FINANCIAL INTELLIGENCE ANALYSIS UNIT

IMPLEMENTING PROCEDURES

WWW.FIUMALTA.ORG

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

ISSUED BY THE FINANCIAL INTELLIGENCE ANALYSIS UNIT IN TERMS OF THE PROVISIONS OF THE PREVENTION OF MONEY LAUNDERING AND FUNDING OF TERRORISM REGULATIONS (S.L. 373.01)

PART II

FIRST ISSUED ON 3 FEBRUARY 2020

65C, Tower Street,
Birkirkara BKR 4012,
Malta

Telephone: (+356) 21 231 333
Fax: (+356) 21 231 090
E-mail: info@fiumalta.org
Website: www.fiumalta.org

TABLE OF CONTENTS

TABLE OF CONTENTS CONTINUED

ABBREVIATIONS

AML	Anti-Money Laundering
ATM	Automated Teller Machine
BRA	Business Risk Assessment
BTC	Bitcoin
CDD	Customer Due Diligence
CFT	Countering the Funding of Terrorism
CRA	Customer Risk Assessment
DASH	Dash
DLT	Distributed Ledger Technology
EDD	Enhanced Due Diligence
EEA	European Economic Area
EUROPOL	European Union Agency for Law Enforcement Cooperation
FATF	Financial Action Task Force
FIAU	Financial Intelligence Analysis Unit
FIU	Financial Intelligence Unit
FSRB	FATF-Style Regional Body
FT	Funding of Terrorism
IOCTA	Internet Organised Crime Threat Assessment
IP	Internet Protocol
LEA	Law Enforcement Agency
ML	Money Laundering
NRA	National Risk Assessment
PMLA	Prevention of Money Laundering Act
PMLFTR	Prevention of Money Laundering and Funding of Terrorism Regulations
SNRA	Supranational Risk Assessment
STR	Suspicious Transaction Report
TESAT	Terrorist Situation and Trend Report
TOR	The Onion Router
VFA	Virtual Financial Asset
VPN	Virtual Private Network
XML	Lumen
XMR	Monero
ZEC	ZCash

INTRODUCTION

Legal Notice 430 of 2018 extended the application of the PMLFTR to activities regulated by the VFA Act, rendering VFA agents, VFA service providers and anyone offering VFAs to the public subject persons. This entails that anyone carrying out the said activities has to comply with the obligations arising from the PMLA, the PMLFTR and the Implementing Procedures – Part I. However, in view of the specific characteristics of VFAs and related activities, it is recognised that there is a need for sector-specific guidance to assist in ensuring compliance with the AML/CFT obligations arising from the PMLFTR. The FIAU is therefore issuing the present sector-specific Implementing Procedures.

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 thereof to the VFA area. 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-related activities. In case of any such conflicts, these sector-specific Implementing Procedures are to prevail over the relevant sections of the Implementing Procedures – Part I.

Other subject persons may be handling VFAs in the course of carrying out either relevant financial business or relevant activity even though not licensed as VFA service providers[1]. Any such subject person would not only be expected to abide by the Implementing Procedures – Part I and any sector-specific Implementing Procedures that the FIAU may issue relative to the particular relevant financial business or relevant activity it is carrying out but, to the extent applicable, even with these Implementing Procedures.

1. Reference is here being made to the activities falling within paragraphs (f), (g), (n) and (o) of Regulation 4(1) of the Virtual Financial Assets Act Regulations, all of which fall to be considered as either relevant financial business or relevant activity in terms of the PMLFTR. Depending on the particular context in which they take place, other activities listed in paragraphs (c), (j) and (k) of Regulation 4(1) may also fall to be considered as relevant financial business or relevant activity.

CHAPTER 1 - ML/FT RISKS INHERENT in VFAs and VFA ACTIVITIES

Regulation 5 of the PMLFTR obliges subject persons to carry out a BRA to identify the ML/FT risks they are exposed to, i.e. what vulnerabilities does a given activity present that may be exploited for ML/FT and what threats the said activity is exposed to which may seek to exploit the identified vulnerabilities for ML/FT. Any such assessment has to include a qualitative and quantitative analysis. This obligation equally extends to subject persons carrying out the activities listed in paragraph (l) to paragraph (n) of the definition of "relevant financial business".

The Implementing Procedures – Part I already provide a series of risk factors to be taken into consideration by all subject persons, including anyone carrying out any of the aforementioned activities. Thus, aspects like the customer and the geographical risk factors would be equally applicable in all circumstances. By way of example, a PEP and/or a family member and/or close business associate of a PEP is always to be regarded as a customer presenting higher risks of ML, as would someone who resides in and/or has activities located in a non-reputable or high risk jurisdiction.

However, in the case of VFA activities there may be particular risk factors to consider that may not be applicable across the board. By way of example, one would have to consider whether:

(a) The customer resides or is established in jurisdictions known for the carrying out or conduct of cybercrime activities – where this is the case, the possibility that any VFAs already held by the customer and which he proposes to use in transactions involving the subject person may have been derived through criminal activity like ransomware attacks and hacks may be higher;

(b) A customer who has a VFA-related business is subject to regulation and supervision in the area of AML/CFT. While international and national standards are evolving to cater for this new reality and ensure that operators in this area are subject to AML/CFT requirements and a proper level of supervision, it is not a given that all jurisdictions are applying the said requirements or are equally supervising the application and enforcement of the said requirements;

(c) The customer receives frequent or large value deposits of VFAs through crypto-ATMs located in high risk jurisdictions or areas known for their high rate of criminal activity. Considering the high incidence of cash in the criminal world, crypto-ATMs may provide a useful channel through which any such proceeds of crime is introduced into the financial system. The same can be said where withdrawals are affected through these ATMs, especially if their operators are not subject to any form of regulatory or supervisory oversight.

1. ML/FT RISKS INHERENT IN VFAS AND VFA ACTIVITIES CONTINUED

The interface risk may be especially relevant in this context due to the remote nature of most interaction that takes place between service providers and customers in this area, especially considering the possible use of VPNs, proxy servers or TOR to obfuscate one's IP address. In addition, there is a greater risk that customers may seek to submit false, altered or forged identification verification documents. It is therefore important that adequate mitigating measures are taken in this respect.

When it comes to the consideration of the product/service/transaction risk, it is expected that the BRA of a subject person involved in VFA activities will take into account the particular nature of VFAs as well as the underlying and associated technologies that can impact the ML/FT risk arising therefrom. Because of determinate characteristics, VFAs are often associated with illicit activities and ML as well as providing an additional means for FT. These characteristics are:

Anonymity: VFAs are often described as being anonymous and allowing for transactions to take place anonymously. However, it has to be remarked that different VFAs will present different levels of anonymity. BTC is often described as being a pseudo-anonymous VFA as its blockchain still allows for the identification of the address from which BTC were sent and the address where they were received. However, it is not possible on the basis of the blockchain to link the address with the identity of an individual or entity as the BTC protocol does not require that whoever is exercising control over an address be identified and verified.

In addition, it has to be borne in mind that there are a number of technological means that can further obfuscate the traceability of VFA transactions. These would include the use of coin mixing or tumbling services.

Other VFAs often termed as "privacy coins" provide an even higher level of anonymity. These would include VFAs like XMR, ZEC and DASH. Some of these VFAs have features which allow for the obfuscation of the address of both the sender and the receiver as well as of the amount sent, significantly increasing anonymity and the risk that they may be used for illicit activities and ML/FT. It has to be pointed out that any subject person willing to be involved in transactions involving privacy coins may find himself to be running counter to the basic principle of the risk-based approach if, as explained later on, no mitigating measure

can be applied to undo the anonymity and/or inability to trace transactions associated with privacy coins.

Immediacy and Irrevocability: VFA transactions can be very quick, with the speed varying depending on the VFA being used. Moreover, VFAs are supported by a whole ecosystem of services and products which allows them to be accessed anytime anywhere: one's physical location is irrelevant. In addition, the development of crypto-ATMs and crypto-backed debit cards further increases the ability to use and/or convert one's VFAs.

VFA transactions are also irrevocable, i.e. once VFAs are sent to an address, they can be recovered by the sender only if the recipient agrees to return the same and transfers them back. Unlike in the case of more conventional services, no chargebacks are possible nor is it possible for the authorities to enforce the freezing and/or seizure of VFAs held in an address associated with a private wallet given that no identity is associated therewith.

Decentralisation: VFAs are one category of DLT assets, i.e. they are dependent on and make use of DLT. This implies an element of decentralisation which can vary from one VFA to another but is usually taken to mean that there is no central authority overseeing what is taking place on the underlying blockchain nor is there the need for a third party intermediary when VFAs are to be transferred from one address to another.

The payment or funding means accepted also have to be factored in, as some of the said means may expose the subject person to a higher ML/FT risk than others. While accepting funds held in accounts or made available by credit or financial institutions located within the EEA or other reputable jurisdictions may not increase the risk of ML/FT, accepting payment in cash or through pre-paid cards would increase the risk of ML/FT that a subject person is exposed to. The same applies where funds are made available through crypto-backed debit cards.

The same applies with regards to the kind of wallet used by one's customers. While understandable from a security perspective, the use of private wallets, especially when they allow for cold storage, increases the risk of ML/FT as does

1. ML/FT RISKS INHERENT IN VFAS AND VFA ACTIVITIES CONTINUED

the use of custodial wallets held with institutions that are not subject to any level of AML/CFT regulation and/or effective supervision.

All of the above render VFAs an ideal medium for ML/FT, as also evidenced by the trends and case-studies provided in Annex I to this document. Hence why both the NRA and the SNRA regard VFAs as presenting a considerable risk from a ML/FT perspective.

