Implementing Procedures

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

PART II

CONSULTATION DOCUMENT

7 November 2024

REVISION OF THE IMPLEMENTING PROCEDURES – PART II ADDRESSED TO THE VIRTUAL FINANCIAL ASSETS SECTOR - CONSULTATION EXERCISE

INTRODUCTION

On 30 December 2024, a comprehensive EU-wide legislative framework for the provision of crypto-asset services is set to become applicable. This framework is composed of a series of legislative instruments that will replace national frameworks, including Malta's own Virtual Financial Assets Act. Complementing these instruments, the European Banking Authority issued sets of guidelines that will also become applicable on the aforementioned date.

As a result, the Financial Intelligence Analysis Unit (FIAU) is taking a number of steps to ensure that the domestic Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) regime reflects this new reality. These measures are described in further detail below.

CHANGES TO THE DOMESTIC AML/CFT FRAMEWORK APPLICABLE TO CASPS

On 30 July 2024, the FIAU had issued a consultation document on a series of proposed amendments to the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR). These amendments seek to align the local AML/CFT legislative framework with recent EU and local legislative developments in the crypto-assets sector, namely:

- The **MiCA Regulation** (Regulation (EU) 2023/1114) and the consequential amendments to **the Virtual Financial Assets Act** which came into force by virtue of Act XIV of 2024.
- The **recast of the Transfer of Funds Regulation** (Regulation (EU) 2023/1113).
- The amendments to the **4th AML Directive** (Directive (EU) 2015/849) as set out in Article 38 of the recast of the Transfer of Funds Regulation.

To complement the above, the FIAU is today issuing the present Consultation Document on the revision of the Implementing Procedures – Part II for the Crypto-Assets Sector. The proposed changes mainly seek to align these Implementing Procedures with the above-mentioned proposed amendments to the PMLFTR. They also reflect the revised EBA ML/FT Risk Factor Guidelines that were published on 16 January 2024.

Subject persons are to note that the feedback received in response to the consultation exercise on the amendments to the PMLFTR has also been taken into account while drafting these revisions to the Implementing Procedures – Part II. To a large extent, the said feedback focused on requesting further clarification regarding the correct implementation of revised or new

obligations resulting from the proposed changes. One major change introduced on the basis of the feedback received and reflected in the FIAU's proposed amendments to the PMLFTR is the exclusion of crypto-asset issuers as subject persons from scope of the AML/CFT regime, this with the exception of those that issue electronic money tokens.

Additionally, it is to be noted that the document had to be extensively restructured to cater for the proposed revisions. Therefore, while the Consultation Document is not published in track changes, the proposed revisions can be summarised as follows:

- The introduction of additional risk factors and corresponding measures specific to the crypto-assets sector as outlined in the revised EBA ML/FT Risk Factor Guidelines.
- The removal of Chapters 3 and 4 of the current Implementing Procedures – Part II which make reference to specific AML/CFT measures to be undertaken by VFA Issuers and VFA Agents respectively.
- The updating of terminology to align it with the terminology used under the MiCA Regulation, the amendments to the 4th AML Directive and the recast of the Transfer of Funds Regulation.
- A reference to the measures outlined in the amendments to the 4th AML Directive with respect to (i) cross-border correspondent relationships involving crypto-asset service providers; and (ii) transactions to or from self-hosted addresses.
- The inclusion of specific guidance on Multi-Party Computational Wallets.
- A reference to the requirements under the recast of the Transfer of Funds Regulation, as further explained in the EBA Travel Rule Guidelines published on 4 July 2024, both of which will become applicable as of 30 December 2024.
- The updating of Annex 1 to include new trends and case studies.

With reference to the EBA Travel Rule Guidelines, it is to be noted these are only mentioned sporadically throughout the document in view of the FIAU's intention to adopt them in their entirety and incorporate them as they are within the body of its legally binding guidance notes.

CONSULTATION EXERCISE

The consultation document is set out below. Interested parties may submit their feedback via e-mail on consultations@fiaumalta.org by not later than **Friday 29 November 2024**.

Table of Contents

ABBREVIATIONS

4AMLD	Directive (EU) 2015/849
AML	Anti-Money Laundering
ATM	Automated Teller Machine
BRA	Business Risk Assessment
BTC	Bitcoin
CASP	Crypto-Asset Service Provider
CDD	Customer Due Diligence
CFT	Countering the Funding of Terrorism
CRA	Customer Risk Assessment
DASH	Dash
DLT	Distributed Ledger Technology
EBA	European Banking Authority
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
MiCAR	Regulation (EU) 2023/1114
NRA	National Risk Assessment
PEP	Politically Exposed Person
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
TFR (recast)	Regulation (EU) 2023/1113

VPN	Virtual Private Network
XML	Lumen
XMR	Monero
ZEC	ZCash

1. INTRODUCTION

In 2018, the application of the PMLFTR was extended to cover activities that were, at the time, regulated by the Virtual Financial Assets Act. Thus, anyone conducting those activities was made subject to the AML/CFT framework.[1] With the introduction of the MiCAR, the amendments to the 4AMLD and the TFR (recast), the regulation of crypto-asset services is now harmonised at EU level. As a result, the PMLFTR were further amended in 2024 to bring it in line with these developments and with the amendments to the Virtual Financial Assets Act.[2]

The definition of "relevant financial business" found in Regulation 2(1) of the PMLFTR includes a reference to "the activity of a crypto-asset service provider". Thus, anyone who is defined as a crypto-asset service provider under Regulation 2(1) of the PMLFTR is considered a subject person in terms of the PMLFTR. The same applies to branches of any such service providers established in Malta but whose head offices are situated outside Malta, where these provide crypto-asset activities.

The definition of a "crypto-asset service provider" under the PMLFTR is equivalent to the definition provided for under point (15) of Article 3(1) of the MiCAR, when such service provider is performing one or more of the crypto-asset services defined in point (16) of Article 3(1) of the MiCAR. The definition excludes from its scope the provision of advice on crypto-assets as referred to in point 16(h) of Article 3(1), as well as the categories listed in Article 2(2) of the MiCAR. Equally within scope of the definition are those service providers that are licensed to provide either one or more of the services listed in the Second Schedule of the Virtual Financial Assets Act and that, as at 30 December 2024, are benefitting from the transitory period allowed for the granting of authorisation under the MiCAR.

Since crypto-assets and related activities have very specific characteristics, the present sector-specific Implementing Procedures provide tailored guidance to assist CASPs in ensuring compliance with the AML/CFT obligations arising from the PMLFTR. These sector specific Implementing Procedures are issued in terms of Regulation 17 of the PMLFTR.

This document is to be read in conjunction with the Implementing Procedures – Part I. 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 construed as a derogation from such obligations for CASPs. Moreover, in so far as the Implementing Procedures – Part I are not in conflict with these sector-

[1] This includes the obligations arising from the PMLA, PMLFTR and the Implementing Procedures Part I.

[2] By virtue of Act XIV of 2024, the Virtual Financial Assets Act was amended to align the local legislative framework with the MiCAR.

specific Implementing Procedures, they are still applicable to CASPs. In case of any such conflicts, these sector-specific Implementing Procedures are to prevail over the relevant sections of the Implementing Procedures – Part I.

