Key Results of the Sectoral Risk Assessment on Virtual Financial Assets

National Coordinating Committee on Combating Money Laundering and Funding of Terrorism

February 2020

Table of Contents

Acronyms used in this assessment

AML	Anti-Money Laundering
AMLU	Anti-Money Laundering Unit of the Malta Police Force
BO	Beneficial Owner
CFT	Combating the Financing of Terrorism
CFP	Combating the Financing of Proliferation
DD	Due Diligence
DLT	Distributed Ledger Technology
DNFB	Designated Non-Financial Businesses and Professions
EU	European Union
FATF	Financial Action Task Force
FI	Financial Institution
FIAU	Financial Intelligence Analysis Unit
FIU	Financial Intelligence Unit
FT	Financing Terrorism
IIP	Individual Investor Programme
ITAS	Innovative Technology Arrangements and Services
MBR	Malta Business Registry
MDIA	Malta Digital Innovation Authority
MFSA	Malta Financial Services Authority
MIIPA	Malta Individual Investor Programme Agency
ML	Money Laundering
MSB	Money Service Business
MLA	Mutual Legal Assistance
NCC	National Coordinating Committee on Combating Money Laundering and Terrorism Financing
NRA	National Risk Assessment
NPO	Non-Profit Organisations
PMLFTR	Prevention of Money Laundering and Funding of Terrorism Regulations (Legal Notice 180 of 2008)
PIF	Professional Investor Funds
PMLA	Prevention of Money Laundering Act (Chapter 373 of the Laws of Malta)
PQ	Personal Questionnaire
ROLP	Registrar of Legal Persons
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Provider
TFS	Targeted Financial Sanctions
VFA	Virtual Financial Asset
VFAA	Virtual Financial Assets Act
VO	Voluntary Organisation

1. Introduction

The DLT landscape is developing at a very fast pace in Malta. Malta has positioned itself as a leading jurisdiction in this aspect by creating the EU's first comprehensive legislation and regulatory framework covering DLT-enabled services that offer legal and regulatory certainty in an environment that was previously unregulated. The related regulatory frameworks in Malta cover the broader scope of DLT assets. The Virtual Financial Assets Act (VFAA), the Malta Digital Innovation Authority (MDIA) Act and the Innovative Technology Arrangements and Services (ITAS) Act are the three pieces of legislation adopted by the Maltese Parliament to regulate this area of activity in 2018. This legislation has been supplemented by regulations issued by the relevant Ministers and rules issued by the MFSA, Malta's single regulator for financial services, the MDIA, which is the regulator for innovative technology arrangements and related services and the FIAU, which is Malta's primary supervisory authority for ML/FT.

In terms of the VFA Act, 'virtual financial asset' means any form of digital medium recordation that is used as a digital medium of exchange, unit of account or store of value and that is not electronic money, a financial instrument or virtual token. In light of the fact that such factors are dynamic and developing at a significant pace, Malta is developing a robust regulatory, supervisory and enforcement framework. Malta is thoroughly committed to combatting all forms of ML/FT and this assessment is intended to develop a deeper understanding of the specific risks posed by this new sector, while at the same time embracing the opportunities presented by recent technical advancements. However, it is to be noted that since the cut-off date for the collection of all the statistics and the feedback from the competent authorities and the private entities essential for the analysis was October 2018, this assessment does not take into account the developments at the international level of the revised FATF recommendations and does not consider to what extent the domestic legislative framework is compliant with the revised FATF recommendations. To this end, a paper is presented with this assessment, that proposes a series of recommended actions to ensure that the domestic framework is better aligned with the revised FATF recommendations. Furthermore, this paper addresses in more detail the risks and challenges that the law enforcement structure in Malta has to face when dealing with these issues.

In October 2018, the FATF adopted changes to its Recommendations to explicitly clarify that such recommendations apply to financial activities involving virtual financial assets and added two new definitions for 'virtual asset' and for 'virtual asset service provider'. Accordingly, virtual financial assets are defined as 'a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual financial assets do not include digital representation of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations'. Meanwhile, the FATF definition for 'virtual asset service provider' is now found as being 'any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) exchange between virtual financial assets and fiat currencies; (ii) exchange between one or more forms of virtual financial assets; (iii) transfer of virtual financial assets; (iv) safekeeping and/or administration of virtual financial assets or instruments enabling control over virtual financial assets; and (v) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.'