To better understand the ML/FT risks associated with VFAs, subject persons can refer to a number of publications including Guidance Documents issued by the FATF[2] and criminal activity assessments carried out by EUROPOL[3]. A number of reputable service providers active in the VFA area also issue publications that can further assist subject persons in deepening their understanding of ML/FT risks associated with VFAs. FSRBs and individual FIUs are also known to publish trends and typologies that could be of assistance to subject persons active in this area. It should also be borne in mind that subject persons have to take into account the SNRA and NRA whenever considering and assessing the ML/FT risk inherent to their activities.

2. VFA related documents issued by the FATF include *Virtual Currencies: Key Definitions and Potential AML/CFT Risks* (2014), *Guidance for a Risk-Based Approach to Virtual Currencies* (2015); and *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (2019).
3. EUROPOL publishes periodical reports that can shed light on current criminal trends and how these involve VFAs. These include the *Internet Organised Crime Threat Assessment* and the *Terrorist Situation and Trend Report*.

CHAPTER 2 – THE IMPLEMENTING PROCEDURES

The definition of "relevant financial business" includes a reference to "VFA services carried out by a person or institution licensed or required to be licensed under the provisions of the Virtual Financial Assets Act". Thus, anyone who is either in possession of a valid licence granted in terms of the VFA Act to provide a VFA service, or who has notified the MFSA of its intention to apply for a licence and is allowed to continue providing VFA services pending filing and consideration of the said licence application, is considered a subject person in terms of the PMLFTR. The same applies with regards to anyone providing a VFA service requiring a licence in terms of Article 13(1) of the VFA Act but who, for one reason or another, would not have obtained a licence as set out hereabove.

2.1 THE RISK-BASED APPROACH

The PMLFTR adopt a risk-based approach to AML/CFT, i.e. it is the risk of ML/FT inherent in a subject person's activities that has to determine the nature and extent of the mitigating measures adopted to address the same. Hence why the PMLFTR require subject persons to carry out both a BRA as well as a CRA, the former to identify the ML/FT risks to which the VFA service provider is exposed to at the business level and the latter to determine the ML/FT risks inherent in a given business relationship or occasional transaction. While the BRA will allow the VFA service provider to identify what kind of mitigating measures it needs to adopt, the CRA will allow the VFA service provider to determine to what extent and at which stage it is to apply the said mitigating measures when it comes to an individual business relationship or an occasional transaction.

The Implementing Procedures – Part I set out risk factors that are to be taken into account by any subject person. These are equally applicable to VFA service providers. However, as already set out in Chapter 1, subject persons have to also consider risk factors particular to their activity and associated therewith. A case in point would be privacy coins, i.e. VFAs that have features intended to enhance the pseudo-anonymity usually associated with VFAs. Transacting in such VFAs would increase the risk of ML/FT to which the VFA service provider is exposed to, especially if a customer's portfolio includes only privacy coins, as it becomes even more difficult to establish some form of connection with the customer. Moreover, their enhanced anonymity entails that they are more likely to have been acquired through, or that they will be used in, criminal activity[4].

The BRA is not intended to be a static document but has to be reviewed from time to time and, where necessary, updated. The Implementing Procedures – Part I set out when this should be done. Possible instances include the launch of a new product or service, targeting a new customer segment or jurisdiction, a merger

or acquisition, the organisational structure of your business and the use made of any agents, branches etc. However, given the nature of the VFA area and the rapidity with which developments take place, VFA service providers are expected to review the BRA on a six-monthly basis rather than on an annual basis as provided for in the Implementing Procedures – Part I. Should any change, as is referred to in the Implementing Procedures – Part I, occur prior to the lapse of the said six months, then the VFA service provider would need to review its BRA and consider whether any updates are necessary.

The BRA is a key in determining the mitigating measures to be adopted by the VFA service provider: understanding one's risks allows the proper design, implementation and application of the measures necessary to control, mitigate and where possible neutralise the risks identified. As implied by the risk-based approach, measures are to be stricter and resources are to be invested where the risk is higher. Mitigating measures consist in CDD measures as well as internal procedures and controls designed to ensure the proper, correct and uniform application of mitigating measures. Employee screening and training measures also form part of these mitigating measures. An update of the BRA should lead to a reconsideration of one's mitigating measures to make sure that the existing mitigating measures are sufficient to address any newly identified ML/FT risks. In addition, it is possible that an update of the BRA may also require a revision of individual CRAs.

The CRA is also to be carried out in line with the Implementing Procedures – Part I, though here again there are risk indicators specific to VFA service providers. In addition, it is important to bear in mind that the CRA is not static but has to be kept updated to reflect aspects encountered throughout a business relationship. By way of example, this may include the use of proxies, unverifiable IP addresses or geographical location, disposable email addresses or mobile numbers, and the use of different devices to conduct transactions by the customer to obscure his actual location or to circumvent restrictions on activity imposed by the VFA service provider. All of these aspects should be duly considered from the risk point of view and factored into the CRA, whether they are manifested at the initial stages of a business relationship or otherwise.

4. Where the ML/FT risk arising from a business relationship or occasional transaction is due to the presence of privacy coins, mitigating this risk would require obtaining reliable and independent information on the transaction history of the given coins. Should it not be possible to trace at all from where the privacy coins originated, and absent any additional risk mitigating measure that could sufficiently mitigate the risk associated with these coins, then a subject person would have to reconsider dealing in the same as it would be acting outside the parameters of the risk based approach

A series of red flags are provided in Annex I hereto which are not only intended to highlight possible instances where the subject person is expected to question further the customer as to its conduct and, if warranted, file a STR, but should also lead the VFA service provider to consider (a) whether the ML/FT risk levels associated with the said customer are still current; and (b) where this is not the case what additional mitigating measures need to be taken so as to better cater for the increased risk levels identified.

The request of additional services and/or an increase in activity by the customer should also lead the VFA service provider to review the CRA so as to determine if an update is required and/or additional mitigating measures are to be applied. Having a customer who acquires EUR 100 worth of BTC on a quarterly basis presents a given level of ML/FT risk but if he increases his activity to acquire EUR 1000 worth of BTC on a monthly basis, the associated level of ML/FT risk will inevitably increase.

2.2 CUSTOMER DUE DILIGENCE

The BRA is to lead to the adoption of risk mitigating measures, including the CDD measures required in terms of Regulation 7 to Regulation 11 of the PMLFTR as further explained in the Implementing Procedures Part I and the present document. A VFA service provider has to carry out CDD on any customer that wants to make use of its services as set out in Chapter 4 of the Implementing Procedures – Part I. The said chapter makes considerable allowances with regards to the use of technological means for the carrying out of CDD measures, including when it comes to the identification of the customer, the verification of the customer's identity and on-going monitoring. VFA service providers have therefore to ensure that any AML/CFT measures, policies, procedures and controls they adopt reflect the requirements of the PMLFTR and the Implementing Procedures – Part I.

CDD measures are to be applied on a risk sensitive basis, i.e. the VFA service provider can vary the timing and extent of their application depending on the level and nature of ML/FT risks inherent in the business relationship or occasional transaction. Thus, an enhanced level of CDD is to be applied in situations presenting a high risk of ML/FT while a simplified level of CDD can be applied in situations presenting a low risk of ML/FT.

In this regard, subject persons have to note that:

(a) In situations presenting a high risk of ML/FT, the mitigating measure/s adopted as a form of EDD have to address the root cause resulting in the said high

risk. If the causes are more than one, then one has to consider whether one or more mitigating measures need to be applied to properly address the risks identified.

(b) SDD is not to be considered as an exemption from CDD given that, as a minimum, every subject person is expected to identify the customer, and to apply and carry out a level of on-going monitoring to ensure that a business relationship remains at all times low risk: once the risk level increases, the other CDD measures and any necessary EDD measures would have to be applied. The application of these additional measures may be triggered once a given threshold is met or an event materialises itself. SDD may also mean that some measures are applied in a more diluted form than in normal or high-risk situations.

(c) Among the factors that a VFA service provider is to consider in determining whether SDD is to be applied or otherwise is the ease with which the pre-established triggers for the application of any outstanding CDD measures can be circumvented. One such possibility is the circumvention of a threshold-based approach through the opening of multiple accounts by the same customer, whether under his own name or using the identities of third parties, be they real or fake. While there is no limitation on the number of accounts that a customer may hold, it is important that the VFA service provider is in a position to link the same together. For example, this may be done with the monitoring of the IP address and/or the geo-location of the devices used by the customer.

(d) The application of SDD has to comply with the requirements set out in Section 4.8 of the Implementing Procedures – Part I, with the subject person duly documenting why it considers a business relationship to present a low risk of ML/FT. In addition, SDD is not limited to the possible delay of identity verification but can take a number of other forms as explained in Section 4.8 of the Implementing Procedures – Part I.

In all instances, the reasoning which led a subject person to determine a given course of action has to be duly documented and the FIAU may require that the same be made available to it in the course of carrying out its functions at law. The same applies with regards to why determinate triggering events or thresholds leading to the application of more robust CDD measures were selected and mitigating measures considered sufficiently robust to address the identified level and nature of ML/FT risk.

One of the aspects that can influence the level of CDD applicable in a given case is the amount of funds or value of VFAs involved. While amounts and values on

their own are never to be considered in isolation to determine one's ML/FT risk exposure, especially in view of the minimal amounts/values that can be used for FT purposes, the risk of ML/FT will be lower where the amount/value involved is itself low. What amount or value can be considered as sufficiently low as to justify the application of SDD? In the absence of any indicators of a higher level of ML/FT risk, an amount or value that is below Euro one thousand (€1,000) can be taken as being representative of a low risk of ML/FT, warranting the application of SDD. In this context, and without prejudice to the generality of what has already been stated on the application of the risk-based approach, paragraph (b) and paragraph (c) above acquire particular significance and have to be given particular attention by VFA service providers. As to how it is to be determined whether this threshold is met or otherwise, reference is to be made to Section 2.2.2 hereunder.