CASPs are reminded that the Implementing Procedures Part I and Part II are also to be read together with the Travel Rule Guidelines issued by the European Banking Authority and setting out how CASPs are to meet their obligations under the TFR (recast). CASPs are to take into account the requirements of all three documents and ensure that the systems, controls, policies and procedures they put in place for AML/CFT purposes reflect and implement the same.

Other subject persons may be handling crypto-assets in the course of carrying out either relevant financial business or relevant activity even though not licensed as CASPs[3]. Any such subject person would not only be expected to abide by the Implementing Procedures – Part I and any other 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.

The revised version of the Implementing Procedures shall be applicable as of 30 December 2024.

[3] 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.

2. THE RISK-BASED APPROACH

To be read in conjunction with Chapter 3 of the Implementing Procedures – Part I.

2.1 What constitutes a Risk-Based Approach?

CASPs should be aware that the AML/CFT regulatory framework that applies to them as subject persons mandates the application of a risk-based approach. The risk-based approach requires subject persons to adopt measures, policies, controls, and procedures that are commensurate to the inherent risk of ML/FT that is identified. This is necessary to prevent and mitigate ML/FT risks from materialising.

This approach acknowledges that the ML/FT risks present in different scenarios are different for each unique sector as well as for different subject persons within the same sector. It is a dynamic assessment of the risks presented to a particular subject person, which goes contrary to a perspective tick-box approach in which the same measures are applied to similar scenarios. Thus, a risk-based approach envisages the application of checks that are proportionate to the assessed risk. High risk areas should be subjected to enhanced procedures, whilst simplified or reduced controls may be applied in areas of low risk.

A successful application of the risk-based approach can be achieved through the application of a risk management process in dealing with ML/FT. This includes the identification of risks, the undertaking of risk assessments at business and at customer level, and the implementation of systems to manage and mitigate the identified risks.

2.1.1 The Business and Customer-Related Risk Assessments

The cornerstone of the risk-based approach is the risk assessment which has to be carried out at different stages of a subject person's activities. To this effect, subject persons are required to carry out both a business risk assessment (BRA) as well as a customer risk assessment (CRA). The BRA is required to identify the ML/FT risks to which the CASP is exposed at the business level and has to include both a qualitative and a quantitative analysis of risk. On the other hand, the scope of the CRA is to determine the ML/FT risks inherent in a given business relationship or occasional transaction. While the BRA will allow the CASP to identify what kind of mitigating measures it needs to adopt, the CRA will allow the CASP 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.

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.

2.1.2 The Risk Areas

The Implementing Procedures—Part I set out general risk factors that all subject persons are to consider when drawing up the BRA and CRA, including CASPs. 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 jurisdiction. Risk factors are divided into the following risk areas:

- Product, Service and Transaction risk
- Customer risk
- Geographical risk
- Delivery Channel/Interface risk

However, in addition to the risk factors outlined in the Implementing Procedures – Part I, CASPs have to also consider additional risk factors mentioned in the present document. These risk factors take into account the specific features of their business model and the technology used as part of their business, allowing them to instantly transfer crypto-assets worldwide and onboard customers in different jurisdictions.

These risk factors are explained in further detail in Section 2.2.1 of this document.

2.1.3 The Risk Assessment as a Dynamic Tool

As mentioned above, a practical risk assessment must be dynamic, and subject persons must ensure that they revise the BRA when there are significant developments within the sector in which they operate. Any such changes may affect the risk a subject person is exposed to at business and at customer level. This is more relevant in the case of CASPs, which operate in an ever-growing sector and are constantly exposed to new ML/FT risks due to the sector's rapid development. Identifying these changes through a revision of the risk assessment allows the subject person to ensure that its measures, policies, controls and procedures are robust enough to cater for these changes.

CASPs are to review and, where necessary, update their BRA every six months 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 CASP would need to review its BRA and consider whether any updates are necessary. Such

an exercise is to be carried out prior to the change taking place where the said change is triggered through the CASP's own actions. It is also important for subject persons, including CASPs to always take into consideration any supranational, national or sectoral risk assessments that may be available when conducting and revising their own specific risk assessment.

On the other hand, the customer-specific risk assessment has to be revised when the business relationship entertained with the customer undergoes changes, whether these are manifested at the initial stages of a business relationship or otherwise. It is important that the subject person monitors the activity of the customer to ensure that it is in line with the customer's profile. Any significant changes in the customer's pattern of activity must be analysed to determine whether an update of the customer's profile is necessary. Where any such update becomes necessary, it is also very likely that the CDD measures being applied to the said relationship have to be re-considered and recalibrated to reflect the change in ML/FT risk. The level of monitoring should be commensurate to the risk posed by the particular customer, but systems should also be in place to detect emerging risks.

2.2 Application of the Risk-Based Approach in the Crypto-Asset Sector

2.2.1 ML/FT Risk Factors

This section lays down certain risk factors that are specific to the crypto-asset sector. As previously mentioned, when carrying out their BRA and CRAs, CASPs are to consider these risk factors in conjunction with the general risk factors found in Chapter 3 of the Implementing Procedures Part 1. Additionally, CASPs are to also take into account the EBA Risk Factor Guidelines which also include risk factors applicable to the crypto-asset sector.

i. Product, Service and Transaction Risk

When it comes to the consideration of the product/service/transaction risk, it is expected that the BRA of a subject person involved in crypto-asset activities will take into account the particular nature of crypto-assets as well as the underlying and associated technologies that can impact the ML/FT risk arising therefrom. Because of determinate characteristics, crypto-assets are often associated with illicit activities and ML as well as providing an additional means for FT. The characteristics and factors mentioned below should be taken into account by the CASP when determining the level of risk associated with the products and services that it offers and/or the transactions it facilitates.

Anonymity associated with Crypto-Assets

Crypto-assets are often described as being anonymous and allowing for transactions to take place anonymously. However, it has to be remarked that different crypto-assets will present different levels of anonymity. For instance, BTC is often described as being a pseudo-anonymous crypto-asset 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.

CASPs are therefore to take into consideration the increased risk of ML/FT posed by products and services linked to crypto-assets that provide a higher degree of anonymity. A case in point would be privacy coins, i.e. crypto-assets that have features intended to enhance the pseudo-anonymity usually associated with crypto-assets. These would include crypto-assets like XMR, ZEC and DASH. Some of these crypto-assets 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. Transacting in such crypto-assets would increase the risk of ML/FT which the CASP 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].

Moreover, 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 or decrease the anonymity and/or inability to trace transactions associated with privacy coins.

In addition, a number of technological means can further obfuscate the traceability of crypto-asset transactions. These would include the use of coin mixing or tumbling services.

Immediacy and Irrevocability of Crypto-Asset Transactions

Crypto-asset transactions can be very fast, with the speed varying depending on the crypto-asset being used. Moreover, crypto-assets 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 crypto-assets.

Crypto-asset transactions are also irrevocable, i.e. once crypto-assets 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 crypto-assets held in an address

[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.

associated with a self-hosted wallet given that no identity is associated therewith.

Decentralisation

Crypto-assets 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 crypto-asset 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 in reality the need for a third-party intermediary when crypto-assets are to be transferred from one address to another.