The key results document presents a summarised view of the methodology and key findings of the risk assessment. How this risk assessment was conducted is briefly presented in the third

section. Subsequently, the key findings of this risk assessment follow, while the final section will present the action plans aimed at mitigating such risks. Competent authorities and the private sector can use this key results document of the sectoral risk assessment on VFAs to advance its risk-based approach to regulation, supervision and enforcement, and mitigate the ML/FT risks within this rapidly growing part of the economy.

1. Overview of the Risk Assessment

The past decade has seen numerous technological advancements across multiple fields, one of which has been the development of virtual financial assets and more specifically, virtual currencies. These assets have the potential to transform how people save, transact and invest. They also pose their own unique risks from an ML/FT perspective. Malta is committed to combatting all forms of ML/FT and this document is intended to further strengthen these efforts. This assessment laid out the key ML/FT related threats facing Malta and provides an assessment of the vulnerability and control environment of both the country as a whole and a range of key sectors of the economy. The sectoral risk assessment on VFAs was a joint effort led by the NCC in collaboration with the MFSA, the FIAU, the MDIA, the MGA, the ARB, the SMB, the IFSP, the virtual currency exchanges, the gaming operators, and other private sector participants.

Approach taken

The approach involved four main steps:

- The first step was to assess the impact of VFAs on the threat landscape of predicate offences, both in terms of the impact of VFAs on existing predicate offences and in the context of new types of threat that have arisen due to the growing prevalence of VFAs (e.g. ransomware, ICO fraud etc.)
- The second step was to conduct a vulnerabilities assessment, both of the VA classes themselves, as well as of the Maltese sectors that will be utilising VFAs as part of their operations.
- The third step comprised a review of controls. The three pieces of VA related legislation were reviewed along with the proposed supervisory and enforcement framework.
- As a fourth and final step, recommended enhancement measures and key priorities for the country were outlined across several areas (e.g. governance, processes, capabilities etc.)

In this sectoral risk assessment, the approach does not assess residual vulnerability (which refers to the "remaining" vulnerability after taking into account the impact of mitigation controls that have been put into place). The reason for this is that the sector is still very young and is rapidly developing. As such, a review of control measures were conducted and certain high-level strategic enhancements proposed. A gap analysis was presented with this risk assessment that addressed to what extent the implemented legislative framework governing VFAs, VFA issuers and VFA service providers is compliant with the revised FATF recommendations, as well as addressing the fact that the current law enforcement structure in Malta ignores the risks and challenges dealing with this matter.

In order to establish a holistic picture of the landscape, the assessment incorporated a wider taxonomy of assets, including convertible virtual currencies like crypto-currencies as well as non-convertible virtual currencies and crypto-backed financial products. It is to be noted that since the cut-off date for the collection of all the statistics and the feedback from the competent authorities and the private entities essential for the analysis was October 2018, this assessment

does not take into account the developments at the international level of the revised FATF recommendations and does not consider to what extent the domestic legislative framework is compliant with the revised FATF recommendations. To this end, a paper is presented with this assessment, that proposes a series of recommended actions to ensure that the domestic framework is better aligned with the revised FATF recommendations. Furthermore, this paper addresses in more detail the risks and challenges that the law enforcement structure in Malta has to face when dealing with these issues.

In October 2018, the FATF adopted changes to its Recommendations to explicitly clarify that such recommendations apply to financial activities involving VFAs and added two new definitions for 'virtual asset' and for 'virtual asset service provider'. Accordingly, VFAs are defined as 'a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. VFAs do not include digital representation of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations'. Meanwhile, the FATF definition for 'virtual asset service provider' is now found as being 'any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) exchange between VFAs and fiat currencies; (ii) exchange between one or more forms of VFAs; (iii) transfer of VFAs; (iv) safekeeping and/or administration of VFAs or instruments enabling control over VFAs; and (v) participation in and provision of financial services related to an issuer's offer and/or sale of a VA.'