2.2.1 The Wallet Address

The Implementing Procedures – Part I go into considerable detail as to what information and/or data needs to be collected for identification purposes. In the case of a VFA service provider who receives VFAs or is to send VFAs, the service provider is not to limit itself to the collection of the personal identification details referred to in the Implementing Procedures – Part I but it is also to collect and retain on file the address from which the VFAs are to be received or to which the VFAs are to be sent.

Together with the address, the VFA service provider is also to ask the customer whether the address relates to a private wallet, a multi-signature wallet or a custodial wallet. To the extent that the analytical tools referred to in Section 2.2.3 hereunder provide any information in this regard, the VFA subject person is expected to corroborate the information provided by the customer with the information obtained through the said tools.

The following considerations need to be made:

Private Wallet – In situations where the VFA service provider is to receive VFAs from the customer, the VFA service provider has to establish that the customer has control over the address from which the VFAs are to originate. However, this is not required in all instances but is to be carried out on a risk sensitive basis. Situations where this may be considered necessary include:

(a) Situations involving significant amounts of VFAs or where the amount of VFAs to be transferred does not make sense given the information known about the customer, especially one's source of wealth and source of funds;

(b) Situations where there are doubts as to the actual location of the customer due to discrepancies between the address provided by the customer and other information available to the VFA service provider (e.g. IP address, device geo location, use of cards issued by an institution not located in the customer's country of residence etc.);

(c) Situations where the occasional transaction or business relationship has connections to high risk jurisdictions known to have high levels of asset-generating crime and/or corruption, or otherwise known for the carrying out or conduct of cybercrime activity.

It is left to the subject person to determine how to obtain proof of control. This may be done for example through message signature or by having a small amount of VFAs transferred from the service provider's own address to that of the customer and returned back to the VFA service provider.

Multi-Signature Wallet – In situations where the customer states that the wallet is a multi-signature wallet or the subject person otherwise determines as much, the VFA service provider has to consider whether the different keys are all held by the customer or whether, in addition to the customer, there are other individuals or entities holding the said keys. Where it results that the different keys are held by two or more individuals or entities, these should all be considered as customers and be duly identified and verified as such. The reason for this is that the transaction would not actually be executed on behalf of a single customer but on behalf all those controlling the wallet.

Custodial Wallet – In situations where the address relates to a custodial wallet, the VFA service provider should consider the regulatory status of the custodian and the effect this may have on the ML/FT risk arising from the business relationship or occasional transaction. The use of unregulated custodial wallet providers or custodial wallet providers which, though regulated, are not subject to a sufficient level of oversight or are not subject to any oversight at all would lead to an increase in the ML/FT risk.

2.2.2 Business Relationship v Occasional Transaction

As a subject person, a VFA service provider has to carry out and apply CDD measures whenever it is to enter into a business relationship or carry out an occasional transaction. The obligations to be applied will therefore vary depending on the interaction between the VFA service provider and its customer.

Where for example the customer opens an account with the VFA service provider, the indications are that there is an intention on the part of the parties to extend their relationship over a period of time and therefore it would be considered that there is in place a business relationship. This entails that the CDD obligations would not be limited to the identification and verification of identity of the customer and, where applicable, of the beneficial owner but also to the need to establish the purpose and intended nature of the business relationship as well as carrying out on-going monitoring of the business relationship.

On the other hand, in the case of an occasional transaction, the CDD measures would be limited to the identification and verification of the customer and its beneficial owners where applicable. However, where the occasional transaction presents a high risk of ML/FT, the VFA service provider would be expected to apply EDD measures to mitigate the said risk. This may include obtaining source of wealth and source of funds information as set out in Section 2.2.3 hereunder.

It is important to note that an occasional transaction occurs whenever the VFA service provider carries out a one-off transaction on behalf of a customer outside of a business relationship, **independently of the amounts or values involved**. Moreover, in applying the risk-based approach to an occasional transaction, VFA service providers have to ensure that any CDD measure is carried out before the transaction is concluded and in a manner that the VFA service provider can always take action if the customer refuses to provide the requested information and/or documentation.

As regards the application of the Euro one thousand (€1,000) threshold as an indication of low ML/FT risk (mentioned in Section 2.2.), this is intended to find application within the context of a business relationship rather than an occasional transaction. As already highlighted, the application of the risk-based approach is fairly limited in the case of occasional transactions as in low risk cases there can be at most a delay of the verification of identity measures up until a transaction is executed, which in the context of VFA Service Providers is highly unlikely in view of the rapidity with which transactions are executed. However, the said threshold could be applied within the context of a business relationship, and subject persons can consider business relationships where transaction activity is below €1,000 to be low risk relationships, unless there are other factors that indicate otherwise. VFA Service Providers are to determine when a customer meets the Euro one thousand (€1,000) threshold by adopting either one of the following approaches:

(a) Considering the €1,000 transaction threshold to be met if the customer transfers Euro one thousand (€1,000) or the equivalent in any other FIAT

currency to the VFA service provider from the customer's own funds for the acquisition of VFAs over a ninety (90) day revolving period[5], independently of whether the said funds are actually used or left to the credit of the customer's account with the VFA service provider; or

(b) The customer transfers VFAs to the service provider, either in a single transaction or in multiple transactions, which VFAs are valued at Euro one thousand (€1,000) or more[6].

2.2.3 Purpose and Intended Nature of a Business Relationship

As set out in the Implementing Procedures – Part I, a subject person needs to understand the purpose or reason why a customer is seeking to form a business relationship with it as well as understand how the services and products offered by the subject person will be used in the context of the said relationship. Hence why, depending on the nature of the service or product offered, a VFA service provider is expected to obtain information as to reason/s why the customer requires its service or product, as well as how the customer will be making use of the same (e.g. information on the expected value and volume of transactions to be carried out by the customer as well as the main jurisdictions it will be transacting with when these are identifiable *a priori*). Moreover, the subject person is also expected to collect, on a risk-sensitive basis, source of wealth and source of funds information.

Source of wealth information relates to the activities that generated the customer's overall wealth (i.e. it is not about verifying what assets a customer has but rather on how the customer acquired them) whereas source of funds information relates to the activity that generated the funds to be used in one or more particular transactions. At the inception of a business relationship, a subject person would be expected to collect information on a customer's source of wealth and expected source of funds. Should any deviation from how the customer is expected to use the product or service provided be noted through on-going

5. . This entails that the VFA service provider has to consider whether the customer's overall transfers of FIAT currency in the previous ninety (90) days have reached the Euro one thousand (€1,000) threshold, with VFA service providers being able to make said determination either each time a customer effects a transfer to the VFA service provider or at the end of the day when such a transfer or transfers take place.
6. This entails that the VFA service provider has to consider all the transactions carried out by the customer involving a transfer of VFAs to the VFA service provider to determine the point in time when the amounts transferred are valued at Euro ten thousand (€1,000).

monitoring, the subject person would need to ask about the source of funds being used for the specific transaction that was deemed unusual. Thus, source of funds need not be established for each and every transaction but only for those transactions which fall outside the subject person's expectations and/or the customer's known transactional history.

The extent of information to be collected will vary on the basis of risk. In low risk situations it may be possible to do away with the collection of any such source of wealth information. However, with an increase in risk there has to be a corresponding increase in the information collected and, in high risk situations, the information collected would need to be verified on the basis of an independent and reliable sources, be it documentation provided by the customer or otherwise obtained by the subject person. In this context, the payment method used to fund one's account or transaction will also influence the degree of information and documentation to be requested. As already highlighted in Chapter 1, receiving payment from a credit or financial institution located in a reputable jurisdiction presents a lower risk of ML/FT compared to situations where payment is made through means that are less transparent. Thus, more information and/or documentation on source of funds will be required in the latter instance.

While establishing a customer's source of wealth and his source of funds are applicable requirements in the case of a business relationship, it should be borne in mind that 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, the VFA service provider 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.

In the case of payments effected by means of, or transactions involving, VFAs, the source of funds will consist in determining how these were obtained by the customer. In the event that the VFA service provider establishes and documents that the VFAs have been mined by the customer (e.g. retaining information obtained through the VFA's blockchain), the need to obtain additional information from the customer will be dependent on the amount or value involved. Where the amount is significant, the VFA service provider 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 customer's source of wealth information , i.e. the VFA service provider has to ask itself whether the customer could afford running the mining operation given his source of wealth.

On the other hand, if the VFAs have originated from alternative sources, the VFA service provider must request evidence of how the customer came to have possession of the said VFAs. By way of example, this could be done by asking the customer for evidence of any previous transactions effected by the customer. Thus, if the VFAs were obtained as pay-out from a mining pool, the VFA service provider would be expected to obtain evidence that the address from which the VFAs were received is controlled by a mining pool and that the customer had a connection with the said mining pool justifying the pay-out.

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

(a) Check the wallet addresses associated with the said payment or transaction for any adverse information in the public domain (e.g. OFAC blacklists); and

(b) Use, where available, DLT analytical tools to, *inter alia*, detect potentially fraudulent transactions and other suspicious activity (e.g. the VFAs were used on the darknet or in connection with a ransomware attack).

These checks should be carried out both with respect to the addresses from which VFAs are received as well as in respect of addresses to which VFAs are sent.

