providers are still in their infancy.

This section provides examples of risk factors that are generally inherent to the products and services offered by VFA businesses. These risks should be factored into the business risk assessment carried out by VFA Operators and effective controls should be put in place to mitigate said risks.

Anonymity

- VFAs offer greater anonymity than traditional non-cash payment methods and are therefore more likely to be used for criminal purposes, including the evasion of international sanctions, avoiding detection and identification by victims and/or law enforcement agencies etc.;
- VFAs can be traded on the internet, typically through non-face-to-face customer relationships;
- VFAs permit anonymous funding;
- VFAs may also permit anonymous transfers if the sender and the recipient are not adequately identified, especially where such transfers are not handled by entities that are subject to AML/CFT obligations;
- Decentralised VFA payment providers are particularly vulnerable to anonymity risks (for example, by design, Bitcoin addresses functioning as accounts have no names or other customer identification attached to them);
- The VFA protocol does not require, or provide, identification and verification of participants, and the historical transaction records generated on the blockchain or other distributed ledgers are generally not associated with real world identities but, rather, with a unique account or wallet address which could be used by multiple persons for a variety of purposes;
- Software products have been developed to enhance decentralised VFA’s anonymity features, including mixers, tumblers, foggers and anonymisers, meaning that even if one were to track the relevant IP address, the effectiveness of this mitigating measure may be somewhat limited.

Other risk drivers

- VFA-related services can be accessed via the internet (including via mobile phones) and can be used to make cross-border payments and funds transfers to and from anywhere, including high risk jurisdictions;
- Near real-time settlement and irrevocability of transactions (no chargebacks);
- Challenges in tracing the flow of VFAs, particularly where the VFAs have features which offer higher levels of anonymity;
- A number of VFAs can be used and are accepted as means of payment on the dark web.
In the light of VFAs’ level of anonymity, the ease with which they can be acquired and converted, and the borderless nature of VFAs, ML/FT risks are to be considered as elevated. Annex I hereto provides examples of how particular VFAs and characteristics referred to above, have been exploited for criminal purposes and further highlight the ML/FT risks associated therewith.

2. Risk Assessment

VFA Operators should be aware that the AML/CFT regulatory framework that is applicable to them as subject persons adopts a risk-based approach, i.e. it requires subject persons to adopt measures, policies, controls and procedures that are commensurate to the ML/FT risks to which they are exposed to prevent and mitigate the said risks from materialising themselves.

The risk-based approach recognises that the ML/FT risks faced by each sector and each subject person are different, and allows for resources to be invested and applied where they are most required. It is diametrically opposed to a prescriptive tick-box approach and entrusts subject persons with significant discretion in its application. Thus, a risk-based approach envisages the application of checks that are proportionate to the assessed risk. High risk areas should be subjected to enhanced procedures, whilst simplified or reduced controls may be applied in areas of low risk.

The risk-based approach envisages the application of a risk management process in dealing with ML/FT, including recognising the existence of risks, undertaking a risk assessment, and implementing systems and strategies to manage and mitigate the identified risks.

The cornerstone of the risk-based approach is the business risk assessment which has to be carried out and reviewed at different stages of a subject person’s activities. This assessment allows the subject person to identify its ML/FT vulnerabilities and the ML/FT risks it is exposed to. On this basis, the subject person will be able to draw up, adopt and implement AML/CFT measures, policies, controls and procedures that address any identified risks.

However, each customer exposes the subject person to different risks. A customer risk assessment must therefore be carried out so that VFA Operators are able to identify potential risks upon entering into a business relationship with, or carrying out an occasional transaction for, a customer, as the case may be. This assessment enables VFA Operators to develop a risk profile for the customer and to categorise the ML/FT risk posed by such customer as low, medium or high.

VFA Operators must subsequently apply the AML/CFT measures, policies, controls and procedures adopted in a manner that they address the specific ML/FT risks arising from the particular business relationship or occasional transaction. Thus, it is important that the said measures, policies, controls and procedures be sufficiently flexible to prevent and mitigate specific risks, independently of the extent in which they may potentially manifest themselves. How these measures, policies, controls and procedures are to be applied to particular risk scenarios has to result from the Customer Acceptance Policy adopted by VFA Operators.

The following sections explain the two types of risk assessments that VFA Operators are bound to carry out and provides guidance on how such operators are expected to conduct such risk assessments.
2.1 The Business Risk Assessment

The business risk assessment process is set out in Chapter 3 of the revised Implementing Procedures – Part I. Broadly speaking, the business risk assessment process comprises four steps:

i. Risk identification – Identify the main ML/FT risks associated with customers, products and services, business practices/delivery channels, and geographical locations;

ii. Risk assessment / measurement – Measure the size and importance of ML/FT risks, including their likelihood of their materialising and their impact on the subject person;

iii. Risk management – Manage the identified ML/FT risks by applying measures, policies, controls and procedures which minimise as much as possible the identified risks;

iv. Risk monitoring and review – Monitor, review and keep up to date the ML/FT business risk assessment, while documenting the assessment process and any updates to the business risk assessment and the corresponding AML/CFT measures, policies, controls and procedures.

Any such assessment, revisions thereof, as well as any decision taken in relation thereto, have to be documented and approved by the Board of Directors or equivalent management body of the subject person. External consultants can also be engaged to assist in the carrying out of this process but responsibility for the same will always rest with the subject person.

Without prejudice to the generality of the foregoing, VFA Operators have also to consider the following:

Extent of the Business Risk Assessment

VFA Operators are to ensure that their business risk assessment is commensurate to the size and nature of their business activities, i.e. it should reflect the complexity of their business – the more numerous the services/products offered and the more complex the business structure adopted to deliver the same, the more detailed the business risk assessment should be. Appropriate safeguards have to be implemented to mitigate all related ML/FT risks.

In addition to the above, the business risk assessment should also consider the inherent risk factors referred to in Parts B to D of these sector-specific Implementing Procedures with a note confirming which of the listed factors are applicable to the VFA Operator’s business and why. For those that are applicable, steps have to be taken and processes put in place to mitigate the identified risks. All of this should be duly documented as part of the business risk assessment process.

The risk factors referred to in these Implementing Procedures are intended to supplement those referred to in the revised Implementing Procedures – Part I. Moreover, risks that are identified through any supranational or national risk assessment and which are of relevance to VFA Operators should also be considered when carrying out the business risk assessment as should any other risk factor referred to in reports published by reputable international bodies.

Application of the AML/CFT requirements

The business risk assessment should include a note identifying any difficulties the VFA Operator is likely to face in complying with their AML/CFT requirements incumbent upon them in terms of the
PMLA, the PMLFTR and any Implementing Procedures issued by the FIAU, whilst also detailing the measures that have been put in place to combat each of these difficulties.

VFA Operators will be expected to demonstrate to the FIAU how they have been able to overcome such challenges in order to comply with the AML/CFT requirements. Where such subject persons are not in a position to comply with the AML/CFT requirements, they should assess whether additional mitigating measures are warranted in order to secure compliance or whether the provision of the particular VFA-related services, products or activities should not be undertaken or otherwise discontinued. Such decisions should be in line with the risk appetite of that particular subject person. However, independently of the decision taken, the subject person will always remain responsible for compliance with its AML/CFT obligations.

*Updating the Business Risk Assessment*

Due to the nature of the rapidly evolving sector, VFA Operators are to review their business risk assessment at least on a six-monthly basis to identity whether it needs to be updated. This six-monthly review is without prejudice to any other review or update to the business risk assessment that may become necessary in the interim period in view of any developments to the VFA Operators’ business structure/activities (e.g. starting offering new services or products, accepting new payment methods, targeting new markets etc.), the environment in which one operates or any other developments that may influence the ML/FT risks to which the VFA Operator is exposed.

### 2.2 Customer Risk Assessment

In addition to the business risk assessment, VFA Operators should also assess specific ML/FT risk factors associated with the particular business relationship being entered into or occasional transaction to be carried out. Hence the obligation to carry out a customer risk assessment prior to enter into any such relationship or carry out an occasional transaction. Through the customer risk assessment, a VFA Operator will be able to better understand the source and level of risk it is being exposed to and be able to mitigate the same through the application of its AML/CFT measures, policies, controls and procedures.

As with all types of risk assessments, a holistic approach should be adopted, taking into account all relevant ML/FT risk factors. The hereunder section provides a non-exhaustive list of higher risk factors that are relevant to VFA Operators and that should be considered when carrying out customer risk assessments. Further guidance on the carrying out of customer risk assessments may be found in Chapter 3 of the revised Implementing Procedures - Part I.

*Customer behaviour and activities*

- The customer is overly secretive or evasive about where the money is coming from, and why he is using VFAs;
- The customer is using anonymiser software, a mixer or similar systems or software solutions to obscure the true identity of the remitter;
- The customer favours cold storage of VFAs or makes use of dark wallets;
- The customer is actively avoiding direct contact with the VFA Operator without good reason and/or uses multiple intermediaries without any logical explanation;
• The customer is reluctant or refuses to provide information, data and documents usually required in order to enable the transaction’s execution;
• The customer provides false or counterfeited documentation;
• The customer is a business entity which cannot be found on the internet, especially if the customer is otherwise secretive or avoids direct contact;
• The customer is known to have criminal connections;
• The customer has made payments in VFAs to websites known to be associated with illegal activity;
• The customer is a politically exposed person (“PEP”) or is a family member or close associate of a PEP;
• The transaction being carried out by the customer involves the use of a disproportional amount of accumulated savings, bearer cheques or cash;
• The customer provides inconsistent explanations as to the source of funds that have been used to transact in, or purchase, VFAs;
• The source of wealth and funds associated with the transaction is inconsistent with the socio-economic profile of the individual or the company’s economic profile;
• The source of funds is unusual, for example: (a) funding from a third party who has no apparent connection with the customer or for which there is no legitimate explanation; (b) funds received from a foreign country when there is no apparent connection between the country and the customer; (c) wealth accumulated from and/or funds received from high-risk countries;
• The customer transfers funds or VFAs to a jurisdiction with which he has no apparent connection;
• There is an excessively high or low price attached to the VFA transferred when compared to normal or known market circumstances;
• The customer requests or carries out large financial transactions;
• The transactions involve recently-created companies;
• There is no justification for the transactions being proposed or being carried out (e.g.: they are not justified by the corporate purpose, the activity of the customer or the possible group of companies to which it belongs);
• The customer is using a state-sponsored VFA which is designed to evade international financial sanctions.