Important definitions

Some important definitions need to be outlined prior to assessing the ML/FT context. Primarily, DLT means a database system in which information is recorded, consensually shared, and synchronised across a network of multiple nodes as further described in the First Schedule of the ITAS Act, 2018, whether the same is certified under that Act or otherwise.

Secondly, in line with the joint guidance notes by MFSA and FIAU, 'DLT asset' means (a) a virtual token; (b) a virtual financial asset; (c) electronic money; or (d) a financial instrument; that is intrinsically dependent on, or utilises, DLT. Moreover, in accordance to these guidance notes, 'DLT exchange' means any trading and, or exchange platform or facility, whether in Malta or in another jurisdiction, on which any form of DLT asset may be transacted in accordance with the rules of the platform or facility;

The term 'electronic money' has the same meaning assigned to it under the Third Schedule to the Financial Institutions Act; while 'financial instrument' has the same meaning assigned to it under the Second Schedule to the Investment Services Act, whether or not issued in Malta; result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services; VFA means any form of digital medium recordation that is used as a digital medium of exchange, unit of account, or store of value and that is not (a) electronic money; (b) a financial instrument; or (c) a virtual token; 'virtual token' means a form of digital medium recordation whose utility, value or application is restricted solely to the acquisition of goods or services, either solely within the DLT platform on or in relation to which it was issued or within a limited network of DLT platforms: Provided that the term 'DLT platform' referred to in this definition shall exclude DLT exchanges: Provided further that a virtual token which is or may be converted into another DLT asset type shall be treated as the DLT asset type into which it is or may be converted;

2. Assessment of ML/FT threats

First of all, it is important to highlight that this section does not consider the controls in place or their effectiveness. This section presents the ML/FT threats. Two types of threats were examined: existing threats that may be exacerbated by the rise of virtual financial assets and emerging threats that will be created / enabled by the emergence of VFAs.

The ***existing threats*** are predicate offences that are deemed particularly susceptible to the rise of VFAs, namely:

- ***Illicit trafficking in narcotic drugs and psychotropic substances*** - Virtual currencies have transformed the way in which drugs are bought and sold. Cryptocurrencies offer several notable advantages to those looking to traffic drugs. Their anonymity, cross-border reach and lack of transaction limits make them ideal for transferring the proceeds of drug trafficking quickly and efficiently online. Cryptocurrencies are also popular for buyers of drugs for the same reasons. Numerous 'darknet marketplaces' exist to facilitate illicit crypto-transactions. Typically, a darknet marketplace will include listings for drugs, weapons, stolen credit cards, fake identities, cyber-weapons and other criminal goods and services. Buyers will transfer payment via Bitcoin into an escrow account maintained by the marketplace. On successful receipt of the goods the crypto-funds will be credited to the seller's account.
- ***Corruption and bribery*** - limited known incidents to date of virtual financial assets being used to enable bribery and corruption. This is in part due to their relative low penetration rate in comparison to other payment methods, as well as the inconvenience presented by trying to convert VFAs into fiat currencies.
- ***Fraud (incl. tax evasion)*** - cases for tax evasion can occur by using VFAs is the use of undetectable cross-border fund transfers to a jurisdiction where the funds can be withdrawn without being subject to tax. Another way in which VFAs might be used to facilitate tax evasion concerns the application of capital gains tax. Because VA exchanges and wallet providers are currently not required to report the trading activities of users to the government, investors in VFAs are able to accrue investment gains on their VFAs and withdraw them without paying the necessary tax and without the government's knowledge. Additionally, VFAs can be used to circumvent corporation tax much like cash might be used today. This would involve the provision of goods or services in exchange for VFAs with the transaction not officially recorded towards the company's revenues. This phenomenon mirrors how many criminals use cash to avoid taxation today, but with two key differences: where, VFAs are not bound by physical limitations, meaning that far greater sums can be exchanged with relative ease and with no physical trail of evidence. Secondly, VFAs enable this form of tax evasion to occur online, thereby greatly expanding the reach of businesses looking to exploit this method.
- ***Robbery or theft*** - cryptocurrencies do not in themselves facilitate acquisitive crime. They are more likely to be used in the onward sale of stolen goods using darknet marketplaces. Due to their prolific use online, cryptocurrencies are often used for the onward sale of stolen 'e-goods' (e.g. passwords, credit card details, licensed software etc.) Finally, cryptocurrencies themselves are proving to be increasingly susceptible to acquisitive crime (e.g. theft of Bitcoin via hacking of exchanges).