Any negative information is to be factored into the CRA and has to be considered by the VFA service provider to determine whether it is willing to proceed with the transaction or whether it should desist from doing so and file an STR with the FIAU. In determining whether to do so, VFA service providers should consider the transaction history of the VFAs concerned: for instance, how many transactions took place since the occurrence of the tainting event; with which addresses the VFA have transactional links, and the period of time involved until the VFA was to be transferred to the VFA service provider etc.

The measures referred to in (a) and (b) are to be applied on a risk-sensitive basis, bearing especially in mind the risks associated with FT. It is acknowledged that the DLT analytical tools at present available do not allow for data and/or information to be made available on every VFA that a VFA service provider may encounter or transact in. The absence of any such tool is to be factored into the subject person's risk understanding and assessment, with the subject person considering what alternative measures may be taken to address this lacuna and how these alternative measures can mitigate any corresponding ML/FT risks.

2.2.4 Inability to Complete CDD Measures

Situations may arise in which a customer is not willing to provide the VFA service provider with the necessary information or documentation even though the said service provider may have repeatedly solicited him to forward said information or documentation. In this case, in addition to keeping a record of all the attempts made:

(a) The VFA service provider is not to establish the business relationship with the customer or otherwise carry out the occasional transaction. In situations where the business relationship has been established, the VFA service provider is to terminate its business relationship with the customer.

(b) The VFA service provider is to consider whether there are any grounds giving rise to suspicion of ML/FT. The reluctance of the customer to provide CDD information or documentation on its own should not be automatically equated to a suspicion of ML/FT. The service provider has to consider all factors and information it has at its disposal, including for example the payment method used, the services requested or made use of and any transaction patterns, any information on the customer already held by the VFA service provider, including the jurisdiction of residence, and information which can be obtained through sources such as the internet etc. If there are grounds to suspect ML/FT, then the VFA service provider has to submit an STR to the FIAU.

(c) Where there are 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 service provider would have no reason rooted in the AML/CFT regime justifying the retention of any such funds.

Thus, where funds are to be remitted back, the VFA service provider has to:

i. Consider whether there is any other legal impediment to the remittance of the funds; and

ii. Remit the funds to the same source through the same channels used to receive the funds.

In the event that the VFA service provider is unable to remit the funds 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 service provider, it should submit an STR and suspend the remittance pending the FIAU expressing its opposition or otherwise to the execution of the said transaction.

In the circumstances described above, whenever a VFA service provider is remitting funds it is also, to the extent that this may be possible, indicate in the

script/instructions accompanying the funds that these are being remitted due to their inability to complete CDD.

It should also be borne in mind that this is applicable not only with respect to FIAT currencies but also when the assets held by the subject person consist in VFAs.

2.2.5 On-Going Monitoring

Subject persons who establish business relationships with their customer have on-going monitoring obligations consisting of the following:

(a) Ensuring that the documents, data or information held are kept up to date, i.e.:

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

ii. questioning 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 service provider's knowledge of the customer and the information in its possession is kept up to date. VFA service providers should determine on a risk sensitive basis whether any new information needs to be obtained or whether changes are so substantial as to require the carrying out of its CRA and/or its CDD afresh.

And

(b) Scrutinising the transactions undertaken throughout the course of that relationship to ensure that they are consistent with the VFA service provider's knowledge of the customer and the customer's business and risk profile. Where a VFA service provider 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, or the activity does not reflect a customer's usual transactional patterns), the VFA service provider has to question this unusual activity and, where necessary, establish what is the source of the funds used for the said activity.

To this end, VFA service providers should establish a risk-based transaction monitoring program in line with the requirements of Regulation 7 of the PMLFTR

and Chapter 4 of the Implementing Procedures – Part I. VFA service providers may be carrying out transactions on-chain and/or off-chain, and therefore the transaction monitoring program has to be applied to accordingly to ensure no transaction carried out by customers is ignored. Such transaction monitoring program is to:

(a) Include appropriate risk-based systems and controls to monitor the transactions of customers;

(b) Identify transactions that are considered to be unusual or suspicious; and

(c) 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 (a) above should as a minimum include the following elements:

- risk-based processes for recognising ML/FT typologies and transaction patterns indicating suspicious behaviour (for example, customers making large FIAT deposits, and then subsequently transferring the funds without acquiring any VFAs, the use of tumblers and mixers);
- 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;
- processes to assign alerts to customers identified as high risk or those conducting transactions indicating suspicious behaviour; and
- processes to link accounts held or controlled by the same customer.

What constitutes complex, unusual or large transactions or unusual patterns of transactions for the purposes of (c) above differs for each VFA service provider. 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 service provider'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.

Possible examples of situations that should be detected through on-going monitoring include situations where:

(a) The VFA service provider is informed by the customer that he has a monthly salary of EUR2,000 but the customer carries out multiple transactions of low value that add up to EUR50,000 a month.

(b) The VFA service provider is informed by the customer that he is a passive investor in VFAs and that the VFA service provider will only receive regular VFA transfers. Instead, the customer receives and sends significant amounts of VFAs at irregular intervals.

Depending on the outcome of their ongoing monitoring exercise, VFA service providers may have to take 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;
- consider whether updates to the CRA are warranted; and
- consider whether to file an STR with the FIAU.

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 service providers may wish to put in place to monitor transactions and identify higher risk transactions that may require enhanced monitoring, detailed analysis or reporting. VFA service providers are encouraged to consider the below factors to the extent applicable to the activities undertaken by particular VFA service providers.

Action	Minimum
Develop customer profiles and identify irregular and unusual activities	• identify customers whose predominant source of funds are derived from cash or cash-equivalent transactions, other VFA 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 exchanges in a manner expected of individuals (could indicate a front, shell and/or shelf companies) • identify non-profit organisations transacting through exchanges in a manner expected of individuals (this could indicate misappropriation of funds) • identify, where applicable, large purchases of VFAs • 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 movements of funds	• identify the customer undertaking multiple transactions concurrently of varying amounts and in different VFAs
Identify interactions with known mixers, the use of high-risk counterparties and transactions that use the darknet	• identify customers attempting to obfuscate the movement of funds • identify customers attempting to obfuscate the movement, source or destination of VFAs such as through the use of mixers/tumblers • identify customers who subsequently transact with higher risk counterparties such as illicit marketplaces • identify customers who are trying to obfuscate transactions with higher risk counterparties – for example, by transferring VFAs to a private wallet with links to other wallets flagged for illicit activities

As part of the VFA service provider's obligations under Section 2.5 hereunder, a VFA service provider has to carry out an annual review of its AML/CFT controls, policies, measures and procedures. Included within the said review would be the transaction monitoring program. Given the importance of the said program, it is imperative that it is tested regularly and that any shortcomings identified, even if these arise prior to the review period, are addressed as quickly as possible. Testing may take place through:

(a) **Back-Testing** Using sample data to test and refine the transaction monitoring program to ensure they are current and effective in targeting riskier transactions and behaviour.

(b) **Post-Implementation Testing** Checking already processed transactions to verify that the transaction monitoring program is functioning according to expectations and does not inadvertently compromise the conduct of transaction monitoring.

(c) **Data Integrity Checks** Ensure that the data being captured and transmitted to the transaction monitoring system/s is complete and accurate.

2.3 TRANSACTION RECORDS

Chapter 9 of the Implementing Procedures – Part I sets out the records that need to be retained by subject persons to ensure compliance with the record-keeping requirements arising from Regulation 13 of the PMLFTR. This includes having supporting evidence and records necessary to reconstruct all transactions carried out by that person in the course of a business relationship or any occasional transaction.

This entails that the necessary details have to be retained to allow tracing from where funds, including VFAs, were received and/or to where they were sent to. This would entail retaining the following information:

i. The customer's identification details;

ii. The name of any other party to the transaction;

iii. Details as to the bank account/wallet address used for the transfer of VFAs and/or FIAT currencies;

iv. In the case of custodial wallets, the name of the institution holding the same;

v. The value date and the date of the value transfer; and

vi. The type and value of the VFA involved.

VFA service providers are to note that even in situations where any information is easily available on a public ledger, they are still required to retain that information on file.

2.4 REPORTING OF ML/FT-RELATED ACTIVITY

As subject persons, VFA service providers are required to file an STR with the FIAU whenever they have any knowledge, suspicion or reasonable grounds to suspect that ML/FT is taking place. When there are grounds to submit an STR, this is to be submitted at the earliest possible but not later than 5 working days. In addition, it is to be noted that whenever the STR relates to a transaction that is still to take place, the said transaction can only be executed following one working day from the day when the STR is filed and no directions are received from the FIAU to further delay the said transaction. Where no such directions are received, it is left to the VFA service provider to determine if it wants to execute the transaction or otherwise.

The FIAU is aware that there may be instances in which it is impossible for a transaction to be put on hold (e.g. due to the use of particular smart contracts). This is considered to be a situation that is already catered for under Regulation 15(5) of the PMLFTR and therefore, the VFA service provider need not seek to delay the execution of the transaction but can proceed to allow the same to take place, subject to filing the STR immediately afterwards, i.e. within 24 hours, and setting out in the same STR the reasons why it was not possible to delay the execution of the transaction.

It is to be borne in mind that Regulation 15(3) does not limit the reporting obligation to situations where the person involved is a customer of the subject person. Thus, where prior to the establishment of a business relationship or the carrying out of an occasional transaction, the VFA service provider has knowledge, suspicion or reasonable grounds to suspect ML/FT, the VFA service provider has to desist from establishing the business relationship or carrying out the occasional transaction and file an STR with the FIAU.

It should be noted that anyone holding a licence to provide a VFA service under Maltese law is obliged to submit an STR with the FIAU where the same knows, suspects or has reasonable grounds to suspect ML/FT. However, given the nature of VFA services and the fragmented regulatory framework applicable to the said activities, it cannot be excluded that VFA service providers may have to submit an STR with other FIUs.