Sector Development

Rapid development in the crypto-asset sector naturally leads to new technologies and business practices offered by CASPs to their customers. A significant risk factor in this regard is whether these new business practices, such as new delivery channels for crypto-asset payments and new technologies, are susceptible to misuse for illicit gains such as ML/FT. CASPs must consider whether these new technologies can be reliably assessed for the level of ML/FT risk they pose. If the CASP cannot carry out such an assessment, it would follow that the CASP is significantly increasing the chance that it may be misused for ML/FT.

Type of Transactions allowed by the Product offered by the CASP

Given the nature of the transactions carried out by CASPs through their products, subject persons have to consider who their customers are making transactions with when drawing up their BRA. The risk of ML/FT is affected by the type of third-party accounts the CASPs' customers are allowed to transact with. Products allowing customers to transact with any of the following are considered to present a higher risk of ML/FT:

- Self-hosted addresses;
- Crypto-asset accounts or distributed ledger addresses managed by a provider of crypto-assets services that is not regulated within the EEA and is not subject to an equivalent regulatory or supervisory framework as that that within the EEA;
- A peer-to-peer cryptocurrency exchange platform or another type of decentralised or distributed crypto-assets application, which is not controlled or influenced by a legal or natural person (often referred to as 'decentralised finance' (DeFi));
- Hardware used to exchange crypto-assets to official currencies or vice versa (such as crypto-ATMs), involving the use of cash or electronic money benefitting from CDD exemptions under Article 12 of the 4AMLD and Article 7A of the PMLFTR, or otherwise not falling within an EEA regulatory and supervisory regime.

On the other hand, products allowing customers to transact with any of the following would present a lower risk of ML/FT:

- Crypto-asset accounts or distributed ledger addresses in the customer's name held by a CASP that is regulated under MiCAR.
- A crypto-asset account or distributed ledger address in the customer's name, that is held by a provider of crypto-assets services which is regulated in a jurisdiction outside the EEA but that is subject to a regulatory and AML/CFT framework as robust as that under the 4AMLD.
- Funds deriving from a bank account in the customer's name at a credit institution that is regulated within the EU or that is otherwise subject to a regulatory framework outside the EU that is equally robust.

In addition to the above, CASPs are to consider the increased risk of ML/FT posed by products which allow for payments from third parties that are not associated with the product offered by the CASP, where these have not been identified and verified upfront. In addition, the CRA should consider whether these payments have any apparent economic rationale.

Volume or Value of Transactions

A factor which may increase or mitigate the risk of ML/FT for CASPs is whether the product offered by CASPs has any restrictions on the volume or value of transactions carried out. Should a CASP provide products with reduced functionality, such as low volumes or transaction values, this would reduce the risk of ML/FT. On the other hand, should there not be an upfront restriction, then this would expose the CASP to a higher risk of ML/FT.

Nested Crypto Exchanges

Nested crypto exchanges are similar to the concept of correspondent banking relationships in traditional banking. In the crypto-asset sector, a nested crypto exchange offers crypto-trading services to its users through an account held by the nested exchange with a CASP. This model enables the nested exchange to market crypto-asset services without facilitating direct trading itself. Typically, a nested crypto exchange is characterised by a weak or inexistent AML/CFT control framework, therefore exposing it to exploitation by criminals seeking to launder their funds or to otherwise conduct fraudulent activities. In the absence of adequate controls performed by the nested exchange over its users, the wholesale CASP facilitating such nested services remains exposed to an increased ML/FT risk. When drawing up a BRA, CASPs should therefore consider their exposure to nested accounts and the AML/CFT controls that such nested crypto exchanges have over their client base. In this regard, CASPs may refer to the specific risk mitigating measures for correspondent relationships that are outlined in Section 3.4 of this document.

Results provided by Advanced Analytical Tools

The results of an ML/FT risk analysis run by advanced analytics tools on the CASP's product that indicate a higher risk of ML/FT is to be considered in the BRA. In this regard, CASPs need to bear in mind that (a) they will be exposed to a higher risk of ML/FT where they provide services that allow the processing of transactions in crypto-assets not covered by the analytical tool/s used by the specific CASP; and (b) the results of any such analysis do not constitute the only source of information that the CASP is to take into account, with any such analysis to be complemented by the CASP's own experience and information obtained through other sources.

Type of Payment Channels or Systems used by the CASP

Payment channels or systems used by CASPs reduce the risk of ML/FT when these are limited to closed-looped systems or systems that facilitate micro-payments, government-to-person, or person-to-government payments. The risk is reduced because of the limited features of such channels or systems. Similarly, products that are available to a limited or defined group of customers such as employees of a company also pose a reduced risk of ML/FT.

ii. Customer Risk

When it comes to the CRA, the customer risk factors need to also include a consideration of the nature of the customer and the customer's behaviour. A good understanding of these two categories of risk factors is essential for a complete CRA. CASPs must know who their customers are, what corporate vehicles are being used (if any), and how they behave when using the CASPs' services in order to properly identify any ML/FT risks and how these can be mitigated.

Factors linked to the nature of the customer that are indicative of an increased risk of ML/FT include the following:

- A non-profit organisation linked to or sympathising with extremist propaganda or terrorist activities, or other criminal activities, including ML/FT or corruption.
- An undertaking which is a shell institution as defined in Regulation 2(1) of the PMLFTR or another type of shell company.
- A company that has been recently established and is suddenly processing large volumes of transactions.
- A legally registered entity that is suddenly making large volumes of transactions after a period of inactivity following its establishment.
- A person or undertaking that is using IP addresses associated with a darknet or software allowing for anonymous communication, such as encrypted emails, anonymous or temporary

email services and VPNs.

- A person who is not likely to be a typical customer of a CASP, or displays a lack of knowledge of crypto-assets or the related technology, but nevertheless chooses to make frequent or high-value transactions. A person displaying such characteristics can be indicative of a situation where the customer is being used as a money mule.

An assessment of the customer's behaviour may also indicate an increased the risk of ML/FT in several situations. Behaviours indicative of an increased risk of ML/FT include situations where the customer:

- Tries to open multiple crypto-asset accounts with the CASP with no apparent economic rationale or business purpose.
- Uses an IP address or mobile device that is either linked to multiple customers without any apparent economic reason or that is known to be linked to potentially illegal or criminal activities. This may also include situations where the customer's crypto-asset account is accessed from multiple IP addresses without any evident link to the customer.
- Provides inconsistent information including information that is required to accompany the transfer of crypto-assets in accordance with the TFR (recast), as well as information concerning the habitual residence, business activities, source of wealth and funds of the customer.
- Is using an address, a location or an IP address linked to crypto-asset accounts held with the same CASP and registered to different users.
- Frequently changes its personal information or its payment instruments without obvious reason.
- Frequently receives or transfers small amounts of crypto-assets from or to self-hosted addresses that may be indicative of attempts to circumvent thresholds set by the CASP.
- Indicates that the purpose of the crypto-account is to receive investors' contributions that are intended to be invested in an initial public offering of tokens or in a crypto-asset or product that offers a disproportionately high return and is based in a high-risk jurisdiction or is associated with high fraud-related indications, or which is not supported by a white paper required under the MiCAR. This could be indicative of a customer who is trying to conduct investor fraud.
- Displays behaviour or transaction patterns which are not in line with that expected from the type of customer or the risk category to which it belongs or are unexpected based on the

information the customer has provided to the CASP, either at the start or throughout the business relationship.