It is worth noting that, in contrast to money-laundering using VFAs (which has seen several notable recent cases and is estimated to account for billions of Euro of laundered funds yearly in Europe alone), terrorism financing using VFAs has been limited to date, and mainstream

adoption of cryptocurrencies to fund terrorism has so far not occurred. This is likely due to several barriers:

- High volatility of cryptocurrencies
- Difficulties in converting cryptocurrencies into fiat cash for use in purchases
- Lack of sufficient technical expertise amongst terror groups
- Possibility of tracing and flagging suspicious transactions through the ledger on the most liquid / readily available of cryptocurrencies

Despite these disadvantages it is likely that terrorist groups will continue to solicit funding via cryptocurrencies and the barriers listed above are not insurmountable. In time, it is possible that a stable market value is reached for 'privacy tokens' such as Dash and Monero, rendering them useful to terrorism financers, while the technical expertise of terror groups is only likely to increase.

Emerging threats: recent years have seen an increase in the proliferation of new predicate offences specifically linked to the rise of VFAs. While the offences outlined above have been aided by the rise of VFAs, the following cybercrimes have grown in prevalence precisely because of the increased usage and acceptance of VFAs:

- ***Ransomware attacks*** - payments demanded to unlock the victim's computer are increasingly solicited in cryptocurrency. These attacks typically involve the installation of malware to block or limit access to the victim's personal data. The malware will then promise to return or unblock the data on completion of a ransom payment.
- ***Hacks*** (typically involving the theft of large sums of virtual currency from an exchange provider) - One of the most common examples of hacking is the theft of virtual financial assets. This category is the most prevalent of the new threats arising from the rise of virtual financial assets and has seen billions of dollars' worth of virtual financial assets (almost always cryptocurrencies) stolen by hackers. Typically, criminals will target a prominent virtual currency exchange and exploit weaknesses in system controls to syphon off large sums.
- ***Market manipulation*** - increasingly common among virtual currencies with a low market capitalisation where a few large investors can control prices. Several observers have noted the potential for criminals to abuse crypto-trading markets much in the same way that insider trading or traditional market manipulation might occur. The difference with the nascent cryptocurrency exchanges is that they are particularly vulnerable to abuse owing to their relatively low volumes and the potential for a small number of asset holders to control sizeable percentages of a coin or token's total market value.
- ***Fraudulent ICOs*** – this reflects a phenomenon involving false promises regarding the future value of a crypto-asset before or during its launch. ICOs are increasingly used as a means to raise funds for the future development of an issuer's coin or token. Individuals or organisations will typically purchase pre-mined coins in the hope that the coin will appreciate in value once the proposition gains traction. The greatest risk posed by ICOs is that of fraud. In contrast to more traditional fundraising methods (e.g. IPOs), the lack of regulatory oversight has led to minimal barriers to launching a token while there are unclear penalties in place in case of fraud. In addition to this, many investors are unaware of the risks posed by ICOs; there is limited understanding of key technological concepts among many, while demand is often driven by hype rather than by the proven fundamentals of the proposition.
- VFAs can be used to fund the manufacture, acquisition, purchase of illicit weaponry (nuclear, chemical or biological weapons) and their means of delivery.

3. Assessment of inherent ML/FT risk

VFAs and VA related service providers were reviewed as part of the assessment, in order to determine inherent vulnerabilities.

Assets

The landscape of VFAs was divided into three categories for the purposes of the assessment: convertible virtual currencies, non-convertible virtual currencies and crypto-backed financial products. A vulnerability assessment was conducted to determine the level of ML/FT risk posed by each of the VA classes including the dimensions materiality of the asset class, technological suitability for crime, convenience, and existing criminal precedent.