3. Reporting Requirements

Chapter 5 of the revised Implementing Procedures – Part I explains in detail the reporting requirements that subject persons have to adhere to and a number of other matters related or ancillary thereto. Summarised hereunder are some of the more important aspects related to reporting.

3.1 The Money Laundering Reporting Officer

Subject persons are required to appoint a Money Laundering Reporting Officer (“MLRO”) whose main responsibility is to consider any internal reports of unusual or suspicious transactions and, where necessary, follow up the same by filing a suspicious transaction report (“STR”) with the FIAU. The
MLRO is also considered by the FIAU as its main contact point within the subject person and he is to act as the main channel through which any communications with the FIAU are to be conducted. Given these especially onerous obligations, the MLRO should be an officer of the subject person who has a thorough understanding of AML/CFT regulation and enjoys sufficient seniority and command to be able to act independently of management.

As regards the location of the MLRO, he has to be present where the subject person is actually conducting its activities from, i.e. the jurisdiction from where the operations of the given VFA Operator are being conducted and where the MLRO can have access to all the necessary information/documentation to effectively carry out his obligations.

### 3.2 Reporting Suspicious Activity and Transactions

In terms of Regulation 15 of the PMLFTR and Chapter 5 of the revised Implementing Procedures – Part I, subject persons are required to have internal and external procedures providing for the reporting of suspected or known instances of ML/FT or of proceeds of crime as well as instances where there are reasonable grounds to suspect as much. The internal reporting procedures must allow for subject person’s employees to even report a suspected instance of ML/FT to the MLRO when their immediate superior is in disagreement with them. It will be then up to the MLRO to determine if the information available can be considered as sufficient for a STR to be made to the FIAU.

When the ML/FT suspicion is linked to a transaction still to be processed, it is important that the subject person refrains from carrying out the same, files a STR and delays the execution of the transaction for one (1) working day following the day on which it files the STR. During this time the FIAU has to determine and communicate to the VFA Operator whether it objects to the execution of the said transaction. Should there be an objection to the transaction’s execution, this objection only suspends the execution thereof for a maximum of another two (2) working days. On the other hand, if the transaction is not objected to, the VFA Operator is to determine whether on the basis of all the information in its possession it still wishes to carry out the transaction or otherwise.

Notwithstanding the above, the FIAU does recognise that, within the VFA sector, refraining from carrying out the transaction is not always possible, in which case VFA Issuers and Licence Holders may still proceed with the transaction’s execution but must then submit a STR to the FIAU immediately afterwards and by no later than twenty-four (24) hours from when the transaction was executed. The relative VFA Operator should also provide its reasons why it executed the transaction prior to filing a STR with the FIAU. However, as much as possible, this procedure should be made use of by way of exception and not adopted as a general rule.

To the extent possible, VFA Operators should however stall from allowing any further transactions relating to the customer or VFA in respect of which they have formed a suspicion of ML/FT, either by blocking the account of the customer or otherwise blocking the VFA itself.

Reporting obligations arise in the following circumstances:

---

5 Any reference to knowledge or suspicion of, or reasonable grounds to suspect, ML/FT throughout this document is to be construed as also including knowledge or suspicion that funds or property are derived from criminal activity.
i. Where the subject person suspects that transactions are linked to ML/FT;

ii. Where in the course of its business activities the subject person becomes aware that a person is linked to ML/FT or that ML/FT is being committed or may be committed independently of whether any transactions have taken place or otherwise; and

iii. Where the subject person has reasonable grounds to suspect that ML/FT may be taking place, this being a more objective ground for reporting. This implies that a further obligation to report arises where, on the basis of objective facts, the subject person ought to have suspected that ML/FT existed.

Examples of trigger events that may give rise to such reporting obligations include:

- The customer provides false identification information;
- There are indications that the customer is active on the darknet or makes use of tumblers;
- VFA Operator being unable to identify the beneficial owner of a corporate customer;
- Unusual rapid movement of assets and/or funds; and
- The detection of an unregistered, or operation of, an illegal exchange.

The above non-exhaustive list, as well as other indicators referred to throughout these Implementing Procedures, are red flags that may alert VFA Operators to ML/FT, but they are merely indicative and taken on their own need not necessarily mean that ML/FT is taking place. Red flags are not intended to automatically result in the filing of a STR with the FIAU but are merely indicators that should lead VFA Operators to question the customer’s behaviour – it is only if there is no reasonable explanation for the same that an internal report is to be made to the MLRO for him to determine whether there is a suspicious of ML/FT and, if necessary, file a STR with the FIAU.

The submission of a STR should lead a VFA Operator to question its relation with the customer and whether it wants to continue with the same. Any action undertaken by the VFA Operator has to be in line with what is provided in the PMLA, the PMLFTR and Chapter 5 of the revised Implementing Procedures – Part I. In particular, VFA Operators have to take note of the provisions relating to the execution of transactions which the specific operator either knows or suspects that they are linked to ML/FT and whether they are allowed to proceed with their execution or otherwise.

In situations where a VFA Operator is unable to obtain the necessary information and documentation to identify and verify the identity of its customer and/or to establish, where applicable, the purpose and intended nature of the business relationship, the Operator is to discontinue its interaction with the customer and has to consider whether, taking into account all relative circumstances, it should file a STR with the FIAU.

4. **Record-keeping**

Regulation 13 of the PMLFTR and Chapter 9 of the revised Part I of the Implementing Procedures require the subject person to keep, amongst others, records of customer due diligence ("CDD"), ongoing monitoring, internal and external reports, and such other records as are sufficient to permit the reconstruction of individual transactions and prove compliance with the PMLA, the PMLFTR, and any applicable Implementing Procedures issued by the FIAU, including the present ones.
The rationale for requiring transaction records is to (i) allow a subject person to prove compliance with its AML/CFT obligations, (ii) put the subject person in a better position to carry out a number of its AML/CFT obligations such as on-going monitoring, and (iii) provide a clear audit trail of a transaction which may be used in the event of a ML/FT investigation to determine the source and destination of criminal or terrorist property that the authorities may seek to freeze, restrain or confiscate.

5. Training

Regulation 5(5) of the PMLFTR and Chapter 7 of the revised Implementing Procedures – Part I require subject persons to provide AML/CFT training to all relevant members of staff and directors of the subject person.

In the case of VFA Operators, it is expected that the training program would also cover matters specific to the ML/FT risks associated with VFAs and the systems and controls adopted to mitigate against these risks. In addition, and given the rapidly-changing environment surrounding VFAs, such training programs should also cover regulatory, technological, and other relevant developments in the VFA space and any associated emerging ML/FT risks.
Part B: Virtual Financial Assets Agents

1. Risk Assessment

VFA Agents should approach services and customers connected to VFAs with a full understanding of their proposed business model and any potential ML/FT risks they may be exposed to. As with any new line of business, the main AML/CFT compliance question for VFA Agents will be whether they can sufficiently mitigate and reasonably manage those risks. VFA Agents have to perform business and customer risk assessments in line with Section 3 of the revised Implementing Procedures – Part I as well as with Part A of this document. This will allow them to devise and implement their AML/CFT measures, policies, controls and procedures in a manner which ensures that AML/CFT obligations can still be fulfilled in the VFA context.

When carrying out the business risk assessment, VFA Agents are, amongst other aspects, to consider the specific risks presented by the VFA Issuers and Licence Holders that they service or intend to service, the jurisdictional risks attached to the same, the manner in which the they (intend to) conduct their business (e.g. whether they meet their customers face-to-face or otherwise whether, in the main, they interact with customers remotely), and the ML/FT risks attached to the service that they are providing. Where any of these factors vary over time, the VFA Agent has to consider whether its business risk assessment needs to be updated and whether the measures undertaken to address the risks it is exposed to need to be varied to better mitigate any change in risk.

As part of their risk assessment obligations, and in the context of undertaking their business risk assessment and updating the same, VFA Agents must also be able to monitor and identify changes in their external ML/TF risk environment, so that they can respond by adjusting the administration of their services, customers, relationships and delivery methods in order to mitigate new and emerging ML/TF risks. The same applies when there are internal changes within the VFA Agent, its structures and operations.

On the basis of their business risk assessment, VFA Agents are expected to establish appropriate risk-based systems and controls which include, at least, the following elements:

- Risk-based processes for recognising ML/FT typologies indicating suspicious behaviour;
- Processes to establish customer profiles and undertake a customer risk assessment;
- Processes to compare established customer profiles against risk-based typologies; and
- Processes to assign alerts to customers identified as high risk or those who engage in suspicious behaviour.

When looking at customer risk, VFA Agents may wish to consider the following non-exhaustive list of ML/FT risk indicators, which may become apparent either through its interaction with the same or through consideration of the customer’s whitepaper and/or business model:

- Customer provides insufficient, incomplete or suspicious information or information that cannot be verified;
- Customer has no safeguards against the use of proxies, unverifiable IP address or geographical location, disposable email address or mobile number, and/or to detect ever changing devices used to conduct transactions;
• The VFA Issuer or Licence Holder does not have in place mechanisms to be able to determine the jurisdictions from which its services are accessed and control access thereto;
• There is a willingness to accept or transact in higher risk digital currencies which reduce traceability and allow for anonymity, thus encouraging their use for illicit activity (e.g.: Monero, Dash, Zcash etc.);
• To the extent visible to the VFA Agent, the underlying customers of the prospective VFA Issuer or Licence Holder have a high ML/FT risk profile;
• The initial VFA offering (“IVFAO”) is structured in a way that the sale is not capped per user, thus allowing for unlimited amounts of funds to be transferred to the prospective VFA Issuer;
• Where the AML/CFT program of the prospective VFA Issuer or Licence Holder is not sufficiently robust (for example: (a) the VFA Issuer’s or Licence Holder’s business and compliance model does not permit it to collect information sufficient to perform CDD procedures and to risk rate its own customers or otherwise obtain information on the counterparties and location of the transactions; (b) the VFA Issuer or Licence Holder does not have mechanisms in place for account monitoring and reporting of suspicious transactions), such VFA Issuer or Licence Holder is not willing to address such deficiencies; and
• The VFA Agent considers that the VFA Issuer is not applying its AML/CFT policies and procedures correctly in line with the PMLFTR and Implementing Procedures as applicable to the VFA Issuer.