- Displays unusual patterns of transactions to and from distributed ledger addresses or crypto-asset accounts in multiple jurisdictions without any business or lawful purpose.
- When exchanging crypto-assets to official currencies and vice versa, the customer:
    - uses multiple bank or payment accounts, credit cards or prepaid cards to fund the crypto-assets account;
    - uses a bank or payment account, credit card in the name of a different person than the customer without having evident links to that person;
    - uses a bank or payment account located in a jurisdiction, which is inconsistent with the customer's given address or location;
    - uses multiple providers of payment services;
    - repeatedly requests an exchange of crypto-assets to or from cash or anonymous electronic money;
    - uses protocols that connect two blockchains, to exchange crypto-assets to other crypto-assets on a different network, such as Monero, Zcash or similar crypto-assets;
    - uses Crypto-ATMs in different locations to repeatedly transfer funds to a bank account;
    - transfers crypto-assets that are held with the CASP to a self-hosted address immediately after depositing them or exchanging them for different crypto-assets.
- Is investing or exchanging crypto-assets, which it has borrowed via a peer-to-peer or other lending platform that does not fall within the scope of the MiCAR or under any other relevant regulatory framework within or outside the EEA and, which is notably a decentralised or distributed application with no legal or natural person with control or influence over it.
- Directly or indirectly receives or sends crypto-assets associated with the darknet or that result from illegal activities.
- Appears to exploit technological glitches or failures to its advantage.
- Explains that the crypto-assets transferred to the CASP have been obtained through mining or staking rewards, with these not appearing to be proportionate to the crypto-assets generated through such activities.

- Repeatedly receives crypto-assets from or sends crypto-assets to:
    - a crypto-asset account through an intermediary crypto-asset service provider that is not subject to the MiCAR or to any other relevant regulatory framework within or outside the EEA and is not subject to an AML/CFT framework as robust as that under the 4AMLD;
    - multiple self-hosted addresses or multiple crypto-asset accounts held by the same or different CASPs without an apparent economic rationale for it;
    - a newly created or previously inactive crypto-asset account or a distributed ledger address held by a third party;
    - self-hosted addresses on decentralised platforms, which involve the use of mixers, tumblers and other privacy-enhancing technologies that may obfuscate the financial history associated with the distributed ledger address and the source of funds for the transaction, therefore undermining the CASP's ability to know its customers and implement effective AML/CFT systems and controls;
    - a crypto-asset account shortly after being onboarded by the CASP, which is then followed by a withdrawal or a transfer from such an account in a short period of time without an apparent economic rationale for it;
    - a crypto-asset account by splitting the transactions into multiple transactions which are sent to multiple distributed ledger addresses by using smurfing techniques.

On the other hand, the following are factors that may contribute to a reduced customer risk. These include when the customer:

- Has complied with the information requirements provided for under the TFR (recast) during previous transactions in crypto-assets.
- The customer's previous transactions in crypto-assets have not given rise to suspicion and were in line with the risk profile.
- Requests an exchange of funds to or from an official currency to the source of the original destination of funds or the customer's own bank account in a low risk jurisdiction.
- Requests an exchange and either the source or destination of the crypto-asset relates to:
    - low value payments for goods and services to/from a crypto-asset account;
    - a distributed ledger address on which there is no adverse information available; or
    - the customer's own crypto-asset account or a distributed ledger address hosted

either by a CASP regulated under the MiCAR or by a provider of crypto-asset services subject to a regulatory, supervisory and AML/CFT framework outside the EU that is equivalent to that provided for under the MiCAR and the 4AMLD, and that has been whitelisted or otherwise determined by the CASP as low risk.

- the customer transfers funds between two CASPs which are regulated under the MiCAR or between a CASP and another service provider subject to a regulatory, supervisory and AML/CFT framework equivalent to that provided for under the MiCAR and the 4AMLD.

iii. Geographical Risk

This refers to the risk that arises from connections with one or more geographical areas. The jurisdictions associated with the services provided by a CASP are a key aspect to be considered in the business and customer risk assessments. The jurisdictions to be taken into consideration for this purpose are those (a) where the customer or its beneficial owners are based, have their main place of business or where the activity generating their wealth is carried out, and the jurisdictions with which the customer has especially strong trading or financial connections; or (b) with which the customer or its beneficial owner have relevant personal links (e.g. residence). If these jurisdictions pose a higher risk of ML/FT or their AML/CFT frameworks are deemed to be non-reputable, there is a higher risk that funds connected to the relationship may be tainted.

Chapters 3 and 8 of the Implementing Procedures Part I provide detailed guidance on the factors that are to be taken into consideration when assessing geographical risk. Additionally, the factors listed below provide further sector specific examples of geographical connections presenting a higher risk of ML/FT:

- The customer resides or is established in jurisdictions known for cybercrime activities. Where this is the case, there is a higher probability that any crypto-assets already held and used by the customer in transactions involving the subject person may have derived from criminal activities such as ransomware attacks.
- The customer's funds that are exchanged to crypto-assets are derived from personal or business relationships involving jurisdictions associated with higher ML/FT risk.
- The originating or the beneficiary crypto-asset account or distributed ledger address is linked to a jurisdiction that is either (i) subject to a high ML/FT risk; (ii) known to be linked to terrorist activity; or (ii) subject to restrictive measures or targeted financial sanctions.
- The business relationship is established through a CASP or a crypto-ATM located in a jurisdiction associated with high levels of ML/FT.
- The customer is involved, either directly or indirectly, in crypto-asset mining operations that

take place in a high-risk jurisdiction or in a jurisdiction that is subject to restrictive measures or targeted financial sanctions.

On the other hand, a lower risk of ML/FT would be presented if the transfer of crypto-assets originates from or is sent to a crypto-asset account or distributed ledger address which is hosted by a CASP regulated under the MiCAR and in a jurisdiction with low levels of ML/FT.

iv. Delivery Channel/Interface Risk

The delivery channel, or interface risk, is the risk arising from the distribution channels used to facilitate the service provided to the customer and the communication lines used by the subject person when interacting with the customer.

Given the digital nature of the crypto-asset sector, the use of remote customer onboarding measures is expected to be high, if not the norm. The interface risk is prevalent in the crypto-asset sector also due to 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, including those in relation to non face-to-face customer onboarding as stipulated in Chapter 4 of the Implementing Procedures - Part I.[5]

The following are interface risk factors specific to the crypto-asset sector which may increase the CASP's ML/FT risk exposure:

- The business relationship is established between the CASP and the customer through an intermediary service provider which is not regulated under the MiCAR or under an equally robust regulatory and supervisory framework.
- The identification and verification of the customer is outsourced to another service provider located in a high-risk jurisdiction.

On the other hand, when CASPs rely on third parties to carry out CDD measures, the risk of ML/FT may be reduced should the third party be located within the EU.

Additionally, the following risk factors linked to specific delivery channels in the crypto-asset sector may also be indicative of a higher risk of ML/FT:

- The use of crypto-ATMs to establish a business relationship. Such use would present a higher risk due to the use of untraceable cash that may be exchanged legitimately for crypto-

[5] Section 4.3.1.2 of the Implementing Procedures – Part I

assets within seconds. Considering the high incidence of cash in the criminal world, crypto-ATMs may provide a useful channel through which any such proceeds of crime are introduced into the financial system. The same can be said where withdrawals are affected through these ATMs, especially if their operators are subject to weak regulatory or supervisory oversight. It would not be easy to conduct the necessary CDD measures in such scenarios.