2.5 AML/CFT REVIEW

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 service provider, the FIAU considers that a review of a VFA service provider's measures, policies, controls and procedures should be carried out at least every eighteen (18) months once the VFA service provider has commenced its activities and that such a review should be carried out by a party which is external to the VFA service provider (as well as to the group which the VFA service provider 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 review 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 review is to serve as a systematic check of the VFA service provider's AML/CFT systems and controls and the end result should be a written report on whether:

- the VFA service provider's AML/CFT programme is fit for purpose and compliant with the obligations of the VFA service provider under the PMLA, the PMLFTR and the FIAU's Implementing Procedures;
- the AML/CFT systems and controls were adequate and effective throughout the review period; and
- any changes or enhancements required.

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

- review the VFA service provider's assessment of the ML/FT risks it is exposed to considering the service provider's size, business lines, customer base and geographic expose;
- assess compliance by the VFA service provider with the relevant AML/CFT laws, regulations and procedures, including by considering the adequacy of subject person's internal policies and procedures;
- test the implementation of, and compliance with, internal AML/CFT policies and procedures;
- test the identity verification methods adopted by the VFA service provider;

- test CDD and on-going monitoring processes to determine how effective they are with respect to risk mitigation, this should include a sample – test of transactions in all areas with emphasis on high-risk areas, products and services;
- test the audit trail and record-keeping capabilities of the VFA service provider;
- test the adequacy, accuracy and completeness of training programmes; and
- test the process for flagging unusual and/or suspicious activity, and the reporting process to escalate flagged activities to the MLRO.

The AML/CFT reviewer engaged by the VFA service provider should be proficient in the PMLFTR, the Implementing Procedures, and this Guidance, and should also possess a degree of technological expertise to allow an understanding of any technological means employed by the VFA service provider in the performance of its AML/CFT obligations. Where the AML/CFT reviewer and the Systems Auditor appointed by the VFA Service provider in terms of the MFSA's Rulebook for VFA Service provider are separate, and since it is likely that most VFA service provider will rely on technology to perform their AML/CFT obligations, it is advisable that the AML/CFT reviewer 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 review report should be addressed to the VFA service provider's senior management so they can decide what (if any) next steps are required. A copy of the review report, together with management's responses, shall be made available to the FIAU and relevant supervisory authorities upon request.

2.6 PERIODICAL REPORTS

The FIAU may require VFA service providers to reply to periodical questionnaires and/or to submit periodical reports in relation to the ML/FT risks they are exposed to and/or their set-up and/or their AML/CFT controls, policies, measures and procedures. These reports and questionnaires allow the FIAU to obtain a better understanding of the ML/FT risk that individual service providers present to be able to take a risk-based approach in carrying out AML/CFT supervision.

CHAPTER 3 – OFFERS OF VFAS TO THE PUBLIC

In terms of the PMLFTR, "the issue of virtual financial assets for offer to the public in or from Malta in terms of the Virtual Financial Assets Act" is deemed to constitute "relevant financial business". Thus, in all those instances where the VFA Act imposes a requirement for an issuer's whitepaper to be registered with the MFSA, the issuer is considered to be a subject person and has to ensure compliance with all the obligations arising from the PMLFTR. Even in situations where, for whatever reason, the issuer fails to comply with the whitepaper registration requirement, the issuer would still be expected to meet all of the AML/CFT obligations emanating from the PMLFTR.

VFA issuers are exposed to similar ML/FT risks as VFA service providers as they are also included within the VFA ecosystem. However, it is equally acknowledged that issuing VFAs presents its own particular characteristics, especially when it comes to the nature of the interaction with customers (i.e. VFA subscribers).

Thus, subject to what is stated hereunder, Chapter 2 is equally applicable to any issuer conducting a public offer of VFAs and the requirements arising therefrom are to be complied with also by anyone offering VFAs to the public.

3.1 RISK ASSESSMENT

An offer to the public has to be preceded by a BRA to determine what ML/FT risks can arise from the same, i.e. how it can be abused to facilitate ML or FT. This is to be carried out in line with what is set out in the Implementing Procedures – Part I but is to also take into account the peculiarities of the issue and how it is to be structured. By way of example, it would not be sufficient to take into consideration the jurisdictions targeted for the carrying out of the issue itself but also aspects like the absence of any capping per subscriber, allowing any one single subscriber to transfer an unlimited amount of funds, including VFAs, to the issuer.

It is possible that in the course of an offer, new and additional ML/FT risks may materialise which were not considered when the initial BRA was carried out. In such a situation, the BRA would have to be reviewed and updated. Reference may be made to the situations referred to in Chapter 3 of the Implementing Procedures – Part I; however, this without prejudice to the requirement for the BRA to be reviewed once every six months where the VFA offer to the public lasts in excess of six months.

In addition, there may arise situations where the issuer conducts additional issues of VFAs to the public, in which case it would be necessary for any existing BRA to be reviewed so as to ensure that it considers all ML/FT risks arising from the

additional issues. To the extent that may be necessary, the issuer is to update the BRA and ensure that the mitigating measures being applied are sufficient to address the identified risks. Where it results that existing measures are insufficient, the issuer has to adopt additional ones that provide for an effective mitigation of the said risks.

The outcome of the BRA is to assist the issuer to adopt the necessary ML/FT risk mitigating measures. However, the application of these measures to specific cases will depend on the outcome of the CRA to be carried with respect of each customer.

3.2 CUSTOMER DUE DILIGENCE

In so far as the issuer is concerned, the customer is whoever subscribes for the VFAs offered as part of the issue. It is in relation to any such person that the issuer is expected to apply CDD measures as outlined in the PMLFTR and the Implementing Procedures – Part I. Depending on the risk inherent in its dealings with any one customer, the issuer is able to determine the level of CDD measures to be applied. Thus, while in high risk instances the obligation is to apply EDD measures, in lower risk scenarios it is possible to be less intrusive and request or acquire less information from the customer. The ML/FT risk presented by a given customer is to be determined on the basis of the CRA.

The nature of the CDD measures applied, as well as the ability to vary the extent and timing thereof, are dependent on the nature of the interaction between the issuer and the customer. It is considered that the interaction between the two is somewhat limited in time, given that it is limited to the actual subscription and acquisition of VFAs forming part of the public offer and that the element of duration required to constitute a business relationship does not present itself. Thus, the acquisition of any such VFAs is considered to constitute an occasional transaction rather than a business relationship. On the other hand, if the issuer provides the customer with additional VFA services and there is regular engagement between the two, the two will be considered to have a business relationship and therefore the obligations associated with business relationships will be considered to be applicable.

It is important to note that unlike other situations, no threshold is applicable and therefore CDD measures have to be applied independently of any amount involved. As regards the ability to vary the timing of CDD measures, in the circumstances this is somewhat limited though it may be possible to delay the same until the completion of the transaction as long as the issuer retains control over its completion.

Given that an issuer is not considered to have any business relationships with its customers, it follows that it does not have any obligations with regards to the establishing the purpose and intended nature of the business relationship as set out in Section 2.2.3 nor does it have any obligations with regards to on-going monitoring as provided for under Section 2.2.5.

3.2.1 Source of Wealth and Source of Funds

The non-applicability of Section 2.2.3 does not entail that issuers may not need to establish the source of wealth of a given customer and the source of funds used in an occasional transaction. Where the risk of ML/FT within an occasional transaction is assessed to be high and as requiring the application of EDD, 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 the explanation provided makes sense within the context of a customer's background. 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. Any such determination is to be made as set out in Section 2.2.3.

3.3 AML/CFT REVIEW

Issuers are also required to carry out an AML/CFT review as set out in Section 2.5. However, the external and independent third party who is to carry out the said review is to be engaged prior to the actual commencement of the offer to the public. The review of the issuer's AML/CFT controls, policies and procedures is to be carries out as soon as the offer to the public is exhausted. In the event that an issue is composed of various pre-planned tranches, an AML/CFT review is to be carried out at the end of each tranche. A copy of any such review is to be forwarded to the FIAU as soon as it is completed but not later than three (3) months from the end of the offer to the public or of the tranche concerned.

CHAPTER 4 – THE VFA AGENT

Another activity regulated by the VFA Act and which is considered to constitute relevant financial business in terms of the PMLFTR is that of "a VFA agent carried out by a person or institution registered or required to be registered under the provisions of the Virtual Financial Assets Act". As with the rest of the VFA activities, anyone acting as a VFA agent is considered to be a subject person even though the particular individual or entity is not registered with the MFSA.

One has to remark that the nature of the activities carried out by a VFA agent is somewhat unlike that of the other activities considered as relevant financial business or relevant activity – in all other instances subject persons are either a party to customer transactions or they have visibility of the same as they facilitate the carrying out of the transaction. This is not the case with the VFA agent as its activities are more regulatory in nature, ensuring that prospective service providers and issuers are fit and proper persons, and in the case of issuers ensuring that they comply with their obligations at law, be they statutory or contractual.

In addition, a distinction has to be made between situations where the VFA Agent is offering its services to a prospective VFA service provider or to someone intending to carry out a VFA offering to the public. When it is acting in terms of Article 7 of the VFA Act, a VFA agent is deemed to have a business relationship with its customer as the appointment entails that the VFA agent will continue to follow the issuer until the project financed through the VFA offering is either completed or abandoned. Thus, it is deemed that there is the necessary element of duration required to constitute a business relationship.

On the other hand, no such element of duration presents itself when a VFA agent is acting pursuant to Article14 of the VFA Act as its interaction with the prospective service provider is limited to the licensing process, whatever its outcome may be. Thus, the said interaction is deemed an occasional transaction, independently of the amounts or values involved

All of the above will inevitably influence what is expected from the VFA agent in terms of complying with the AML/CFT obligations arising from the PMLFTR.