More specifically when dealing with VFA Issuers, VFA Agents should consider that there have been a number of initial coin offerings that were identified as fraud schemes, and are therefore expected to exercise extra caution.

At the outset of the business relationships with VFA Issuers, VFA Agents are encouraged to take into consideration the following and factor the same into their customer risk assessment:

• The lack of transparency that may surround the IVFAO, including the rights of holders and how financing will be used;
• The possibility of having IVFAO teams and promoters suddenly withdrawing from the project after the IVFAO sale has been concluded; and
• The project being at a conceptual phase with limited documentation being available and the likelihood of the prospective VFA Issuer providing insufficient or misleading information.

When the VFA Agent identifies any changes in the ML/TF risk environment and/or the VFA Issuer’s profile, the VFA Agent must review and, if necessary, update the business and customer risk assessment respectively, maintaining a record of the changes in risk that are identified, and updating systems and controls to manage the changed risks. One instance in which the customer risk assessment may need to be reconsidered is where the VFA Issuer undertakes additional IVFAOs, especially if these offerings present features which are different from the original one.

Additionally, procedures should be in place to identify suspicious activity and report it to the FIAU in accordance with Regulation 15(3) of the PMLFTR, Chapter 5 of the revised Implementing Procedures – Part I and Section 3.2 of Part A of these sector-specific Implementing Procedures.
2. Customer Due Diligence

The general requirements on CDD are covered in Chapter 4 of the revised Implementing Procedures – Part I, and this section aims to provide more guidance to VFA Agents as to how they are to fulfil their CDD obligations as subject persons under the PMLFTR when offering their services in terms of Articles 7 and 14 of the VFAA.

The nature of the CDD obligations that VFA Agents will have to fulfil will be dependent, amongst others, on the nature of the interaction between the VFA Agent and the (prospective) VFA Issuer and/or Licence Holder. In effect, a VFA Agent appointed by a VFA Issuer in terms of Article 7 of the VFAA will have ongoing obligations in relation to its relationship with the same. More specifically, in terms of the relative Rulebook issued by the Malta Financial Services Authority ("MFSA"), the VFA Agent is required inter alia to submit annually to the said authority a Compliance Certificate, copy of the audit report required in terms of Section 3 of Part C of this document, and ensure that the milestones included in the VFA Issuer’s whitepaper are met.

The interaction between the VFA Agent and the VFA Issuer is thus likely to prolong itself over time, thereby presenting an element of duration. Consequently, the relationship between the two is considered to constitute a ‘business relationship’ in terms of the PMLFTR. In such cases, and subject to what is stated hereunder, CDD measures would not be limited to the identification and verification of the VFA Issuer but would also extend to, inter alia, obtaining information on the purpose and intended nature of the business relationship, ongoing monitoring of the business relationship etc.

On the other hand, where a VFA Agent is appointed by a prospective VFA Licence Holder in terms of Article 14 of the VFAA, this interaction is not expected to have an element of duration, but, rather will be limited to the VFA Agent assisting the prospective VFA Licence Holder with applying for a licence from the MFSA in terms of Article 15 of the VFAA. Any such transaction is therefore not deemed to present the elements necessary to constitute a ‘business relationship’ between the two parties and is to be treated as an ‘occasional transaction’. Thus, subject to what is stated hereunder, CDD measures would be limited to the identification and verification of the prospective VFA Licence Holder. It is important to note that in this case no thresholds will be applicable and AML/CFT obligations, including the carrying out of a customer risk assessment and meeting CDD requirements, would be applicable at all times.

The risk-based approach allows a VFA Agent to vary the extent of the CDD measures applied based on the risk presented by the particular VFA Issuer or Licence Holder. However, as regards the timing of these measures, it is important that the VFA Agent carries out the same prior to the submission of the whitepaper or of the licence application, as may be applicable, to the MFSA.

2.1 On-boarding Procedures

Regulation 7(1) of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I require subject persons to identify the customer and verify the identity of the customer using reliable and independent sources, with verification being possible on the basis of either documentary sources or through electronic means.

---

6 In this regard, it is to be noted that a series of amendments are to be carried out to the PMLFTR and include a widening of the definition of ‘occasional transaction’ to reflect the position described in this document.
For this purpose, VFA Agents should ensure that their customer on-boarding procedures distinguish between customers that are natural persons and those that are either legal persons or legal arrangements. The said procedures should include asking the natural person who seeks to form the business relationship or carry out an occasional transaction to confirm whether he is acting in a personal capacity or on behalf of a legal person or arrangement.

In addition, Regulation 7(3) of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I require VFA Agents to determine whether the person requesting the service is acting on behalf of another person and, if so, identify both persons, and take reasonable measures to verify their identity using relevant information obtained from a reliable independent source. In order to determine whether the person requesting the service is acting for another person, the VFA Agent should consider a number of factors including from where customer instructions are being received; the source of funds; the destination of funds; payment references or rationale that do not appear to relate to the purported customer; and any unusual delay in answering questions due to the purported customer having to refer to a third party.

The ability to establish the identity, jurisdiction, and purpose of each customer and business relationship or occasional transaction is essential to ensure compliance with VFA Agents’ obligations under the PMLA, the PMLFTR and any Implementing Procedures issued by the FIAU. In spite of the challenges that prospective VFA Issuers and Licence Holders pose, a VFA Agent must ensure that its policies and procedures allow it to perform these functions with the same degree of confidence in the VFA context as they do in the case of more traditional services. While the precise measures necessary will depend on the particular customer and service, there are a number of considerations that apply across the board:

- A VFA Agent cannot enter into a business relationship or undertake an occasional transaction unless it has verified the true identity of the customer and its beneficial owners where applicable;
- A VFA Agent is obliged to develop a reasonable understanding of the purpose and intended nature of the business relationship;
- Given the special considerations that apply to VFAs, VFA Agents may likely find it appropriate to develop specific red flags that apply to business models of VFA Issuers and Licence Holders so as to allow the VFA Agent to spot any key ML/FT risk indicators in the whitepaper and/or the prospective VFA Licence Holder’s proposed business model, and must train their employees accordingly;
- The AML/CFT policies and procedures in place should give the VFA Agent assurance that the information that it obtains and retains for the purpose of CDD is accurate and is sufficient to withstand independent challenge.

2.2 Beneficial Ownership and Control of a Legal Person/Legal Arrangement

VFA Agents are reminded that Regulation 7(1) of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I require that the subject person carry out CDD procedures not only in respect of the customer as already described above but also in relation to a customer’s beneficial(s) owner(s), that is the individual(s) who ultimately own/s and control/s the customer. Depending on the nature of the customer, identification and verification measures may have to be applied in relation to
a number of various parties who may own, control or direct the activities of a legal person or arrangement.

2.3 Obtaining Information on the Purpose and Intended Nature of the Business Relationship

As part of their CDD measures, subject persons are required to obtain an understanding as to why a prospective customer is seeking to establish a business relationship with them. This consists of determining the purpose and intended nature of the same. Within the context of business relationships between VFA Agents and VFA Issuers under the VFAA, the purpose thereof is quite self-evident (i.e. registering a whitepaper with the MFSA so as to be able to conduct an IVFAO to finance the project described in the whitepaper), and, limitedly to this aspect, it is not required that VFA Agents obtain any additional information from VFA Issuers.

However, this does not exonerate the VFA Agent from the development of a customer business and risk profile with respect to VFA Issuers, the key element being to have sufficient information available so as to allow a proper appreciation of the risks involved and the detection of unusual activity.

To this end, VFA Agents have to collect sufficient information and, where necessary, documentation to establish a prospective VFA Issuer’s source of wealth as well as the source of the funds to be used for his expected outlays. Source of wealth consists in determining the economic activity or activities which generate the customer’s wealth. This may be comprised of, for instance, income through employment or business, or an inheritance. The source of wealth information will allow the VFA Agent to establish whether, taking into consideration the costs and expenses associated with the launch and running of an IVFAO, the Issuer’s intention to conduct a VFA issue makes sense or otherwise. On the other hand, the source of funds refers to the activity, event, business, occupation or employment generating the funds used in a particular transaction, or to be used in future transactions.

As to the extent of the information that VFA Agents are to collect, it is essential that this reflects the level of ML/FT risk identified through the customer risk assessment referred to in Section 2.2 of Part A of these Implementing Procedures. Where the risk is medium or lower, a declaration from the customer with some details (e.g. nature of employment/business, usual annual salary etc.) can suffice. Where the risk of ML/FT is higher, or VFA Agents have doubts as to the veracity of the information collected, the information obtained would need to be supplemented by means of independent and reliable information and documentation.

2.4 Determining Source of Wealth and Source of Funds

The determination of source of wealth and source of funds forms part of the VFA Agents’ CDD obligations. Although not the norm in the context of an occasional transaction, the determination of source of wealth and source of funds may still be required when the VFA Agent is providing its services to a VFA Licence Holder. In any such circumstances, where the ML/FT risk is assessed by the VFA Agent to be high and therefore requiring the application of enhanced due diligence (“EDD”) measures, it is very likely that the most effective measure that can be taken is to query how the funds to be used have been acquired and whether this makes sense considering the customer’s source of wealth. In any such circumstances, VFA Agents are therefore expected to establish the source of wealth and source of funds of a VFA Licence Holder, unless they are able to apply alternative measures that can be shown to be equally effective to address the risks identified.
On the other hand, due to the nature of their relationship with VFA Issuers, VFA Agents are required to establish source of wealth and source of funds independently of the risk associated with servicing any such customer.

When it comes to the determination of the source of wealth and source of funds, the VFA Agent is required to collect sufficient information and documentation so as to ensure that it has a reasonable understanding of how the customer derived the same. Information gathered may vary from declaration obtained directly from the customer to the collection of documentation to verify the same or information derived from reliable and independent third parties and consider raising an STR in accordance with Section 3.2 of Part A of these sector-specific Implementing Procedures if its requests for additional information and/or documentation go unanswered.