- Like crypto-ATMs, the funding of customer accounts is also a risk factor that CASPs should consider. The absence of restrictions on the funding instrument such as the unrestricted use of cash, cheques, pre-paid cards, crypto-backed debit cards and electronic money products may lead to an increased risk of ML/FT.

- New distribution channels or new technology used to distribute crypto-assets that have not yet been fully tested or that present an increased level of ML/FT risk.

To better understand the ML/FT risks associated with crypto-assets, subject persons can also refer to a number of publications including Guidance Documents issued by the FATF[6] and criminal activity assessments carried out by EUROPOL[7]. A number of reputable service providers active in the crypto-asset area also issue publications that can further assist subject persons in deepening their understanding of ML/FT risks associated with crypto-assets. 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.

In addition to the risk factors contained in this document, a series of red flags are also 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 CASP 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.

[6] Crypto-asset 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).

[7] EUROPOL publishes periodical reports that can shed light on current criminal trends and how these involve crypto-assets. These include the *Internet Organised Crime Threat Assessment* and the *Terrorist Situation and Trend Report*.

3. CUSTOMER DUE DILIGENCE

To be read in conjunction with Chapter 4 of the Implementing Procedures – Part I.

3.1 The CDD Measures

The BRA and the CRA are 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 CASP 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. CASPs 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 CASP 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 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 why the mitigating measures applied are considered sufficiently robust to address the identified level and nature of ML/FT risk.

3.2 Business Relationship v. Occasional Transaction

As a subject person, a CASP 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 CASP and its customer.

Where for example the customer opens an account with the CASP, 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 CASP would be expected to apply EDD measures to mitigate the said risk. This may include obtaining source of wealth and source of funds information.

It is important to note that an occasional transaction occurs whenever the CASP 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, CASPs have to ensure that any CDD measure is carried out before the transaction is concluded and in a manner that the CASP can always take action if the customer refuses to provide the requested information and/or documentation.

3.3 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 CASP 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 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 source, 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. Receiving payments 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 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 application 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 CASP 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, crypto-assets, the source of funds will consist in determining how these were obtained by the customer. In the event that the CASP establishes and documents that the crypto-assets have been mined by the customer (e.g. retaining information obtained through the crypto-asset'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 CASP will be expected to substantiate its determination with documentation on the mining operation that led to the creation of the crypto-assets (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 CASP has to ask itself whether the customer could afford running the mining operation given his source of wealth.

On the other hand, if the crypto-assets have originated from alternative sources, the CASP must request evidence of how the customer came to have possession of the said crypto-assets. 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 crypto-assets were obtained as pay-out from a mining pool, the CASP would be expected to obtain evidence that the address from which the crypto-assets 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 crypto-assets, a CASP 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 crypto-assets 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 crypto-assets are received as well as in respect of addresses to which crypto-assets are sent.

Any negative information is to be factored into the CRA and has to be considered by the CASP to determine whether it is willing to proceed with the transaction or whether it should desist from doing so and file a STR with the FIAU. In determining whether to do so, CASPs should consider the transaction history of the crypto-assets concerned: for instance, how many transactions took place since the occurrence of the tainting event; with which addresses the crypto-assets have transactional links, and the period of time involved until the crypto-asset was to be transferred to the CASP 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 may take a while to align themselves with the technological advancements within the sector. Such limitations are 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 any gaps and how these alternative measures can mitigate any corresponding ML/FT risks.

3.4 Enhanced Due Diligence

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 of 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.

Below is a non-exhaustive list of mitigating measures which CASPs may apply to mitigate higher ML/FT risks as necessary, depending on the risk exposure of the business relationship with the customer. These are:

- Identifying and verifying the identity of the customer on the basis of more than one reliable and independent source.
- Obtaining more information on the customer and the nature and purpose of the business relationship such as:
    - The nature of the customer's business or employment.
    - The source of wealth of the customer and source of the customer's funds that are

exchanged into crypto-assets.

- The source of the customer's crypto-assets that are being exchanged for official currencies and from where they were purchased originally.
- The purpose of the transaction i.e. why is the customer making use of the CASP's service.
- Information on any associations the customer might have with other jurisdictions (headquarters, operating facilities, branches etc.) or individuals who are known to exercise significant influence on the customer's operations.
- Information regarding the customer's past experience trading within the crypto- asset sector. Where the customer is a CASP, information on the trading history from within the CASP's system may also prove to be useful.

- Obtaining evidence about the source of wealth and source of funds/crypto-assets in respect of those transactions which present a higher risk of ML/FT.
- Increasing the frequency of transaction monitoring to identify possible patterns or indicators of suspicious activity when the business relationship poses a higher risk. This includes instances where a pattern of withdrawal or redemptions is not in line with the customer's profile. In such instances, the CASP should add additional measures to ensure that a withdrawal or redemption is requested by the customer and not by a third party.
- Reviewing and where necessary, updating CDD information and documentation more frequently and particularly upon the occurrence of a trigger event.
- Where a customer has multiple distributed ledger addresses or blockchain networks, the CASP should link these addresses to the customer.
- Increasing the frequency of monitoring the customer's IP addresses and checking them against the IP addresses used by other customers.
- Obtaining confirmation about the customer's level of knowledge and understanding of crypto-assets to achieve a level of assurance that the customer is not being used as a money mule.
- Applying advanced analytical tools as a supplement to the standard transaction monitoring tools, including to assess the risk associated with transactions involving self-hosted addresses. Such tools allow the CASP to trace the history of transactions and to identify potential links with criminal activities, persons or entities. CASPs should also obtain confirmation that a self-hosted address from which the transfer is received is under the control or ownership of the CASP's customer.

The additional measure or measures applied will depend very much on the risk factor/s driving ML/FT risk. Thus, if risk is being driven by concerns about the customer's source of wealth or source of funds, it would be no good to apply additional measures focusing on ascertaining the identity of the customer. It would be more appropriate to ascertain how the funds or the crypto-assets involved were generated and the purpose or reason for the carrying out of the particular transactions.

Apart from high-risk situations resulting from the CASP's risk assessment, the application of EDD is also required in situations where these are prescribed by law. This includes when the CASP enters into a correspondent relationship for the execution of crypto-asset services with a respondent institution from a country other than an EEA Member State. In addition to the measures for correspondent relationships as stipulated under Regulation 11(3) and Section 4.9.2.1 of the Implementing Procedures – Part I, CASPs are also required to apply the below EDD measures:

a) Determining whether the respondent institution is licensed or registered.

b) Documenting the reasons for the termination of any such relationship where this is attributable to reasons relating to AML/CFT.

c) Without prejudice to the generality of the obligations arising from other provisions of the PMLFTR:

    - Implementing appropriate measures to mitigate the risks associated with the respondent institution, this after taking into account any information obtained through the carrying out of the above measures; and

    - Updating any information obtained on a regular basis or upon the emergence of new risks in relation to the respondent institution.