4.1 RISK ASSESSMENT

In terms of the PMLFTR, subject persons have to comply with AML/CFT obligations on a risk-sensitive basis. This implies that the subject person has to understand the risks to which it is exposed to due to the activities it is conducting, i.e. what vulnerabilities it has and how these can be exploited for ML/FT. Once these risks are understood, it will be possible for the subject person to adopt the

necessary ML/FT controls, measures, policies and procedures to mitigate the said risks. The application of these controls, measures, policies and procedures in specific cases will be dependent on the outcome of the CRA.

With regards to the BRA, there may be business models proposed by the customer that present a higher risk of ML/FT than is usual. This would be the case for example where:

- A proposal does not include safeguards against the use of proxies, unverifiable IP addresses or geographical location, disposable email addresses or mobile numbers nor have the necessary measures to detect ever changing devices used to conduct transactions;
- The VFA Issuer or service provider 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 without appropriate mitigating measures, thus encouraging their use for illicit activity (e.g.: XMR, DASH, ZEC etc.);
- To the extent visible to the VFA Agent, the underlying customers of the prospective VFA Issuer or service provider have a high ML/FT risk profile;
- The initial VFA offering is structured in a way that the sale is not capped per user, thus allowing for unlimited amounts of funds to be transferred from the same customer to the prospective VFA Issuer, or, even though capped, there are no controls in place to ensure that the capping is not somehow circumvented; and
- Where the AML/CFT program of the prospective VFA Issuer or service provider is not sufficiently robust (for example: (a) the VFA Issuer's or service provider'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 service provider does not have adequate mechanisms in place for account monitoring and reporting of suspicious transactions), such VFA Issuer or service provider is not willing to address such deficiencies.

More specifically when dealing with VFA Issuers, VFA Agents should consider that there have been a number of VFA offerings that were identified as fraud schemes, and are therefore expected to exercise extra caution. The BRA is to be reviewed, and if necessary updated, once every six months. However, it is possible that the

BRA may have to be so reviewed prior to the lapse of six months. The Implementing Procedures – Part I lay down a number of circumstances which are to lead to the review of the BRA, and these are equally applicable in the case of VFA Agents.

Where the BRA is updated, VFA Agents are to consider whether this translates in a requirement to also review the mitigating measures adopted and individual CRAs.

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 CRA:

- The lack of transparency that may surround the issue, including the rights of holders and how financing will be used;
- The possibility of having VFA offerings teams and promoters suddenly withdrawing from the project after the issue 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.

Just like the BRA, a CRA is not static and has to be reviewed from time to time. One of the circumstances which should lead to a review of the CRA is if the VFA Agent notices that a VFA issuer is not applying its AML/CFT controls, policies, measures and controls properly.

4.2 CUSTOMER DUE DILIGENCE

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 issuer or service provider. 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.

4.3 SOURCE OF WEALTH AND SOURCE OF FUNDS INFORMATION

The obligation to collect on a risk-sensitive basis source of wealth and source of funds information arises in the context of a business relationship. Thus, this would be the case when the VFA Agent is engaged by an Issuer. Thus, the VFA Agent is expected to obtain information, and where necessary documentation, on (a) the

source, i.e. the activities, that generated the overall wealth of the issuer; and (b) the expected source of funds to be used to finance any costs and expenses associated with the issue (e.g. company formation, acquiring any IT equipment, meeting regulatory expenses etc.).

In view of what is stated in Section 4.5 hereunder, this information will not be used to determine whether the transactions carried out correspond to the issuer's expected activities but rather they will provide the subject person with a sufficient understanding of whether the customer can afford to carry out the said activity and whether it makes sense for the customer to have that level of financial and economic resources. While recognised that issuers are usually intent on raising finance for their project through VFA offers to the public, it is also true that they must have some form of initial financing to meet the expenses associated with the offer to the public.

In the case of an occasional transaction, such as when the VFA Agent is servicing a prospective service provider, there is no obligation at law to collect any such information in each and every case. However, VFA Agents are to remember that the risk-based approach imposes on them an obligation to take mitigating measures to address any identified risk. Thus, where the main risk identified in an occasional transaction is related to the funds being used by the prospective applicant to finance its activities, the VFA Agent would still be expected to question the customer's source of wealth and source of funds, and obtain sufficient information and documentation on the same. This should be commensurate to the risk identified.

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 Service provider 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 Service provider 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.

To the extent that it may be possible for an issuer or a service provider to finance its activities using VFAs rather than FIAT currency, the VFA Agent would still be expected to collect source of funds information. In this case, it would be a case of establishing the activity that generated those VFAs, obtaining evidence of as much and determine if this makes sense in the context of the information known about the customer.

4.4 NATURE AND PURPOSE OF THE BUSINESS RELATIONSHIP

The VFA Agent is deemed by the PMLFTR to have a business relationship only when it is servicing an issuer. This would entail that the VFA Agent would have to establish the purpose and intended nature of the business relationship, i.e. why is the customer requesting the subject person's services. However, in this case the purpose and nature of the relationship is quite self-evident as the VFA Agent's service can only be used for a very specific purpose and its engagement is a regulatory requirement. Hence, there would be no need for any information to be obtained from the customer.

However, this does not mean that the subject person would not have to obtain information on other aspect of the business and risk profile of the customer (e.g. the customer's source of wealth and source of funds referred to above). Moreover, VFA Agents should also consider to what extent the intended purpose of the VFA offer correlates with the known line of business of the customer.

4.5 ON-GOING MONITORING OBLIGATIONS

On-going monitoring obligations arise once there is established a business relationship between the subject person and its customer. In the case of a VFA Agent, this can come into being only where it is offering its services to anyone carrying out an issue to the public, given that the issuer has to retain the VFA Agent's service until completion of the project financed through the offer of VFAs to the public. In any such case, the VFA Agent would have to ensure that document, data or information collected in carrying out its AML/CFT obligations is kept up to date.

However, unlike other subject persons, a VFA Agent does not have any on-going monitoring obligations vis-à-vis the transactions carried out by the issuer as it is not a party to these transactions nor is it involved therein. In addition, it is very likely that the VFA Agent would not even have visibility of the said transactions.

A question may arise as to what is to happen if an issuer that a VFA Agent is servicing determines to carry out a second VFA issue. In any such case, apart from ensuring that the documents, data and information collected in the first or previous issue is still valid, the VFA Agent is to revise its CRA to determine if the new VFA issue effects its initial risk considerations. In the event that there is an increase in risk or, though maintaining the same risk levels, the risk is arising from a different source, the subject person is to update both its CRA and the measures taken to address the new risks identified.

The same applies with regards to any information obtained by or made known to the VFA Agent that points at situations where funds are being allocated in a manner that does not reflect what is stipulated in a whitepaper or at situations involving irregularities in the development of the project that had to be funded through the offer of VFAs to the public. Any such information should lead the VFA Agent to revisit its CRA for the given customer.

4.6 THE AGENT'S REPORTING OBLIGATIONS

In terms of Regulation 15(3) of the PMLFTR, a VFA Agent has an obligation to file an STR, together with supporting information and documentation, whenever it "knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to funding of terrorism, or that a person may have been, is or may be connected with money laundering or the funding of terrorism". What this obligation entails is further explained in the PMLFTR and in the Implementing Procedures – Part I. In addition, Regulation 16(1) obliges subject persons, including VFA Agents, not to disclose that they have submitted an STR or that they may do so.

Under paragraph R1-3.2.6.2 of Chapter I of the Virtual Financial Assets Rulebook issued by the MFSA, a VFA Agent is also under an obligation to immediately inform the MFSA whenever it considers a customer, or a prospective customer, not to be a fit and proper person to hold a licence or conduct an offer to the public. In so doing, the VFA Agent has to explain, in as much detail as possible, the reasons why it does not consider such person to be fit and proper. This would include situations where the VFA Agent knows, suspects or has reasonable grounds to suspect that the (prospective) customer is involved in ML/FT.

The obligation arising from the Virtual Financial Assets Rulebook should not be considered to conflict with the non-disclosure obligation arising from Regulation 16(1). While it is acknowledged that any hint to the (prospective) customer as to the reasons why services are not to be offered is to be avoided, making reference to suspicions of ML/FT when notifying the MFSA as required in terms of the Rulebook would not be deemed to fall foul of Regulation 16(1) as long as the VFA Agent does not disclose the fact that an STR has been, is or will be filed with the FIAU. In addition, VFA Agents are reminded of the exception to the non-disclosure obligation set out in Regulation 16(2)(a) of the PMLFTR.

ANNEX 1 – VFA-RELATED RED FLAGS, TRENDS AND ML/FT CASE - STUDIES

1. RED FLAGS

Red flags are occurrences which highlight that something unusual is taking place but need not necessarily translate into a breach of regulatory or legal requirements. The following is a list of red flags intended to assist subject persons active in the VFA area to detect unusual transactions, activities or behaviour.

When they manifest themselves, the subject person would be expected to consider them and understand what is causing them. Depending on the nature of its cause, the subject person may need to reconsider its CRA, the nature, extent and timing of the mitigating measures applied as well as whether there is a need to file an STR with the FIAU.

The said list is not exhaustive, and each subject person should seek to develop its own list of red flags taking into account its own experience as to what are unusual practices within the industry and the behaviour exhibited by its customers.