In determining the source of funds, VFA Agents should place particular emphasis on the source of the initial and future capital being injected by the VFA Issuer or VFA Licence Holder for the purpose of carrying out its business activities. The method used to effect these transactions should also be taken into account as this will inevitably impact the nature and degree of information to be collected on source of funds. Where payment is being made in fiat currency and it originates from an account in the name of the VFA Issuer or Licence Holder held with a bank or payment institution established in the EEA or other reputable jurisdiction, or otherwise through a credit or debit card issued by a bank or payment institution established in the EEA or other reputable jurisdiction, the degree of information required for source of funds purposes need not be as extensive as in situations where anonymous payment methods are used.

In the case of payments effected by means of VFAs, the source of funds will consists in determining how these were obtained by the VFA Issuer or VFA Licence Holder. In the event that the VFA Agent determines (and documents) that the VFAs have been created by the prospective VFA Issuer or VFA Licence Holder (e.g.: through mining), the need to obtain additional information from the VFA Issuer or Licence Holder will be dependent on the amount or value involved. Where this is significant, the VFA Agent will be expected to substantiate its determination with documentation on the mining operation that led to the creation of the VFAs (e.g. through the collection of electricity bills, hardware receipts etc.) and consider whether the information obtained makes sense within the context of the source of wealth information obtained by the VFA Agent. On the other hand, if the VFAs have originated from alternative sources, the VFA Agent must request evidence of previous transactions effected by the VFA Issuer or Licence Holder to determine the activity that led to the VFA Issuer or Licence Holder being in possession of these VFAs.

2.5 Politically Exposed Persons

Regulation 11(5) of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I requires the subject person to maintain appropriate procedures for the purpose of determining whether a customer and, where applicable, its beneficial owners are PEPS. Where any PEPS are identified, there is a series of EDD measures that have to be taken by the subject person, irrespective of whether they are foreign or domestic PEPS. It is important to point out that these measures are also applicable where the customer or the beneficial owner is a family member or a known close associate of a PEP.
Compliance with these requirements may be impacted where the VFA Agent has not identified their customer as a legal person/arrangement and therefore has not identified the beneficial owner(s), resulting in the VFA Agent being unable to determine whether they are PEPs or otherwise.

3. Ongoing Monitoring

In the context of its business relationship with a VFA Issuer, a VFA Agent is required to monitor the same on an ongoing basis. For avoidance of doubt, the FIAU is aware that a VFA Agent is not, by the very nature of its relationship with the VFA Issuer, privy to the underlying transactions taking place between the VFA Issuer and its customers. As such, VFA Agents are only required to carry out ongoing monitoring activities limited to ensuring that information, data and documentation pertaining to VFA Issuers and, where relevant, their beneficial owner(s) is kept accurate and up-to-date.

VFA Agents should also ensure that the VFA Issuer’s activities are consistent with the VFA Agent’s knowledge of the VFA Issuer, its business and risk profile. Changes to the VFA Issuer’s business/activities or changes that may be independent of the VFA Issuer but still effect the risk presented by the VFA Issuer should lead the VFA Agent to review its customer risk assessment and, if necessary, update the same and modify the CDD measures applied if required to mitigate the new source or level of risk identified.

4. Reliance and Outsourcing

4.1 Reliance

Regulation 12 of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I allow for the exercise of reliance, with the subject person relying on the information and documentation collected at customer on-boarding stage by any other person or entity in an EU Member State or a reputable jurisdiction subject to AML/CFT requirements equivalent to those arising from the PMLFTR and a level of supervision equal to that required in terms of Directive 2015/849/EU. In determining as much, VFA Agents can refer to FATF/Moneyval mutual evaluation reports, IMF Country Reports etc.

When exercising reliance, a VFA Agent has to obtain the identification information from the third party it is relying upon but does not need to obtain any verification documents. However, the VFA Agent must have an agreement with the third party being relied upon for any such documents to be made available upon request and this arrangement must be tested from time to time to ensure that it actually functions as set out in the agreement. Moreover, the VFA Agent remains responsible for the carrying out of customer risk assessment, determining whether the customer is a PEP and conducting on-going monitoring. VFA Agents will be able to exercise reliance to meet their CDD obligations as long as the conditions described above are met.

4.2 Outsourcing

Where a VFA Agent considers outsourcing the implementation of its AML/CFT obligations, it is important that the VFA Agents bears in mind that it will remain responsible at all times for compliance with the said obligations. More importantly, VFA Agents are to comply with the outsourcing conditions and limitations set forth under Chapter 6 of the revised Implementing Procedures – Part I.
VFA Agents are to remember that, whether they exercise reliance or enter into an outsourcing arrangement, they remain responsible for ensuring compliance with their AML/CFT obligations at all times.
Part C: Virtual Financial Assets Issuers

1. Risk assessment

VFA Issuers are to carry out business and customer risk assessments in line with the requirements of Section 3 of the revised Implementing Procedures – Part I and of Part A of these sector-specific Implementing Procedures.

When carrying out the business risk assessment, VFA Issuers are, amongst other aspects, to consider how they intend to structure their IVFAO and how this may be abused for ML/FT purposes. Thus, for example, particular attention should be paid to characteristics which may result in the IVFAO being particularly vulnerable to ML/FT such as the absence of any capping per subscriber, allowing an unlimited amounts of funds to be transferred to the VFA Issuer. The subscriber is the person acquiring VFAs through the IVFAO and is therefore considered as the VFA Issuer’s customer.

The business risk assessment should be reviewed and, if necessary, updated whenever new factors materialise themselves which may increase the ML/FT risks to which the VFA Issuer is exposed. One such instance is where the VFA Issuer conducts a subsequent IVFAO, especially if it presents characteristics and features different from the previous one and/or it targets different markets. If it results that the risks have increased, or are originating from different sources then those previously identified, the VFA Issuer would have to consider whether the mitigating measures taken originally are still adequate. Should this not be the case, then additional measures would have to be implemented.

In addition, VFA Issuers may wish to consider the following list of ML/FT risk indicators, which is not meant to be exhaustive, both when carrying out their business as well as their customer risk assessment:

- customer provides insufficient, incomplete or suspicious information or information that cannot be verified;
- use of proxies, unverifiable IP address or geographical location, disposable email address or mobile number, ever changing devices used to conduct transactions;
- unusual patterns of transaction activity (e.g. volumes, velocity, structuring to avoid detection/reporting obligations, source, destination);
- the potential for cybercriminals to launch ransom-ware attacks in light of the combination of decentralisation and anonymity; and
- accepting higher risk digital currencies which reduce traceability and allow for anonymity, thus increasing the chance that they were used for illicit activity (e.g.: Monero, Dash, Zcash etc.).

As potential mitigating measures against these elevated threats, VFA Issuers should establish and implement robust CDD procedures (and collect IP addresses and other device identifiers when appropriate) as described in Section 2 below. Additionally, procedures should be in place to identify suspicious transactions and report these to the FIAU in accordance with Regulation 15(3) of the

---

7 The same would be true where the limits imposed are either too high or the VFA Issuer does not have proper systems in place to detect linked transactions, i.e. transactions carried out by the same customer, as well as to detect the moment in time when any thresholds imposed are met.
PMLFTR, Chapter 5 of the revised Implementing Procedures – Part I and Section 3.2 of Part A of these Implementing Procedures.

2. Customer Due Diligence

The general requirements of CDD are covered in Chapter 4 of the revised Implementing Procedures – Part I. This Part C aims to provide more guidance to VFA Issuers as to how to fulfil their CDD obligations as subject persons under the PMLFTR.

The nature of the CDD obligations that VFA Issuers will have to carry out will be dependent, amongst others, on the nature of the interaction between the VFA Issuer and its customers, especially the temporal duration of the same. In effect, since the transactions between VFA Issuers and their customers are not expected to have an element of duration (as they are limited to the acquisition of VFAs in the course of an IVFAO) any such transaction is not deemed to present the elements necessary to constitute a ‘business relationship’ between the two parties and is to be treated as an ‘occasional transaction’. It is important to note that in this case no thresholds will be applicable and AML/CFT obligations would be applicable at all times\(^8\).

In accordance with Regulation 8 of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I, VFA Issuers are allowed to determine, on a risk-sensitive basis, the extent and timing of CDD measures to be applied in relation to the customer. This is dependent on the outcome of the customer risk assessment referred to in Section 2.2 of Part A of these Implementing Procedures. VFA Issuers are reminded that they should be able to demonstrate to the FIAU that the extent and timing of CDD measures applied by them on the customer is appropriate in view of the risks of ML/FT posed by the occasional transaction.

2.1 On-Boarding Procedures

Regulation 7(1) of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I require subject persons to identify the customer and verify the identity of the customer using reliable and independent source documents, with such verification measures being undertaken on the basis of either documentary sources or through electronic means.

For this purpose, VFA Issuers should ensure that their customer on-boarding procedures distinguish between customers that are natural persons and customer who are legal persons or arrangements. This should include asking the natural person who seeks to form the business relationship or carry out an occasional transaction to confirm whether they are acting in their own personal capacity or on behalf of a legal person or arrangement.

In addition, Regulation 7(3) of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I require VFA Issuers to determine whether the person requesting the service is acting on behalf of another person and, if so, identify both persons, and take reasonable measures to verify their identity using relevant information obtained from a reliable independent source. In order to determine whether the person requesting the service is acting for another person, the VFA Agent should consider a number of factors such as from where customer instructions are being received; the

\(^8\) In this regard, it is to be noted that a series of amendments are to be carried out to the PMLFTR and include a widening of the definition of ‘occasional transaction’ to reflect the position described in this document.
source of funds; the destination of funds; payment references or rationale that do not appear to relate to the purported customer; and any unusual delay in answering questions due to the purported customer having to refer to a third party.

While the precise CDD measures to be applied will necessarily depend on the particular circumstances of the individual case, some broad considerations apply:

- A VFA Issuer cannot undertake an occasional transaction unless it has identified and verified the true identity of the customer and its beneficial owners where applicable; and
- The AML/CFT policies and procedures in place should give the VFA Issuer assurance that the information that it obtains and retains for the purpose of CDD is accurate and is sufficient to withstand independent challenge.

In addition to the identity details to be collected for identity purposes in terms of Chapter 4 of the revised Implementing Procedures, VFA Issuers are also to obtain the address of the wallet/account number to be used by the customer to either receive the VFA being acquired or to transfer VFAs to the VFA Issuer as payment for the VFAs being acquired through the IVFAO.