3.5 Simplified Due Diligence

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 several other forms as explained in Section 4.8 of the Implementing Procedures – Part I.

When it comes to the determination as to whether SDD is to be applied or otherwise, one of the factors that should be considered 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 either in their 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 CASP is in a position to link them together. This may be done through a number of means, including by monitoring the IP address and/or the geo-location of the devices used by the customer.

Another one of the aspects that can influence the level of CDD applicable in a given case is the amount of funds or value of crypto-assets 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.

CASPs are to note that this threshold 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. In low risk occasional transactions, there can be at most a delay of the verification of identity measures up until a transaction is executed, which in the context of CASPs 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. CASPs 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 CASP from the customer's own funds for the acquisition of crypto-assets over a ninety (90) day revolving period[8], independently of whether the said funds are actually used or left to the credit of the customer's account with the CASP; or

b) The customer transfers crypto-assets to the service provider, either in a single transaction or in multiple transactions, which crypto-assets are valued at Euro one thousand (€1,000) or more[9].

In any case, SDD is not to be considered as an exemption from CDD given that, as a minimum, every

[8] This entails that the CASP 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 CASPs being able to make said determination either each time a customer effects a transfer to the CASP or at the end of the day when such a transfer or transfers take place.

[9] This entails that the CASP has to consider all the transactions carried out by the customer involving a transfer of crypto-assets to the CASP to determine the point in time when the amounts transferred are valued at Euro one thousand (€1,000).

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.

In addition to the above and to what is stipulated in Section 4.8 of the Implementing Procedures – Part 1, below are additional SDD measures that CASPs may apply in low risk scenarios. These include:

- For customers subject to a statutory licensing and regulatory regime in the EEA or in a non-EEA country, verifying the identity based on evidence of the customer being subject to that regime, for example through a search of the regulator's public register.
- Lowering the frequency of transaction monitoring for products involving recurring transactions.

3.6 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 CASP who receives crypto-assets or is to send crypto-assets, 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 crypto-assets are to be received or to which the crypto-assets are to be sent.

Together with the address, the CASP is also to ask the customer what kind of wallet the address relates to (e.g. a self-hosted wallet, a multi-signature wallet, a custodial wallet etc.). To the extent that this may be possible, CASPs are expected to corroborate the information provided by the customer with the information obtained through the use of analytical tools.

The following considerations need to be made:

Self-hosted Wallet – CASPs are to ensure that their policies and procedures identify and assess the risks of ML/FT associated with transfers of crypto-assets directed to or originating from a self-hosted address. Depending on the level of risk identified, CASPs are to apply appropriate measures to mitigate the ML/FT risks identified. This may include any one or more of the following measures:

- The identification and verification of the identity of the originator or beneficiary, including of the beneficial owner where applicable, of a transfer made to or from a self-hosted address.

This is to ensure that address is under the control and ownership of the CASP's customer.

- Requiring additional information on the origin and destination of the transferred crypto-assets.
- Conducting enhanced ongoing monitoring of those transactions.

Situations where this may be considered necessary include those:

a) where the CASP encounters unusual or suspicious patterns of transactions, including transactions involving significant amounts of crypto-assets or where the amount of crypto-assets 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) where the wallet allows for cold storage;

c) where the CASP is or becomes aware that the information on the originator or beneficiary using the self-hosted address as required in terms of the TFR recast is inaccurate;

d) 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 CASP (e.g. IP address, device geo location, use of cards issued by an institution not located in the customer's country of residence etc.);

e) 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.

When transactions carried out by the CASP involve the transfer or receipt of funds to or from a self-hosted address, it is necessary to also comply with the requirements stemming from paragraph 5 of Article 14 of the TFR recast, as explained further under Section 4.8 of the EBA Travel Rule Guidelines. These requirements include *inter alia* the obligation of the originator's CASP to take adequate measures to assess whether the address is owner or controlled by the originator, where the transfer to a self-hosted address exceeds EUR 1 000.

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 CASP 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.

Multi-Party Computational Wallet – Where the transaction involves the use of a multi-party computational wallet, a CASP has to likewise consider all the different parties holding parts of the key and apply identification and verification measures on all such parties.

On the other hand, there may be situations where corporate bodies make use of such wallets by granting different parts of the key to different representatives within the corporate body. In such cases, CASPs are to consider such individuals as equivalent to account signatories and apply the measures set out under Section 4.3 of the Implementing Procedures – Part I.

Additionally, where the software provider of such wallet retains part of the private key, the likelihood is that such retention would be part of the services being offered by the software provider and should not be considered to entail evidence of ownership over the said wallet. In such a case, the CASP would need to identify the software provider and verify its identity as provided for under paragraph (i) of Section 4.3.3 of the Implementing Procedures – Part I. This would therefore not entail the need to establish the ownership and control structure of the software provider and to identify and verify its beneficial owners.

On the other hand, where the MPC wallet is a custodial wallet and the custodian holds part of the private key, the CASP is to consider applying the measures set out in the subsequent paragraph. If the custodian found to present a higher risk, the CASP should additionally seek to identify and verify the identity of the custodian in line with paragraph (i) of Section 4.3.3 of the Implementing Procedures – Part I.

Custodial Wallet – In situations where the address relates to a custodial wallet, the CASP should carry out background checks on the custodian to consider the effect that the custodian may have on the ML/FT risk arising from the business relationship or occasional transaction. This would include:

a) Considering the regulatory status of the custodian. CASPs should note that the use of unregulated custodial wallet providers or regulated custodial wallet providers with no or weak regulatory and supervisory oversight, would both lead to an increased ML/FT risk. CASPs should therefore also consider whether the custodian is established in a EEA Member state or in a reputable jurisdiction.

b) Checking for any publicly available adverse information on the custodian.

c) Obtaining information on the AML/CFT control framework that the custodian has in place.

Custodial wallets presenting a higher risk of ML/FT require the application of appropriate mitigating measures depending on the reasons which led to the higher risk rating. In such cases, CASPs should consider obtaining senior management approval in addition to the application of one or more of the measures listed in Section 3.4 of this document.

3.7 Inability to Complete CDD Measures

Situations may arise in which a customer is not willing to provide the CASP 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 CASP 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 CASP is to terminate its business relationship with the customer.

b) The CASP 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 CASP, 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 CASP 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 CASP 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 CASP 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 CASP 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 CASP, 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 CASP 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 crypto-assets.

3.8 Ongoing Monitoring

Subject persons who establish business relationships with their customers 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 CASP's knowledge of the customer and the information in its possession is kept up to date. CASPs 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 CASP's knowledge of the customer and the customer's business and risk profile. Where a CASP 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 CASP 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, CASPs 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. CASPs may be carrying out transactions on-chain and/or off-chain, and therefore the transaction monitoring program has to be applied accordingly to ensure that 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 crypto-assets, 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 crypto-asset or changes wallets for the same crypto-asset;
- 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 CASP. 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 CASP'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 CASP 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 CASP is informed by the customer that he is a passive investor in crypto-assets and that the CASP will only receive regular crypto-asset transfers. Instead, the customer receives and sends significant amounts of crypto-assets at irregular intervals.

Depending on the outcome of their ongoing monitoring exercise, CASPs 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 crypto-assets;
- 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 CASPs may wish to put in place to monitor transactions and identify higher risk transactions that may require enhanced monitoring, detailed analysis or reporting. CASPs are encouraged to consider the below factors to the extent applicable to the activities undertaken by particular CASPs.