1.1 CUSTOMER-RELATED RED FLAGS

- Customer shows considerable curiosity as to the service provider's AML/CFT policies, procedures, measures and controls, or shows interest in forming close relationships with employees, including through the giving of gifts etc.
- Customer (a) provides inconsistent, misleading or false information/documentation; or (b) refuses to provide any information/documentation and terminates relationship with the service provider when requested to provide information.
- Customer provides contact details that reflect, in whole or in part, contact details provided by an already existing customer.
- Customer makes statements about his involvement in illicit activities.
- Customer makes use of privacy coins or has a portfolio largely composed of such coins.
- Customer's IP address (a) appears to be connected to a VPN or other similar IP anonymizers; or (b) changes repeatedly; or (c) does not tally with other information held by the subject person as to the customer's location (e.g. residential address, payment institution used etc.).
- Customer makes use of encrypted or temporary email services.
- There is publicly available adverse information on the customer (e.g. association with a fraudulent VFA issue etc.).

- An existing customer has been the subject of a FIAU or LEA request for information.
- Customer opens more than one account for the same VFA without providing any reason for doing so.
- Customer is part of a complex structure that makes the determination of the beneficial owner more difficult.
- Customer is willing to pay higher than usual fees for the carrying out of a given transaction which do not reflect market conditions.
- The bank account or credit/debit card linked to the customer's account is changed often.

1.2 ACCOUNT and TRANSACTION-RELATED RED FLAGS

- Funds are deposited soon after registration and withdrawn again shortly afterwards without making use of any of the services and/or products provided by the service provider.
- Customer deposits funds or VFAs in an account but leaves the same dormant.
- Customer requires the processing of a transaction within a timeframe that is shorter than that provided for in the service provider's terms and conditions.
- Funds are received from or transferred to an address with direct or indirect links to darknet marketplaces, mixing services, wallets associated with illicit activities.
- Funds have been reported as stolen or otherwise reported to have been obtained illegally.
- Transactions are conducted in large volume/amounts or at a high velocity that is inconsistent with peer-group or customer-specific transaction patterns.
- Account is funded though funds held with institutions located in jurisdictions which are either unstable or considered to be high-risk.
- Transactions are carried out in a manner that is inconsistent with reasonable trading patterns/ strategies or at specific times and amounts not congruent with normal industry practices.

- The transaction's script suggests an illicit activity.
- The customer either makes repeated transactions between own accounts or off-chain transactions with other customers of the same subject person.

2. TRENDS AND CASE-STUDIES

The purpose of this section is to set out how VFAs may be exploited for illicit purposes. The vulnerabilities described in Chapter 1 render VFAs an attractive tool for criminals, be it as a means of payment, where VFAs would be the direct proceeds of crime, or are used as part of the laundering process to legitimize proceeds resulting from their criminal activities. The introduction and development of VFA ATMs and of VFA-backed debit cards, making it easier to acquire and use VFAs, have further increased the attraction that VFAs present for criminals.

2.1 VFAs as Proceeds of Crime – General Trends

The association between VFAs and the sale of illicit goods or services on the darknet is well documented. Starting off with the Silk Road case, there have been repeated instances where LEAs shut down marketplaces on darknet and simultaneously seize significant amounts of VFAs. By way of example, the recent shut down of the Wall Street Market by German authorities led to the confiscation of VFA in six-digit amounts while a joint operation between the Spanish *Guardia Civil* and the Austrian Federal Police against a drug trafficking operation in 2018 led to the seizure of EUR4.5 million in different VFAs, including BTC, IOTA and XML. Similarly, the closure of the Black Hand marketplace by French authorities led to the seizure of EUR25,000 in various VFAs.

VFAs are also a preferred payment method when it comes to ransomware attacks. A 2018 study, focusing on 35 different ransomware cases involving the use of BTC, puts the figure of BTC paid as ransom to BTC 22,967.54 over the period 2013 to mid-2017. The study also made the assumption that the hackers immediately cashed out the BTC collected, meaning that they made off with some USD12.8 million. EUROPOL's 2018 IOCTA had concluded that ransomware attacks were likely to continue to be a trend in cyber-crime in the coming years, a conclusion also confirmed in this year's edition of the said assessment.

The same report highlighted how the abuse of VFAs by criminal elements has led to VFA users and service providers becoming victims of cybercrimes themselves. Exchangers, mining services and other wallet holders are facing hacking attempts

as well as extortion of personal data and theft. Known figures suggest that hacks have led to the loss of more than USD 1.3 billion worth of VFAs.

Akin to the increase of attacks on VFA users and service providers, is the emerging trend in crypto-jacking to mine VFAs, especially BTC and XMR. It is not clear how prevalent is the crypto-jacking trend. While in 2018 EUROPOL had considered that it was possible that crypto-jacking would eventually overtake ransomware attacks, the 2019 IOCTA has highlighted a decline in known instances of crypto-jacking though this may also be due to the lack of reporting.

Scams remain an ever popular means how to defraud individuals and entities of their funds, including VFAs. In 2018, the Dutch and UK authorities managed to arrest the individuals behind a massive fraud scheme that had led to the loss of EUR 24 million in VFAs. Through typosquatting, where a well-known online VFA exchange was 'spoofed' – or recreated to imitate the genuine site – they managed to gain access to victims' BTC wallets, steal their funds and login details.

2.2 VFAs as a Laundering Tool - General Trends

The use of VFAs as a laundering tool can take a number of forms as evidenced by any number of cases. By way of example, in 2016 an operation by the Spanish National Police dismantled a criminal network specialised in the illegal distribution of pay-tv channels. It resulted that the proceeds were being used to finance the operations of six BTC mines which were also dismantled by the authorities. 78.3 BTC (worth a total of EUR 31,320 at the time) were also seized.

The conversion of illicit proceeds into VFAs seems to have become another staple of money laundering rings. A number of other operations carried out by the Spanish *Guardia Civil*, with the support of other LEAs, in the course of 2018 revealed how drug proceeds were being used to acquire BTC. The BTC were either converted into FIAT currency again, and then remitted to the traffickers in their country of origin, or sent to addresses associated with wallets controlled by the narcotics' organisation.

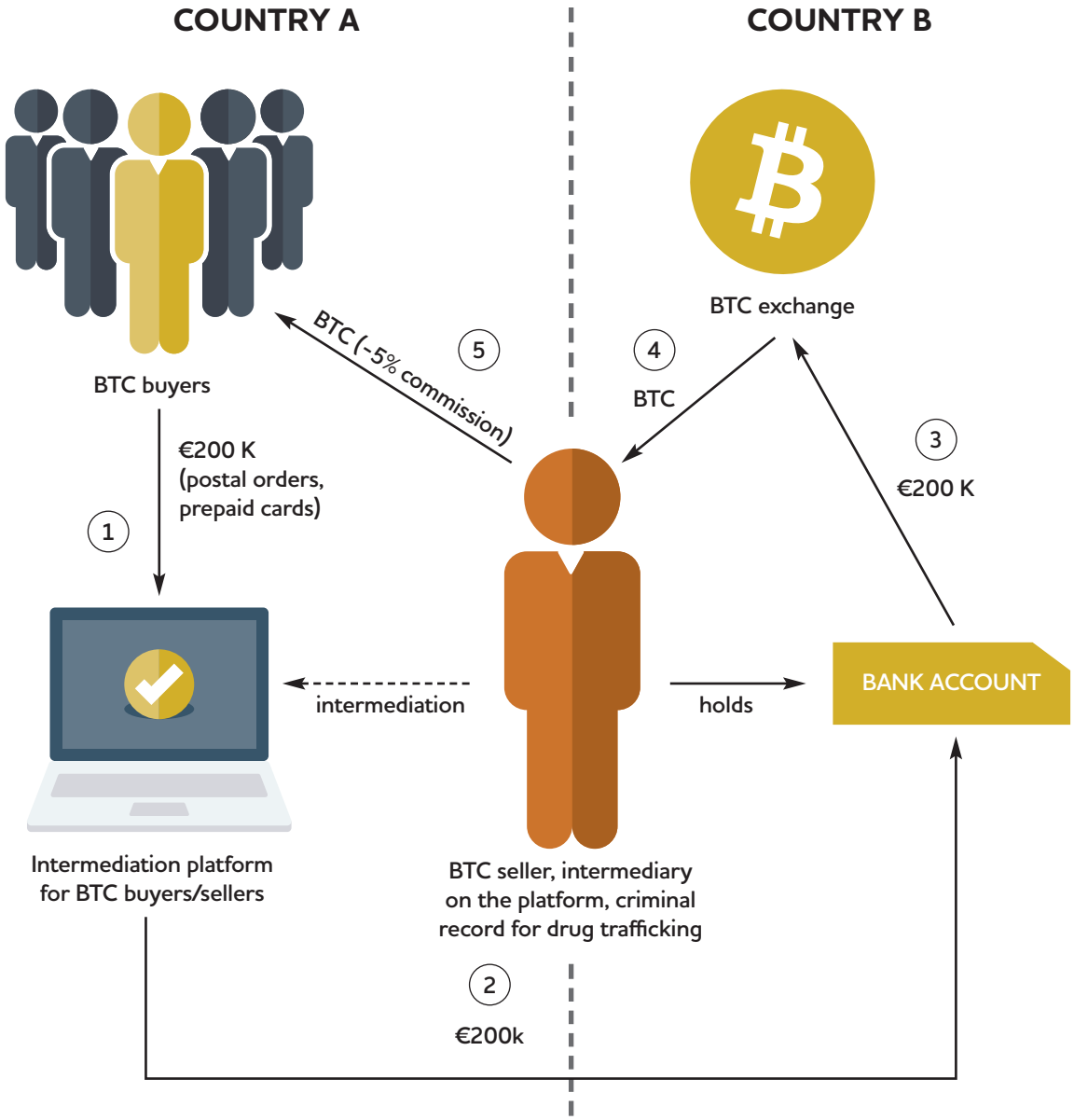
Cards linked to VFA wallets were also one of the means how the organisation behind a series of malware attacks against financial institutions were able to launder the funds derived from their illicit activities. Through pre-paid cards linked to VFA wallets, the organisation was able to acquire high-value luxury items.