Verification of identity would therefore also require the verification of the wallet address/account number, i.e. before accepting any VFAs originating from the wallet address indicated by the customer, the VFA Issuer is to verify that the said wallet actually belongs to its customer. The same is true with respect to the wallet address to which any VFAs are to be transferred by the VFA Issuer, with the VFA Issuer having to verify the wallet address/account number prior to transferring any VFAs thereto.

2.2 Beneficial Ownership and Control of a Legal Person/Legal Arrangement

VFA Issuers are reminded that Regulation 7(1) of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I require that the subject person carry out CDD procedures not only in respect of the customer and its agent(s) as already described above but also in relation to a customer’s beneficial(s) owner(s), that is the individual(s) who ultimately owns and controls the customer. Depending on the nature of the customer, identification and verification measures may have to be applied in relation to a number of various parties who may own, control or direct the activities of a legal person or arrangement.

2.3 Politically Exposed Persons

Regulation 11(5) of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I requires the subject person to maintain appropriate procedures for the purpose of determining whether a customer and, where applicable, its beneficial owners are PEPs. Where any PEPs are identified, there a series of additional CDD measures that have to be taken by the subject person, irrespective of whether they are foreign or domestic PEPs. It is important to point out that these measures are also applicable where the customer or the beneficial owner is a family member or a known close associate of a PEP.

Compliance with these requirements may be impacted where the VFA Issuer has not identified its customer as a legal person/arrangement and therefore has not identified the beneficial owner(s), resulting in the VFA Issuer being unable to determine whether they are PEPs or otherwise.
2.4 Inability to Complete CDD Measures

Where it proves impossible to complete the CDD measures, the VFA Issuer:

i. is not to allow any activity of any kind by the VFA holder or provide any other service to the VFA holder and, to this end, a VFA Issuer is not to on-board the customer. If it has already done so, the VFA Issuer is to either close the VFA holder’s profile or to keep it deactivated in its entirety; and

ii. determine whether it is necessary to lodge a STR with the FIAU.

Where in these circumstances the VFA Issuer is in possession of funds or assets belonging to the VFA holder which may have been received in advance for the acquisition of VFAs, and there no grounds to suspect ML/FT or the transaction has not been suspended by the FIAU or by operation of the law, nor is there an attachment or freezing order, the VFA Issuer is to remit the funds or assets to the same source and through the same channels used to receive them, and this after having considered whether there is any other legal impediment to their remittance9. To the extent possible, the VFA Issuer should indicate in any transaction script that the funds or assets are being returned due to the inability to complete CDD.

2.5 Determining the Source of Wealth and the Source of Funds

Source of wealth consists in the economic activity or activities which generate the customer’s wealth. This may be comprised of, for instance, income through employment or business, or inheritance. The term ‘source of funds’ refers to the activity, event, business, occupation or employment generating the funds used in a particular transaction, or to be used in future transactions.

The determination of source of wealth and source of funds is not the norm in the context of an occasional transaction. However, their determination may still be required in the context of an occasional transaction, such as in the context of a sale of VFAs by VFA Issuers in an IVFAO. Where the ML/FT risk within an occasional transaction is assessed by the VFA Issuer to be high and therefore requiring the taking of EDD measures, it is very likely that the most effective measure that can be taken is to query how the funds being used have been acquired and whether this makes sense considering the customer’s source of wealth. In any such circumstances, subject persons would therefore still be expected to establish their customer’s source of wealth and source of funds, unless they are able to apply alternative measures that can be shown to be equally effective to address the risks identified.

When it comes to the determination of the source of wealth and source of funds, the VFA Issuer is required to collect sufficient information and documentation so as to ensure that it has a reasonable understanding of (a) how the customer generated his wealth and (b) how he derived the funds being used to carry out the particular transaction. The VFA Issuer is to then determine whether the transaction makes sense within the context of the information collected. Information gathered may

---

9 In the event the VFA Issuer is unable to remit the funds or assets to the same source through the same channels, it will inevitably have to request fresh instructions from the customer. In the event that these instructions give rise to a suspicion on the part of the VFA Issuer, it should submit a STR and suspend the remittance pending the FIAU expressing its opposition or otherwise to the said transaction.
vary from sufficiently detailed declaration obtained directly from the customer to the collection of
documentation to verify the same or information derived from reliable and independent third parties.
In determining the source of funds, i.e. how the funds to be used for a given transaction were
generated, VFA Issuers should consider the method used to effect payment as this will inevitably
impact the nature and degree of information to be collected on source of funds.

Where payment is being made in fiat currency and it originates from an account in the name of the
customer held with a bank or payment institution established in the EEA or other reputable
jurisdiction, or otherwise through a credit or debit card issued by a bank or payment institution
established in the EEA or other reputable jurisdiction, the degree of information required for source
of funds purposes need not be as extensive as in situations where anonymous payment methods are
used.

In the case of payments effected by means of VFAs, the source of funds will consists in determining
how these were obtained by the customer. In the event that the VFA Issuer determines (and
adequately documents) that the VFAs have been created by the customer (e.g. through actively mining
the same), the need to obtain additional information from the customer will be dependent on the
amount or value involved. Where this is significant, the VFA Issuer will be expected to substantiate its
determination with documentation on the mining operation that led to the creation of the VFAs (e.g.
through the collection of electricity bills, hardware receipts etc.) and consider whether the
information obtained makes sense within the context of the source of wealth information obtained
by the VFA Issuer. On the other hand, if the VFAs have originated from alternative sources, the VFA
Issuer must request evidence of previous transactions effected by the VFA holder to determine the
activity that led to the customer being in possession of these VFAs.

Independently of whether an occasional transaction requires the determination of the source of
wealth or the source of funds, a VFA Issuer who accepts VFAs as payment is required to have systems
in place to:

- check the wallet address/account for negative information in the public domain; and
- use distributed ledger analytical tools, *inter alia*, detect potentially fraudulent transactions
  and other suspicious activity (e.g.: the VFAs were used on the darkweb or in connection with
  a ransomware attack).

Any negative information should be factored into the customer risk assessment and should be
considered by the VFA Issuer to determine whether it is willing to proceed with the transaction or
whether it should desist from doing so and file a STR with the FIAU. In determining the way forward,
the VFA Issuer should consider how remote is the connection both from the temporal aspect as well
as from the transactional aspect.

It is important to note that the use of these systems is not dependent on risk and they must therefore
be used whenever one accepts VFAs as payment.

3. **AML/CFT Audit**

In terms of Regulation 5(5)(d) of the PMLFTR, subject persons are to implement, where appropriate
with regard to the nature and size of its business, an independent audit function to test its internal
measures, policies, controls and procedures. Given the nature of the business undertaken by VFA Issuers, the FIAU considers that an audit of a VFA Issuer’s measures, policies, controls and procedures should be carried out at least annually once the IVFAO has commenced until it is exhausted. This audit should be carried out by a party which is external to the VFA Issuer (as well as to the group which the VFA Issuer may form part of) to ensure independence.

This audit is being required in an effort to ensure the effectiveness of the said measures, policies, controls and procedures. Such an AML/CFT audit, must also be carried out upon any material changes/enhancement to the AML/CFT programme or at such more frequent intervals as may be directed by the FIAU.

The purpose of an AML/CFT audit is to serve as a systematic check of the VFA Issuer’s AML/CFT systems and controls and the end result should be a written report on whether:

- the VFA Issuer’s AML/CFT programme is fit for purpose and compliant with the obligations of the VFA Issuer under the applicable AML/CFT framework;
- the AML/CFT systems and controls were adequate and effective throughout the audit period; and
- any changes are required.

For the purposes of the report, the AML/CFT audit must:

- attest to the overall integrity and effectiveness of the AML/CFT systems and controls;
- test the VFA Issuer’s risks and exposures with respect to size, business lines, customer base and geographic locations;
- assess the adequacy of internal policies and procedures;
- test compliance with the relevant laws and regulations;
- test transactions in all areas with emphasis on high-risk areas, products and services;
- test the accuracy and quality of data;
- test the verification methods adopted by the VFA Issuer;
- test the audit trail and record-keeping capabilities;
- test employees’ knowledge of the laws, regulations, guidance, and policies and procedures;
- test the adequacy, accuracy and completeness of training programmes; and
- test the adequacy of the process of identifying suspicious activity.

The AML/CFT auditor engaged by the VFA Issuer should be proficient in the PMLFTR, the Implementing Procedures and these sector-specific Implementing Procedures, and should also possess technological expertise specific to the system used by the VFA Issuer in the performance of its AML/CFT obligations. Where the AML/CFT auditor and the Systems Auditor appointed by the VFA Issuer in terms of the MFSA’s VFA Rules for VFA Issuers are separate, and since it is likely that most VFA Issuers will rely on technology to perform their AML/CFT obligations, it is advisable that the AML/CFT auditor liaises with the Systems Auditor so as to obtain an in-depth understanding of the functionalities and capabilities of the system and therefore be in a better position to test their effectiveness.

The audit report should be addressed to the VFA Issuer’s senior management so they can decide what (if any) next steps are required as well as being made available to its VFA Agent for the purpose of complying with any regulatory requirements applicable thereto. A copy of the audit report, together
with management’s responses, shall be made available to the FIAU and relevant supervisory authorities upon request.

4. **Reliance and Outsourcing**

4.1 **Reliance**

Regulation 12 of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I allow for the exercise of reliance, with the subject person relying on the information and documentation collected at customer on-boarding stage by any other person or entity in an EU Member State or a reputable jurisdiction who is subject to AML/CFT requirements and supervision equivalent to those required in terms of Directive 2015/849/EU. In determining as much, VFA Issuers can refer to FATF/Moneyval evaluation reports, IMF Country Reports etc.

When exercising reliance, a VFA Issuer has to obtain the identification information from the third party it is relying upon but does not need to obtain any verification documents. However, the VFA Issuer must have an agreement with the third party being relied upon for any such documents to be made available upon request and this arrangement must be tested from time to time to ensure that it actually functions as set out in the agreement. Moreover, the VFA Issuer remains responsible for the carrying out of a customer-specific risk assessment and determining whether the customer is a PEP. VFA Issuers will be able to exercise reliance to meet their CDD obligations as long as the conditions described above are met.