Convertible virtual currencies

'Convertible virtual currencies' is a broad category incorporating a wide range of VFAs. The following sub-categories were considered in assessing inherent vulnerabilities (taking into account the fact that the categories listed here are not mutually exclusive):

- Cryptographic coins and tokens
    - Payment tokens
    - Utility tokens
    - Security tokens
- Centralised, non-cryptographic currencies

Payment tokens represent the most vulnerable of all VFAs. This category includes those cryptocurrencies whose sole purpose is to function as a means of exchange. They have the highest market capitalisation of any virtual currency and are expected to grow in popularity with both retail and institutional investors. Technologically speaking they typically operate on public distributed ledgers, meaning that all transactions can be traced but users can maintain 'pseudonymity'. Monero and Dash, on the other hand, allow for fully anonymous transactions and are growing in popularity with both legitimate and illegitimate users. In comparison to other virtual financial assets, the most popular of the payment tokens offer a high level of convenience to users and can be readily purchased and traded on a variety of exchange platforms. The specific level of convenience depends greatly on the popularity of the payment token in question, but the most popular examples enjoy relative liquidity on exchanges. Payment tokens are also the category most likely to be accepted by merchants as a means of payment. Given these qualities, payment tokens are the VA class of choice for many looking to commit ML/FT offences. One common example is the prevalent use of Bitcoin on darknet marketplaces, where the currency is used to enable predicate offences such as drug-trafficking as well as to launder the resulting funds.

Utility and security tokens also pose a high risk but are not as vulnerable to ML/FT abuse as payment tokens. Despite many utility and security tokens displaying the same characteristics as payment tokens, their relative illiquidity, low level of acceptance with merchants and smaller share of the overall market capitalisation of crypto-assets makes them a less attractive prospect to criminals looking to exploit them for ML/FT purposes. Utility tokens vary greatly in their ease of access and convertibility. Some tokens (e.g. Ethereum) benefit from high liquidity and a range of exchanges on which the currency can be purchased. However, the clear majority of utility tokens are illiquid and require a considerable time investment and base level of technical understanding to access. This renders them less likely to be used for ML/FT purposes. Therefore, despite many utility tokens displaying the same characteristics as many payment

tokens, their relative illiquidity, low level of acceptance with merchants and smaller share of the overall market capitalisation of crypto-assets makes them a less attractive prospect to criminals looking to exploit them for ML/FT purposes. Known criminal use of utility tokens is low, and despite some darknet marketplaces accepting ETH as a means of payment, this is rare, and the vast majority of transactions are carried out in Bitcoin, Monero and other payment tokens. In fact, the greater risk presented by utility tokens is that of ICO fraud (covered separately in detail). In this respect utility tokens are vulnerable to abuse via a predicate offence (fraud), but the resulting criminal proceeds are harder to layer and integrate than if they were in payment token form.

At present the total market capitalisation of ***security tokens*** is minimal in comparison to payment tokens and utility tokens and they are often subject to substantially greater regulatory and supervisory scrutiny than other token types. Given their status as securities in several jurisdictions, they are likely to be subject to far tighter reporting and trading restrictions. Despite this, security tokens are still highly vulnerable to ICO fraud. This category is made up of those tokens which represent ownership of an underlying asset. This might be company stock (in the case of equity tokens like the Neufund token) or could represent a physical asset (as with the gold-backed token, Digix). The core principle of security tokens is that their value is inextricably linked to that of the underlying asset. The benefits of security tokenisation include: 24/7 availability (versus traditional securities only operating during business hours); global reach; lower costs (no clearing, settlement, or custody fees); democratisation of funding (anyone with internet access can participate in ICOs). At present the total market capitalisation of security tokens is minimal in comparison to payment tokens and utility tokens. Much of this is because security tokens are subject to substantially greater regulatory and supervisory scrutiny than other token types. Criminal use of security tokens is low to date (partly due to their low numbers). Additionally, given their status as securities in several jurisdictions, they are likely to be subject to far tighter reporting and trading restrictions. This is not to say that money laundering could not occur using these tokens (e.g. via OTC trades on exchanges) but the risks are not as great as those posed by payment tokens.

Centralised non-cryptographic currencies are not as vulnerable as their cryptographic counterparts because they are typically more traceable, less anonymous, and have a lower market capitalisation.