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 crypto-asset 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 crypto-assets • identify instances where account holders have multiple self-hosted 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 crypto-assets
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 crypto-assets 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 crypto-assets to a self-hosted wallet with links to other wallets flagged for illicit activities

As part of the CASP's obligations, a CASP 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.

3.9 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 crypto-assets, 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 crypto-assets 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 crypto-asset involved.

CASPs are to note that even in situations where any information is easily available on a public ledger, they should not place reliance on the ledger for record keeping purposes but are instead required to retain that information on file.

3.10 Reporting of ML/FT-Related Activity

As subject persons, CASPs 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. Thus, when there are grounds to submit an STR, the MLRO should promptly submit this on goAML. More guidance may be found in Chapter 5 of the Implementing Procedures Part I. 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 CASP 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 CASP 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 CASP has knowledge, suspicion or reasonable grounds to suspect ML/FT, the CASP 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 crypto-asset 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 crypto-asset services and the fragmented regulatory framework applicable to the said activities, it cannot be excluded that CASPs may have to submit an STR with other FIUs.

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

- the CASP's AML/CFT programme is fit for purpose and compliant with the obligations of the CASP 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 CASP's assessment of the ML/FT risks it is exposed to considering the service provider's size, business lines, customer base and geographic exposure;
- assess compliance by the CASP 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 CASP;
- 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 CASP;
- 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 CASP 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 CASP in the performance of its AML/CFT obligations. Where the AML/CFT reviewer and the Systems Auditor appointed by the CASP in terms of the MFSA's Rulebook are separate, and since it is likely that most CASPs 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 CASP'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.

3.12 Periodical Reports

The FIAU may require CASPs 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.

4. REPORTING UNDER THE TFR (RECAST)

As of 30 December 2024, CASPs have additional obligations under the TFR (recast), namely when it comes to the information on the originator and beneficiary that is to accompany a transfer of crypto-assets. These obligations are explained in more detail in the EBA Travel Rule Guidelines which the FIAU is adopting as its own legally binding guidance.

Additionally and in line with Articles 17(2) and 21(2) of the TFR (recast), the CASP of the beneficiary or intermediary CASP has the obligation to report to the FIAU a CASP that repeatedly fails to include the information on the originator and beneficiary as required in terms of the Regulation.

Such report should be submitted electronically on compliance@fiaumalta.org by using the template form below. Reporting should take place without undue delay, and no later than three months after identifying the repeated failure.

Notification pursuant to point (2) of Article 17 and point (2) of Article 21 of the TFR (recast)	
Name of reporting CASP/ICASP	
Address of reporting CASP/ICASP	
Date	
Name of repeatedly failing CASP/ICASP	
Name of country in which the repeatedly failing CASP/ICASP is authorised	
Short description of the nature of the breach, including: • the frequency of transfers with missing information • the period of time during which the breaches were identified; and • reasons given by the repeatedly failing entity, if any, to justify the breach.	
Short summary of the steps that the reporting CASP/ICASP has taken.	

ANNEX 1 – CRYPTO-ASSET-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 crypto-asset 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.

Subject persons are also urged to familiarise themselves with the FATF's report on Red Flag Indicators of Money Laundering and Terrorist Financing concerning Virtual Assets, published in September 2020, and any updates thereto or related documents

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 crypto-asset 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 crypto-asset 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 crypto-assets 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 crypto-assets may be exploited for illicit purposes. The vulnerabilities described in Section 2 of this document render crypto-assets an attractive tool for criminals, be it as a means of payment, where crypto-assets 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 crypto-asset ATMs and of crypto-asset-backed debit

cards, making it easier to acquire and use crypto-assets, have further increased the attraction that crypto-assets present for criminals.

2.1 Crypto-Assets as Proceeds of Crime – General Trends

The association between crypto-assets 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 the darknet and simultaneously seize significant amounts of crypto-assets. By way of example, the shut down of the Wall Street Market by German authorities led to the confiscation of crypto-assets 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 crypto-assets, 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 crypto-assets. More recently, an operation in 2021 saw the German authorities shutting down the Monopoly Market's criminal infrastructure, leading to the arrest of 288 persons suspected of drug trafficking and the seizure of circa EUR51 million in cash and virtual currencies.

Crypto-assets 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 2024 IOCTA noted that while ransomware operators usually demand BTC as ransom, there are cases where demands have been made in other crypto-assets such as Monero. In general, the report also noted the growing use of alternative coins (altcoins) in a number of areas of crime.

The abuse of crypto-assets by criminal elements has led to crypto-asset 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. The 2024 IOCTA features the most active cyber-crime related forums and marketplaces known for sharing hacking knowledge, trading in stolen data and hacking tools. It also notes an increased trend in marketing of AI tools and services on the dark web, including the sale of AI generated fake IDs that can be used to open accounts with service providers while bypassing CDD measures.

Akin to the increase of attacks on crypto-asset users and service providers, is the emerging trend in crypto-jacking to mine crypto-assets, especially BTC and XMR. The 2024 IOCTA noted that in 2024, Ukrainian law enforcement, with the support of EUROPOL, arrested an individual suspected of being the mastermind of a sophisticated cryptojacking scheme that made use of compromised computers to mine crypto-assets. The scheme is said to have generated over EUR 1.8 million in mined Etherium, Monero and TON.

Scams remain an ever popular means how to defraud individuals and entities of their funds, including crypto-assets. 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 crypto-assets. Through typosquatting, where a well-known online crypto-asset 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. The 2024 IOCTA also notes that crypto-assets are the payment method of choice for subscriptions to phishing services. These crime-as-service models enable criminals who are not as technologically capable to perform criminal activities that require a level of knowledge of technology.

The 2024 IOCTA also noted that fraud is the most frequently identified predicate offence involving the illicit use of crypto-assets. The increased value of some cryptocurrencies and the growing media attention on crypto-investments are also contributing to the rise in investment fraud cases. As a result, crypto-assets are the most reported product offered to victims in investment fraud. In 2021, Belgian authorities uncovered a criminal network using the social media platform 'Vitae.co' and the website 'Vitaetoken.io' to trick people into investing in a cryptocurrency Ponzi scheme. Around 223 000 individuals from 177 countries are believed to have fallen victim to it. Over EUR 1 million in cash was seized, along with EUR 1.5 million in cryptocurrencies and 17 luxury vehicles.

EUROPOL's 2023 European Financial and Economic Crime Threat Assessment also noted the exploitation of liquidity mining to conduct crypto-related fraud. The report remarks that developments in the crypto-asset market may impact the forms of crypto-asset abuse adopted by criminals in the future. This includes the potential abuse of BTC exchange-traded funds (ETFs), which allows investors to speculate on the price of BTC without owning them.

2.2 Crypto-Assets as a Laundering Tool – General Trends

The use of crypto-assets as a laundering tool can take a number of forms as evidenced by a 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 crypto-assets 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.