In the context of reliance, it is possible for VFA Issuers to place reliance on VFA exchanges licensed under the VFAA. In fact, VFA exchanges licensed under the VFAA could act as a first filter of due diligence for a number of VFA Issuers which would be able to rely on the CDD measures undertaken by these exchanges. This could allow for a more streamlined and efficient CDD process.

4.2 **Outsourcing**

Where a VFA Issuer considers outsourcing the implementation of its AML/CFT obligations, it is important that the VFA Issuer bears in mind that it will remain responsible at all times for compliance with the said obligations. More importantly, VFA Issuers are to comply with the outsourcing conditions and limitations set forth under Chapter 6 of the Revised Implementing Procedures – Part I.

**VFA Agents are to remember that, whether they exercise reliance or enter into an outsourcing arrangement, they remain responsible for ensuring compliance with their AML/CFT obligations at all times.**
Part D: Virtual Financial Assets Licence Holders

1. Risk Assessment

VFA Licence Holders are to carry out a business and customer risk assessment in line with the requirements of Chapter 3 of the revised Implementing Procedures – Part I and of Part A of these sector-specific Implementing Procedures.

In relation to the carrying out, review and updating of the business risk assessment, VFA Licence Holders must be able to monitor and identify changes to their external ML/TF risk environment, so they can respond by adjusting the administration of their services, customers, relationships and delivery methods in order to mitigate new and emerging ML/TF risks. If and when any such changes are identified, VFA Licence Holders must update their business risk assessment accordingly, maintaining a record of the changes in risk that are identified, and updating systems and controls to manage the changed risks. The same applies where the increase in risk is occasioned by changes within the VFA Licence Holder and its structures.

When carrying out their business and customer risk assessments, VFA Licence Holders may wish to consider, to the extent applicable, the following suggested list of ML/FT risk indicators, which is not meant to be exhaustive:

- customer provides insufficient, incomplete or suspicious information or information that cannot be verified;
- use of proxies, unverifiable IP address or geographical location, disposable email address or mobile number, ever changing devices used to conduct transactions;
- unusual patterns of transaction activity (e.g. volumes, velocity, structuring to avoid detection/reporting obligations, source, destination);
- the potential for cybercriminals to launch ransom-ware attacks in light of the combination of decentralisation and anonymity; and
- transactions in higher risk digital currencies which reduce traceability and allow for anonymity, thus encouraging their use for illicit activity (e.g.: Monero, Dash, Zcash etc.).

As potential mitigating measures against these elevated threats, VFA Licence Holders should establish robust CDD procedures (and collect IP addresses and other device identifiers when appropriate) as well as continuing applying the ongoing monitoring measures that shall be referred to in Section 3 below. Additionally, procedures should be in place to identify suspicious transactions and report these to the FIAU in accordance with Regulation 15(3) of the PMLFTR, Chapter 5 of the revised Implementing Procedures – Part I Section 3.2 of Part A of this Guidance.

2. Customer Due Diligence

The general requirements of CDD are covered in Chapter 4 of the revised Implementing Procedures – Part I. This section aims to provide more guidance to VFA Licence Holders as to how to fulfil their CDD obligations as subject persons under the PMLFTR.

In accordance with Regulation 8 of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I, VFA Licence Holders are allowed to determine, on a risk-sensitive basis, the extent and timing of CDD measures to be applied in relation to the customer, depending on the outcome of the customer

Page 27 of 40
risk assessment referred to in Section 2.2 of Part A of this Guidance. VFA Licence Holders are reminded that they should be able to demonstrate to the FIAU that the extent and timing of CDD measures applied by them on the customer is appropriate in view of the risks of ML/FT posed by the occasional transaction.

2.1 On-boarding Procedures

Regulation 7(1) of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I require subject persons to identify the customer and verify the identity of the customer using reliable independent source documents, such verification measures being undertaken on the basis of documentary sources or through electronic means.

For this purpose, VFA Licence Holders should ensure that their customer on-boarding procedures distinguish between customers that are natural persons or legal persons or arrangements. This should include asking the natural person who seeks to form the business relationship or carry out an occasional transaction to confirm whether they are acting in their own personal capacity or on behalf of a legal person or arrangement.

In addition, Regulation 7(3) of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I require VFA Licence Holders to determine whether the person requesting the service is acting on behalf of another person and, if so, identify both persons, and take reasonable measures to verify their identity using relevant information obtained from a reliable independent source. In order to determine whether the person requesting the service is acting for another person, the VFA Licence Holder should consider a number of factors including from where customer instructions are being received; the source of funds; the destination of funds; payment references or rationale that do not appear to relate to the purported customer; and any unusual delay in answering questions due to the purported customer having to refer to a third party.

The ability to establish the identity, jurisdiction, and purpose of each customer and business relationship or occasional transaction is essential to the compliance with the VFA Licence Holders’ obligations under the PMLA, the PMLFTR and the Implementing Procedures. In spite of the inherent challenges that prospective VFA customers pose, a VFA Licence Holder must ensure that its policies and procedures allow it to perform these functions with the same degree of confidence in the VFA context as they do for the more traditional services.

While the precise CDD measures to be applied will necessarily depend on the particular circumstances of the individual case, some broad considerations apply:

- a VFA Licence Holder cannot enter into a business relationship or undertake an occasional transaction unless it has verified the true identity of the customer and its beneficial owners where applicable;
- a VFA Licence Holder is obliged to develop a reasonable understanding of the purpose and intended nature of the business relationship;
- given the special considerations that apply to VFAs, VFA Licence Holders may likely find it appropriate to develop specific red flags that apply to dealings in VFA markets, and must train employees accordingly;
the AML/CFT policies and procedures in place should give the VFA Licence Holder assurance that the information that it obtains and retains for the purpose of CDD is accurate and is sufficient to withstand independent challenge.

In addition to the identity details to be collected for identity purposes in terms of Chapter 4 of the revised Implementing Procedures, where VFA Licence Holders are involved in any transfer of VFAs, be it as the a party to the transfer or as a facilitator thereto, they also to obtain the address of the wallet/account number to be used by the customer to either receive the VFA or to transfer VFAs.

Verification of identity would therefore also require the verification of the wallet address/account number, i.e. before the transfer of VFAs takes place, the VFA Licence Holder is to verify that the said wallet actually belongs to its customer.

2.2 Business Relationship v Occasional Transaction

The nature of the CDD measures to be carried out will be dependent amongst others on the nature of the Licence Holder’s interaction with its customers. It is assumed that in this context, VFA Licence Holders are likely to open an account for all, or at least the majority, of their customers. This is considered to be indicative of a relationship that is expected to have or has an element of duration and therefore it is deemed that there subsists a business relationship between the VFA Licence Holder and its customer. In these instances, CDD will entail identification and verification of identity obligations, establishing the intended nature and purpose of the business relationship, including source of wealth and having a customer business and risk profile, as well as on-going monitoring of the business relationship.

On the other hand, where VFA Licence Holders carry out transactions that do not meet the criteria for a ‘business relationship’, they should treat such transactions as ‘occasional transactions’ for the purposes of the PMLFTR and the Implementing Procedures. Thus, in such instances, there will be no on-going monitoring obligations and even the collection of any information on source of wealth and source of funds will be dependent on what is stated in Section 2.6 hereunder. It is important to note that in this case no thresholds will be applicable and any AML/CFT obligations would be applicable at all times.

2.3 Beneficial Ownership and Control of a Legal person/Legal arrangement

VFA Licence Holders are reminded that Regulation 7(1) of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I require that the subject person carry out CDD procedures not only in respect of the customer and its agent(s) as already described above but also in relation to a customer’s beneficial(s) owner(s), that is the individual(s) who ultimately owns and controls the customer. Depending on the nature of the customer, identification and verification measures may have to be applied in relation to a number of various parties who may own, control or direct the activities of a legal person or arrangement.

---

10 In this regard, it is to be noted that a series of amendments are to be carried out to the PMLFTR and include a widening of the definition of ‘occasional transaction’ to reflect the position described in this document.
2.4 Politically Exposed Persons

Regulation 11(5) of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I requires the subject person to maintain appropriate procedures for the purpose of determining whether a customer and, where applicable, its beneficial owners are PEPs. Where any PEPs are identified, there a series of EDD measures that have to be taken by the subject person, irrespective of whether they are foreign or domestic PEPs. It is important to point out that these measures are also applicable where the customer or the beneficial owner is a family member or a known close associate of a PEP.

Compliance with these requirements may be impacted where the VFA Issuer has not identified its customer as a legal person/arrangement and therefore has not identified the beneficial owner(s), resulting in the VFA Issuer being unable to determine whether they are PEPs or otherwise.

2.5 Inability to Complete CDD measures

Where it proves impossible to complete CDD within the stipulated timeframe, the VFA Licence Holder: (a) is not to allow any activity of any kind by the customer or provide any other service to the customer and, to this end, a VFA Licence Holder may decide to either close the customer’s account or profile or to keep it deactivated in its entirety\(^\text{11}\); and (b) determine whether it is necessary to lodge a STR with the FIAU.

Where in these circumstances the VFA Licence Holder is in possession of funds or assets belonging to the customer which may have been received in advance in relation to a service to be provided by the VFA Licence Holder, and there no grounds to suspect ML/FT or the transaction has not been suspended by the FIAU or by operation of the law, nor is there an attachment or freezing order, the VFA Licence Holder is to remit the funds or assets to the same source and through the same channels used to receive them, and this after having considered whether there is any other legal impediment to their remittance\(^\text{12}\). To the extent possible, the Licence Holder should indicate in any transaction script that the funds or assets are being remitted back due to the inability to complete CDD.

2.6 Obtaining Information on the Purpose and Intended Nature of the Business Relationship and Determining the Source of Wealth and the Source of Funds

When establishing a business relationship with a customer, VFA Licence Holders are required to obtain information on the purpose and intended nature of that relationship in accordance with the requirements of Regulation 7(1)(c) of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I. In so far as the purpose of the business relationship is concerned, VFA Licence Holders are to determine the purpose behind the dealing(s) in VFAs, i.e. why is the customer seeking to acquire, dispose or otherwise invest in VFAs. With regards to the intended nature of the business relationship, VFA Licence Holders must collect sufficient information and, where necessary,

---

\(^\text{11}\) In the context of a business relationship, therefore, although an account may be opened for the customer, no activity on the same is to be allowed.