The use of VFAs as a laundering tool need not be limited to the laundering of FIAT currency but may also involve the laundering of VFAs obtained through illicit activities. Witness to this was the taking down in 2019 of Bestmixer.io which

offered mixing services for BTC, bitcoin cash and litecoins. The service started in May 2018 and achieved a turnover of at least USD200 million (approx. BTC 27,000) in a year's time and guaranteed customers would remain anonymous. Investigations revealed that most of the VFAs mixed were derived from illegal activities.

2.3 VFAs and Money Laundering – Case Studies

CASE No. 1

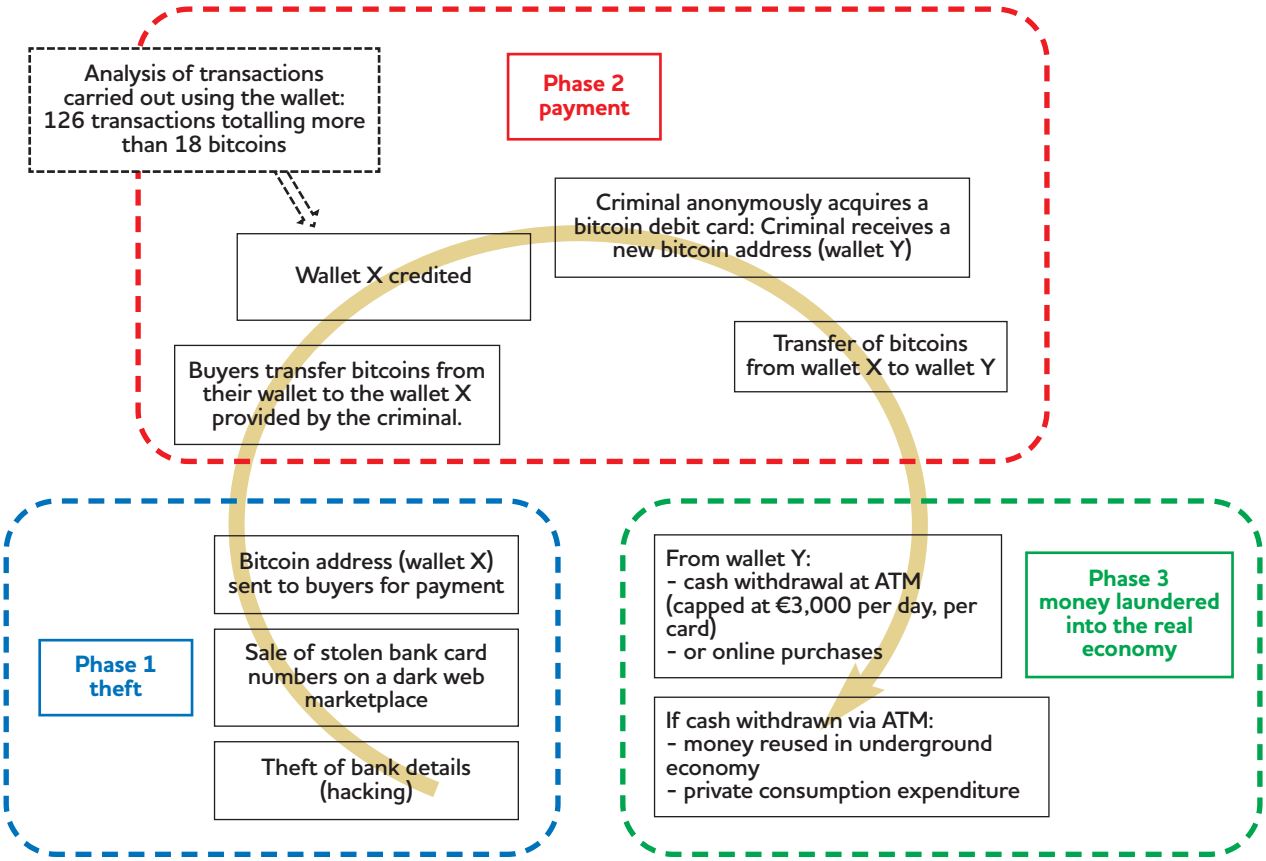


A number of individuals involved in drug trafficking sought to launder *circa* EUR 200,000 obtained from drug trafficking by acquiring BTC through an intermediation platform. The EUR 200, 000 were deposited with the platform using payment means like postal orders and pre-paid cards that provide a level of anonymity and/or do not allow for ease of traceability (1). These funds were then transferred to a BTC seller active on the said platform who was himself involved in drug trafficking (2), with the said funds being transferred to a bank account held by the BTC seller. Using these funds, the BTC seller acquired BTC through another platform (3) (4) and he then transferred the BTC to the BTC buyers less a 5% commission (5).

Once the BTC buyers acquired BTCs, they could (a) use them online to acquire goods and/or services; (b) sell the BTCs; or (c) convert the BTCs into FIAT currencies through the use crypto-debit cards.

(TRACFIN - *2015 Money Laundering and Terrorist Financing Risk Trends and Analysis*)

CASE No. 2



Phase 1 – Theft: An individual was illegally acquiring third party bank details through hacking, selling bank card numbers on the dark web. Buyers would be provided with a BTC address to which they were to send BTC as payment.

Phase 2 – Payment: Buyers would send BTC to the BTC address provided by the seller. The said individual then acquired a BTC debit card and links the same to a new BTC address to which he transferred all the BTCs acquired through the sale of the stolen bank card numbers.

Phase 3 – Integration: The individual then either used the BTCs to acquire services and/or products online, or withdraw them as cash through ATMs.

(TRACFIN – *2016 Money Laundering and Terrorist Financing Risk Trends and Analysis*)

CASE No. 3

An individual sold computer software and hardware online, with customers having the ability to pay either using FIAT currencies, or BTC or NXT. The same individual offered customers the possibility to download software for free, with some of the said software containing malware that allowed the individual to use the victim's computer power to mine BTC without the victim's knowledge or consent.

In a few weeks, the said individual managed to collect 50 BTC (*circa* EUR 160,000 at the time) from his mining activities which BTC he mingled with the BTC legitimately derived from his online sales. The BTC were held using a private wallet and were subsequently converted into FIAT currency through two exchange platforms. The said funds were then transferred to bank accounts held in jurisdictions other than the one where he resided.

(TRACFIN – *2017/2018 Money Laundering and Terrorist Financing Risk Trends and Analysis*)

CASE No. 4

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

CASE No. 5

An organised crime group engaged in 'crypto-cleansing'. To do so, they opened verified accounts at BTC 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 **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 BTC addresses to exchanges, using mixers/tumblers. Finally, BTC would be transferred from the exchanger to the local bank accounts opened by the 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.

2.4 INITIAL VFA OFFERINGS

Initial VFA Offerings or, as they are more commonly termed, 'ICOs' are vulnerable to being exploited by criminals in two main ways:

(a) They can be used to launder already held proceeds of crime - Proceeds of crime may be used to purchase VFAs, which can be sold on to other investors

and then converted into FIAT currency. The launderer can then justify the funds by stating that he or she has financed a project and has made a profit. Hence the importance of being able to establish, at the launch of the VFA launch, the origin of subscribers' funds.

(b) They can be a means how to defraud subscribers – Fraudulent VFA offerings can take place in a number of ways:

i. Issuers may make false statements to increase market interest in their VFA offering;

ii. False statements can also be part of a 'Pump-and-Dump' scheme, i.e. using the false representations to inflate the price of a VFA which is owned in significant quantities by the fraudster. While the fraudster will sell off his holdings at an inflated price, the subscribers will be left to absorb the loss once market prices adjust to normal levels.

iii. The issuer disappears with the funds collected through the issue after the issue is exhausted, without creating any underlying use or asset, resulting in the purchased tokens losing all value.

2.5 VFAs and the Funding of Terrorism

Terrorist and terrorist organisations seem to be less proficient in the use of VFAs and the related technologies to finance their activities. Known instances where VFAs were used as a means of terrorist financing are sporadic but not unheard of. Indeed, EUROPOL's TESAT for 2018 remarks how sympathisers of terrorist organisations are continuing to adopt and familiarise themselves with VFAs. Some known instances in which VFAs were linked to terrorist funding include the following:

i. In January 2015, it became known that an alleged ISIS cell had carried out fundraising by soliciting BTC donations. Prior to action by LEAs, a total of five BTC (*circa* USD 1,000 at the time) were received in donations.

ii. In June 2015, a terrorist organisation launched a social media campaign to raise funds for its activities. A year later, it added the possibility for donations to be made in BTC. It managed to receive a total of 0.929 BTC in donations (*circa* USD 540 at the time) in two separate transactions.

iii. In January 2017, the FIU of Indonesia reported that BTCs remitted from abroad had been used to finance the activities of domestic terrorist organisations.

iv. Towards the end of 2017, a self-described charity organisation started a social media campaign to raise funds for jihadist activities. Initially, donations were solicited in BTC and in one transaction it received 0.075 BTC, with the value thereof increasing from USD 685 to USD 803 in one day. The said organisation is still active, though it is now soliciting donations also through privacy coins.

3. 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 appear 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 distributing, storing and laundering the proceeds of a number of illicit activities, 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 anti-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.

FIAU
MALTA

FINANCIAL INTELLIGENCE ANALYSIS UNIT

IMPLEMENTING PROCEDURES

PART II

WWW.FIUMALTA.ORG