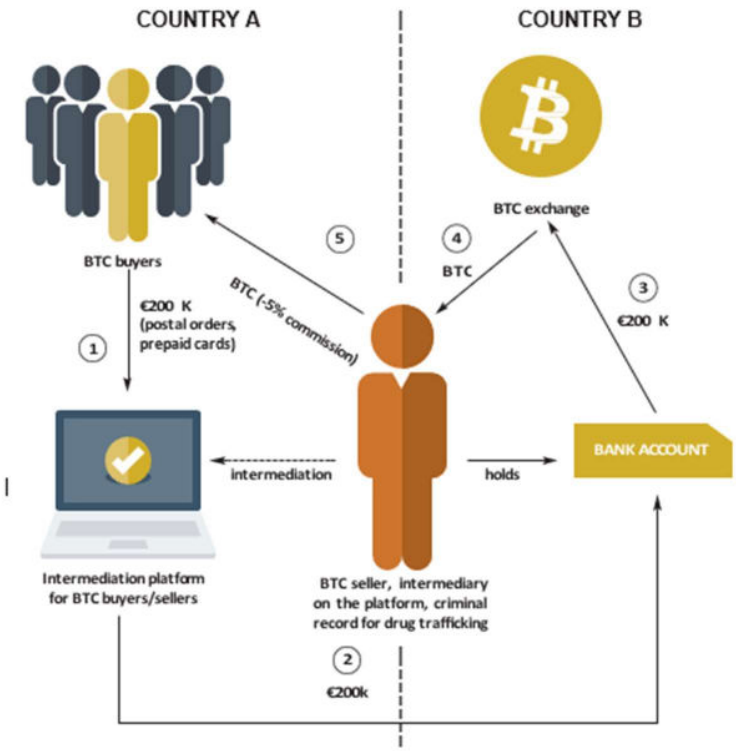
Cards linked to crypto-asset wallets were also one of the means how the organisation behind a series of malware attacks against financial institutions were able to launder the funds derived from their illicit activities. Through pre-paid cards linked to crypto-asset wallets, the organisation was able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

The use of crypto-assets as a laundering tool need not be limited to the laundering of FIAT currency but may also involve the laundering of crypto-assets 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 crypto-assets mixed were derived from illegal activities.

The 2024 EUROPOL IOCTA notes an increased use of underground banking for laundering of crypto-assets, as well as the re-emergence of crypto-backed debit cards and the frequent criminal use of swapping services. The techniques used to launder crypto-assets vary depending on the predicate offence committed.

2.3 Crypto-Assets and Money Laundering – Case Studies

Case No. 1

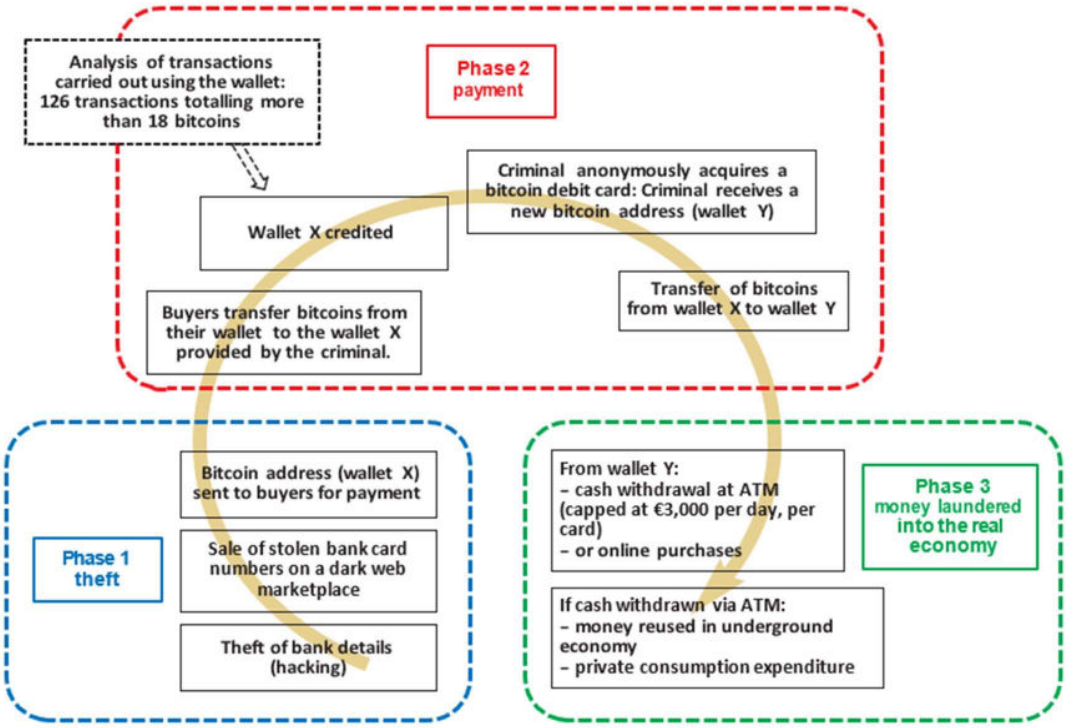


A number of individuals involved in drug trafficking sought to launder *circa* EUR 200,000 obtained from drug trafficking by acquiring BTC through an intermediation platform. The EUR 200, 000 were deposited with the platform using payment means like postal orders and pre-paid cards that provide a level 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 provide 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 self-hosted 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.

Case No. 6

A group of individuals were involved in a rug-pull scam consisting of the creation of a token listed on a decentralised platform and operating by a smart contract with the following provisions:

- The token is associated with a known crypto-asset.
- For each token purchase made by an investor, 60% of the amount invested is converted into tokens while the remaining 40% is theoretically used for the project's operating costs. The supposed increase in the value of the token is said to make up for the initial 40% loss.
- For each purchase of a token by an investor, the group of individuals would receive a profit from the payment corresponding to 5% of the investment. These are listed as transaction, liquidity and withdrawal fees.

Once the liquidity threshold as provided by the smart contract was reached, the group of individuals performed a liquidity withdrawal where they exchanged all the tokens they held for the known crypto-asset. Thus, the tokens held by the investors lost their value and no longer remained exchangeable.

(TRACFIN – *2023/2024 AML/CFT: State of the Threat)*

2.4 Initial Crypto-Asset Offerings

Initial Crypto-asset 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 crypto-assets, 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 crypto-asset, the origin of subscribers' funds.

b) They can be a means how to defraud subscribers – Fraudulent crypto-asset offerings can take place in a number of ways:
   i. Issuers may make false statements to increase market interest in their crypto-asset

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 crypto-asset 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 Crypto-Assets and the Funding of Terrorism

Terrorist and terrorist organisations seem to use crypto-assets and their service providers for terrorist financing- related crowdfunding activities.

Terrorist organisations and sympathisers are known to prefer transferring funds through the traditional banking system, money transfer services and informal value transfer systems such as *hawala.* However, the use of crypto-assets and their service providers has been noted among terror groups and their sympathisers. EUROPOL's TESAT for 2023 remarks how some terrorist elements are increasingly making use of crypto-assets and their service providers as these provide higher levels of anonymity for donors and recipients. For instance, crypto-assets would be paid to an account in one country where they are withdrawn, split and then sent via *hawala* to other countries and further transferred via money transfer services. Certain right-wing extremists have also been observed using crypto-assets to collect and channel funds needed to finance their terrorist activities.

Some known instances in which crypto-assets 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 Crypto-Assets

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.