\(^\text{12}\) In the event the VFA Licence Holder is unable to remit the funds or assets to the same source through the same channels, it will inevitably have to request fresh instructions from its customer. In the event that these instructions give rise to a suspicion on the part of the VFA Licence Holder, it should submit a STR and suspend the remittance pending the FIAU expressing its opposition or otherwise to the said transaction.
documentation, to establish a prospective customer’s proposed level of activity as well as to determine his source of wealth and his expected source funds.

Source of wealth consists in the economic activity or activities which generate the customer’s wealth. This may be comprised of, for instance, income through employment or business, or inheritance. The term ‘source of funds’ refers to the activity, event, business, occupation or employment generating the funds used in a particular transaction, or to be used in future transactions.

Existing requirements for checking the source of wealth and funds are risk-sensitive, such that VFA Licence Holders are given the flexibility to adapt their actions to the perceived risks depending on the outcome of the risk assessment referred to in Section 2.2 of Part A of these sector-specific Implementing Procedures. Whilst VFA Licence Holders are entitled to rely on sufficiently detailed declarations provided by the customer, they must assess whether such information actually makes sense in light of what they know about the customer and whether this matches the profile of that customer. Where gaps remain or discrepancies arise, or the business relationship is otherwise deemed to be high risk, the VFA Licence Holder should make further inquiries, request independent third party evidence of source of wealth and consider raising an STR in accordance with Section 3.2 of Part A of these Implementing Procedures if its requests for additional information and/or documentation go unanswered.

It is important to note that source of funds information will not be required for each and every transaction but (a) at the inception of the business relationship so as to establish from where funds to be used are likely to originate; and (b) when an unusual transaction is detected. In determining the source of funds, VFA Licence Holders should consider the method to effect payment or carry out the transaction as this will inevitably impact the nature and degree of information to be collected on source of funds. Where payment is being made, or the transaction is carried out, in fiat currency and it originates from an account in the name of the customer held with a bank or payment institution established in the EEA or other reputable jurisdiction, or otherwise through a credit or debit card issued by a bank or payment institution established in the EEA or other reputable jurisdiction, the degree of information required for source of funds purposes need not be as extensive as in situations where anonymous payment methods are used.

In the case of payments effected by means of, or transactions involving, VFAs, the source of funds will consists in determining how these were obtained by the customer. In the event that the VFA Licence Holder determines (and adequately documents) that the VFAs have been created by the customer (e.g. through actively mining the same), the need to obtain additional information from the customer will be dependent on the amount or value involved. Where this is significant, the VFA Licence Holder will be expected to substantiate its determination with documentation on the mining operation that led to the creation of the VFAs (e.g. through the collection of electricity bills, hardware receipts etc.) and consider whether the information obtained makes sense within the context of the source of wealth information obtained by the VFA Licence Holder. On the other hand, if the VFAs have originated from alternative sources, the VFA Licence Holder must request evidence of previous transactions effected by the customer to determine the activity that led to the customer being in possession of these VFAs.

In addition, whenever payments or transactions are made using VFAs, a VFA Licence Holder is required to have systems in place to:

- check the wallet address/account for negative information in the public domain; and
• use distributed ledger analytical tools to, *inter alia*, detect potentially fraudulent transactions and other suspicious activity (e.g.: the VFAs were used on the darkweb or in connection with a ransomware attack).

Any negative information should be factored into the customer risk assessment and should be considered by the VFA Issuer to determine whether it is willing to proceed with the transaction or whether it should desist from doing so and file a STR with the FIAU. In determining the way forward, the VFA Issuer should consider how remote is the connection both from the temporal aspect as well as from the transactional aspect. It is important to note that the use of these systems is not dependent on risk and they must therefore be used whenever one accepts VFAs as payment.

While establishing a customer’s source of wealth and his source of funds are express requirements in the case of a business relationship, it should be borne in mind determining a customer’s source of wealth and source of funds may still be required in the context of an occasional transaction. Where the ML/FT risk within an occasional transaction is assessed to be high and therefore requiring the taking of EDD measures, it is very likely that the most effective measure that can be taken is to query how the funds being used have been acquired and whether this makes sense considering the customer’s source of wealth. In any such circumstances, VFA Licence Holders would therefore still be expected to establish a customer’s source of wealth and source of funds, unless they apply alternative measures that can be shown to be equally effective to address the risks identified.

3. **Ongoing Monitoring**

To the extent that a VFA Licence Holder maintains an ongoing business relationship with a customer, the VFA Licence Holder is obliged to have in place ongoing monitoring procedures as required by Regulation 7 of the PMLFTR and Chapter 4 of the Revised Implementing Procedures – Part I.

In carrying out on-going monitoring of a business relationship, VFA Licence Holders have to:

i. ensure that the documents, data or information held are kept up-to-date, i.e.:

   a. obtain fresh identification documents when the expiry date of identification documents held on the customer is reached. This can be done on a risk-sensitive basis or be linked to specific trigger events;

   b. question the data and information already in its possession whenever any inconsistencies with the same arise however noticed.

   This is not a requirement to carry out CDD measures afresh but to ensure that a VFA Licence Holder’s knowledge of the customer and the information in its possession is kept up to date. VFA Licence Holders should determine on a risk sensitive basis whether any new information needs to be verified or whether changes are so substantial as to require the carrying out of its customer risk assessment and/or its CDD afresh.

   And

   ii. scrutinise the transactions undertaken throughout the course of that relationship to ensure that they are consistent with the VFA Licence Holder’s knowledge of the customer and that
customer’s business and risk profile. Where a VFA Licence Holder notices that a customer’s account activity is not in keeping with what it knows or expects from the customer (e.g. activity not justified on the basis of a customer’s source of wealth or not in keeping with the average profile or account activity noted to date, activity does not reflect a customer’s usual transactional patterns etc.), the VFA Licence Holder has to question this unusual activity and, where necessary, establish what is the source of the funds used for the said activity.

For this purpose, VFA Licence Holder should establish a risk-based transaction monitoring program in accordance with the requirements of Regulation 7 of the PMLFTR and Chapter 4 of the revised Implementing Procedures – Part I. Such transaction monitoring program should:

- include appropriate risk-based systems and controls to monitor the transactions of customers;
- identify transactions that are considered to be unusual or suspicious; and
- be capable of identifying complex, unusually large transactions and unusual patterns of transactions which have no apparent economic or visible lawful purpose.

A risk-based transaction monitoring program in terms of (i) above should include, at least, the following elements:

- risk-based processes for recognising ML/FT typologies and transaction patterns indicating suspicious behaviour (for example, customers making large, structured cash deposits, and then subsequently transferring the funds electronically to unrelated accounts);
- processes to establish customer transaction profiles that include the customer’s transaction history (for example, to identify instances where a customer has conducted activity inconsistent with their profile);
- processes to identify situations where a customer uses multiple wallets for the same VFA or changes wallets for the same VFA;
- processes to compare established customer transaction profiles against risk-based typologies and transaction patterns; and
- processes to assign alerts to customers identified as high risk or those conducting transactions indicating suspicious behaviour.

What constitutes complex, unusual or large transactions or unusual patterns of transactions for the purposes of (iii) above differs for each VFA Licence Holder. It depends on the size, types of customers, products and delivery channels and risk profile. However, generally, complex and unusual transactions might include:

- transactions of an unusually large size or volume relative to the customer profile (or usual customer behaviour);
- transactions that exceed the VFA Licence Holder’s internal thresholds or reporting triggers;
- transactions to or from a high-risk country;
- transfers to or from a designated person on a sanctions list;
- changes in transaction activity that are inconsistent with the size of past patterns or risk profile; and
- irregular patterns of account activity that are characteristic of ML/FT.
Depending on the outcome of their ongoing monitoring exercise, VFA Licence Holders should consider taking one or more of the following measures:

- seek further information from the customer or third party sources to clarify/update the customer’s information, obtain further information about the customer, and/or obtain more detailed information about the source of wealth/funds the customer is using to invest/ transact in VFAs;
- undertake more detailed analysis of the customer’s information and/or transaction history;
- re-verify CDD information;
- seek senior management approval for processing any future transactions; and
- consider whether updates to the customer risk assessment are warranted.

Without prejudice to the generality of the foregoing, the below table sets out some non-exhaustive indicative examples of processes and system capabilities that VFA Licence Holders may wish to put in place to monitor transactions and identify higher risk transactions that may require enhanced monitoring, investigation or reporting. VFA Licence Holders are encouraged to consider the below factors to the extent applicable to the activities undertaken by particular VFA Licence Holders and to the extent that VFA Licence Holders are able to monitor the activities of their customers.

<table>
<thead>
<tr>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Develop customer profiles and identify irregular and unusual transactions | • identify customers whose predominant source of funds are derived from cash or cash-equivalent transactions, other digital currency exchanges and third-party payment processes that provide anonymity to the source of funds  
• identify transactional activity that appears excessive for the customer, given their known source of wealth  
• identify businesses transacting through digital currency exchanges in a manner expected of individuals (could indicate a front, shell and/or shelf companies)  
• identify non-profit organisations transacting through digital currency exchanges in a manner expected of individuals (this could indicate misappropriation of funds)  
• identify, where applicable, large purchases  
• identify instances where account holders have multiple private wallets and frequent changes are made in these wallets potentially with the intention to bypass the system |
| Identify rapid exchange of currencies | • identify rapid incoming and outgoing exchange transactions  
• identify rapid flow through of funds to external financial institutions, where deposit and outflow |
| Identify rapid movements of funds | • identify the customer undertaking multiple transactions concurrently of varying amounts and in different digital currencies |
| Identify interactions with known mixers, the use of high-risk counterparties and | • identify customers attempting to obfuscate the movement of funds |
| transactions that use the darknet | • identify customers attempting to obfuscate the movement, source or destination of funds such as through the use of digital currency mixers/tumblers  
• identify customers who subsequently transact with higher risk counterparties such as illicit marketplaces and/or illegal offshore gambling websites  
• identify customers who are trying to obfuscate transactions with higher risk counterparties – for example, by transferring funds to a private wallet which then deals with the higher risk counterparty  
• identify customers who are trying to obscure the perpetrators of ransomware |

4. AML/CFT Audit

In terms of Regulation 5(5)(d) of the PMLFTR, subject persons are to implement, where appropriate with regard to the nature and size of its business, an independent audit function to test its internal measures, policies, controls and procedures. Given the nature of the business undertaken by VFA Licence Holders, the FIAU considers that an audit of a VFA Licence Holder’s measures, policies, controls and procedures should be carried out at least annually once the VFA Licence Holder has commenced its activities and that such an audit should be carried out by a party which is external to the VFA Licence Holder (as well as to the group which the VFA Licence Holder may form part of) to ensure independence; this in an effort to ensure the effectiveness of the said measures, policies, controls and procedures. Such an AML/CFT audit must also be carried out upon any material changes/enhancement to the AML/CFT programme or at such more frequent intervals as may be directed by the FIAU.

The purpose of an AML/CFT audit is to serve as a systematic check of the VFA Licence Holder’s AML/CFT systems and controls and the end result should be a written report on whether:

- the VFA Licence Holder’s AML/CFT programme is fit for purpose and compliant with the obligations of the VFA Licence Holder under the applicable AML/CFT framework;
- the AML/CFT systems and controls were adequate and effective throughout the audit period; and
- any changes are required.

For the purposes of the report, the AML/CFT audit must:

- attest to the overall integrity and effectiveness of the AML/CFT systems and controls;
- test the VFA Licence Holder’s risks and exposures with respect to size, business lines, customer base and geographic locations;
- assess the adequacy of internal policies and procedures;
- test compliance with the relevant laws and regulations;
- test transactions in all areas with emphasis on high-risk areas, products and services;
- test the accuracy and quality of data;
- test the verification methods adopted by the VFA Licence Holder;
- test the audit trail and record-keeping capabilities;
• test employees’ knowledge of the laws, regulations, guidance, and policies and procedures;
• test the adequacy, accuracy and completeness of training programmes; and
• test the adequacy of the process of identifying suspicious activity.

The AML/CFT auditor engaged by the VFA Licence Holder should be proficient in the PMLFTR, the Implementing Procedures, and this Guidance, and should also possess technological expertise specific to the system used by the VFA Licence Holder in the performance of its AML/CFT obligations. Where the AML/CFT auditor and the Systems Auditor appointed by the VFA Licence Holder in terms of the MFSA’s VFA Rules for VFA Licence Holder are separate, and since it is likely that most VFA Licence Holder will rely on technology to perform their AML/CFT obligations, it is advisable that the AML/CFT auditor liaises with the Systems Auditor so as to obtain an in-depth understanding of the functionalities and capabilities of the system and therefore be in a better position to test compliance thereto.

The audit report should be addressed to the VFA Licence Holder’s senior management so they can decide what (if any) next steps are required. A copy of the audit report, together with management’s responses, shall be made available to the FIAU and relevant supervisory authorities upon request.

5. Reliance and Outsourcing

5.1 Reliance

Regulation 12 of the PMLFTR and Chapter 4 of the Revised Implementing Procedures – Part I allow for the exercise of reliance, with the subject person relying on the information and documentation collected at customer on-boarding stage by any other person or entity in an EU Member State or a reputable jurisdiction who is subject to AML/CFT requirements and supervision equivalent to those required in terms of Directive 2015/849/EU. In determining as much, VFA Licence Holders can refer to FATF/Moneyval evaluation reports, IMF Country Reports etc.

When exercising reliance, a VFA Licence Holder has to obtain the identification information from the third party it is relying upon but does not need to request the customer to provide it with any verification documents. However, the VFA Licence Holder must have an agreement with the third party being relied upon for any such documents to be made available upon request and this arrangement must be tested from time to time to ensure that it actually functions as set out in the agreement. Moreover, the VFA Licence Holder remains responsible for the carrying out of a customer-specific risk assessment and determining whether the customer is a PEP. VFA Licence Holders will be able to exercise reliance to meet their CDD obligations as long as the conditions described above are met.

In the context of reliance, it is possible for VFA Licence Holders to place reliance on other subject persons licensed under the VFAA. This could allow for a more streamlined and efficient CDD process.

5.2 Outsourcing

Where a VFA Licence Holder considers outsourcing the implementation of its AML/CFT obligations, it is important that the VFA Licence Holder bears in mind that it will remain responsible at all times for compliance with the said obligations. More importantly, VFA Licence Holder are to comply with the outsourcing conditions and limitations set forth under Chapter 6 of the Revised Implementing Procedures – Part I.
VFA Licence Holders are to remember that, whether they exercise reliance or enter into an outsourcing arrangement, they remain responsible for ensuring compliance with their AML/CFT obligations at all times.
Annex I

1. **Case Law highlighting the ML/FT Risks of VFAs**

*United States of America vs. Ross William Ulbricht, aka “Dread Pirate Roberts”, aka “DPR”, aka “Silk Road”, Southern District of New York Court, filed on 27 September 2013*

Convicted on seven counts in February 2015, Ross William Ulbricht – under the username Dread Pirate Roberts (“DPR”) – was the creator and operator of Silk Road, a large and anonymous criminal marketplace which operated using Tor Network, which in turn makes internet traffic extremely difficult to trace. Users of Silk Road bought illegal material such as hacking software and illegal substances; and the transactions on Silk Road used Bitcoins exclusively (Bitcoins were in this case described as an anonymous but traceable crypto-currency) – to the extent that even Silk Road’s employees were paid in this currency. Ulbricht was arrested in October 2013, and the government declared that between the years 2011 and 2013, thousands of vendors had used Silk Road to sell an estimate of $183 million worth of illegal material, goods and other services; of which the defendant earned millions of dollars from the proceeds of this crime. One of the charges brought against Ulbricht was that of facilitating the laundering of the proceeds of sales through the use of Bitcoin.

Owing to the anonymity surrounding Silk Road’s operation, discovering DPR’s actual identity proved troublesome to law enforcement agents. Any party interested in using Silk Road could only do so through the Tor browser, which hides the IP addresses of its users. Accounts on Silk Road were created swiftly since users did not disclose any personal information and no user identification was required. Transactions on Silk Road were all done using Bitcoin. Users were required to deposit Bitcoin into their account, and transact with sellers using the same. To exchange Bitcoins into FIAT currencies, the Bitcoin had to be withdrawn and exchanged using a Bitcoin to FIAT exchange. Further, allegedly, a Bitcoin tumbler was implanted to the payment system, with the intention of ‘mixing’ the addresses of incoming and outgoing transactions with dummy transactions, making it extremely hard to detect and trace transactions back to their respective owners. The installation of a tumbler – which is a feature independent of Bitcoin – evidences an intention to facilitate the laundering of criminal proceeds, since it adds a thick layer of anonymity. Hence, Bitcoin can be made to be as anonymous as the user wishes it to be since albeit it is naturally pseudonymous, a tumbler is anonymous and thus may be used and implemented to ‘hide’ the provenance of a Bitcoin transaction.

*United States of America v. Liberty Reserve S.A., United States District Court for the Southern District of New York, filed on 28 May 2013*

Liberty Reserve was designed to avoid regulatory and law enforcement scrutiny and aid criminals in their distribution, store and launder of the proceeds of a number of illicit activity, including credit card fraud, investment fraud, computer hacking, identity theft, narcotics trafficking and child pornography. This was achieved by enabling criminals to conduct anonymous and untraceable financial transactions. Payment was made through its own crypto-currency – the Liberty Dollars – however, at each end, transfers were denominated and stored in FIAT currency. Basic identification was required for users of Liberty Reserve, however Liberty Reserve did not validate or verify the data.

To add a further layer of anonymity, Liberty Reserve did not allow direct deposits or withdrawals from users, but required its users to make deposits and withdrawals through recommended third party
exchangers – which were generally unlicensed money transmitting businesses operating in several countries without significant governmental money laundering oversight or regulation – and in so doing, Liberty Reserve evaded collecting information and creating a central paper trail about its users. Moreover, Liberty Reserve also allowed its users to create an extra layer of privacy by granting its users the possibility of hiding their Liberty Reserve account numbers when transferring funds at an extra “privacy fee”, rendering the transfers completely untraceable.

2. Case Studies on the Use of VFAs for ML/FT Purposes

Case Study 1

An organised crime group engaged in ‘crypto-cleansing’. To do so, they opened verified accounts at Bitcoin exchanges, where money mules were used as frontmen with false identity documents (purchased over the dark web) for verification. Their anonymity was further strengthened by adopting pseudonyms, using anonymous e-wallets and running log-less virtual private networks (“VPNs”) and blockchain-optimised smartphones. Bank accounts were then opened by money mules in a third country with false foreign identity documents. In turn, the money mules pass on all the credentials to the criminals, this includes the online credentials in relation to the bank account, the debit and credit cards.

They would then transfer the ‘dirty’ Bitcoins from Bitcoin addresses to exchanges, using mixers/tumblers. Finally, Bitcoins would be transferred from the exchanger to the local bank accounts opened by money mules. Since the criminal money was previously already separated from its original source, the criminals appeared to simply request a transaction from the exchange to the local bank account that was opened by money mules. These bank accounts were typically used for short periods of time.

In order to conceal the primary coin’s audit trail, the criminals used tumblers or mixers, which in turn swap primary coin addresses for temporary digital wallet addresses to hinder audit traceability. Another tactic used by these criminals was to intentionally use false recipient addresses to re-route transactions to backup addresses, in so doing disrupting the audit ledger.

Case Study 2

To avoid identification procedures, the criminal depositors used crypto-currency ATMs and applied smurfing techniques to split the funds into insignificant batches of money. Subsequently, they made multiple deposits to several crypto-currency ATMs machines in different locations, totalling to aggregate, significant amounts.

Case Study 3

A terrorist organisation ran a social media fundraising campaign and provided a bitcoin address to which donors could send funds. It was subsequently revealed that this address was part of a bitcoin wallet which included 16 other bitcoin addresses. A single donor was detected as having effected a considerable amount of transactions, with the bitcoins transferred to the said wallet always being obtained through an online cryptocurrency exchange that allowed the instant acquisition of crypto-currencies without customers having to identify themselves or undergo any verification of identity measures.
A number of outbound transactions were made to wallets belonging to other online cryptocurrency exchanges, probably to have the bitcoin converted into FIAT currency and transferred further into bank accounts controlled by the fund raising organiser. Other transactions were made to e-commerce sites that accept payment in bitcoins for the acquisition of goods.