Non-convertible virtual currencies

This asset class poses a low ML/FT risk, largely because they cannot be converted out of or into fiat currencies. Non-convertible virtual currencies are those that are restricted to circulation within their given system or domain. This includes currencies that are open to one-way transfer (into or out of fiat currency), as well as currencies that have no direct link to the real-world economy. The ML/FT use cases of these are limited by the fact that they are not able to be purchased using fiat currency and exchanged back into fiat. This renders them useless from an ML/FT perspective.

Crypto-based financial products

These assets are moderately vulnerable to ML/FT exploitation and are comparable to other financial products with exotic underlying assets. This category incorporates the many current and planned financial products which perform based on one or more underlying cryptocurrencies, including products such as crypto-ETFs.

Currently the total value of crypto-based financial products is low, but numerous firms have expressed interest in participating in the space. One of the key differentiating factors between

these financial products and the other prioritised asset classes is that there is an existing regulatory and supervisory framework under which these crypto-based financial products would fall. To some extent this key difference nullifies much of the ML/FT risk, because any company looking to offer crypto-backed financial products will need to abide by the same KYC/AML procedures that are in place today for traditional financial products.

VFA Businesses

As with VFA classes, the landscape of DLT and VFA related businesses was divided into three categories for the purposes of the vulnerabilities' assessment: VFA specific businesses, businesses looking to leverage VFAs, and gatekeepers. The dimensions used included size of the sector in Malta, nature of products/services offered, typical clients and distribution methods and current level of AML/CFT expertise.

VFAs specific businesses tend to pose a high or very high risk, largely because their entire business model is reliant on virtual financial assets.

- The ***issuer*** (or ICO) sector is highly vulnerable to ICO fraud and many companies are expected to seek funding via this means in Malta in the future. Issuers pose a very high ML/FT risk predominantly because of the potential use of ICOs to commit fraud, as seen in numerous recent exit scams. As a rule, an issuer's 'clients' (those looking to invest in the project) will be located across the world and the vast majority of interactions will occur solely online, thereby eliminating the potential to conduct face-to-face due diligence. Additionally, issuers will typically be new to the AML/CFT obligations that come with raising funds, and while traditional businesses are supported by advisers when pursuing an IPO (e.g. banks), issuers are under no obligation to do the same.
- ***Custodial wallet providers*** are also a very high risk because of the nature of the service that they provide. They offer custody of crypto-assets which leaves them vulnerable to those looking to store illicit funds. They also have very limited experience in KYC/AML procedures in comparison to established banks.
- ***Exchanges*** pose perhaps the greatest overall risk owing to their position at the crossroads of fiat and virtual currency. All exchange providers are inherently vulnerable to ML/FT abuse because of their function in the crypto-ecosystem; at their most vulnerable (crypto-fiat) they can be used by criminals to place, layer and integrate funds. Like wallet providers, crypto-exchanges are often young businesses with minimal expertise in anti-ML/FT processes and the majority provide services for the highest risk currencies (e.g. Bitcoin).
- ***ATM providers*** pose a marginally lower risk partly due to the size of the sector in Malta but partly due to the fact that clients have to be physically present in Malta in order to use the service. Crypto ATMs are largely unregulated at present and significant variation can be seen across providers and across geographies in robustness of KYC procedures (e.g. deposit / withdrawal limits, ID requirements, camera installations etc.)

Businesses looking to leverage VFAs:

- At present Maltese ***banks*** are not providing banking services to virtual asset businesses (except for servicing operating expense accounts that are ring-fenced from VFA-related activities). This is driven by the lack of certainty surrounding the current regulatory framework and the policies and procedures in place at VFA businesses. It is also connected to the fact that many Maltese banks rely on correspondent banks and have to operate in a way that matches their risk appetite. However, this is not to say that in the future the sector will not begin to cater to the needs of VFA businesses and their customers. In such a scenario there are clear opportunities for criminals to exploit banks for ML/FT purposes. The clearest risk posed to banks is that of criminals using their services to integrate virtual

financial assets into the real economy by depositing sums into accounts held by the bank. Practically speaking this would most likely occur via withdrawals of fiat sums from a virtual exchange provider. An alternative scenario might involve a VFA business holding compromised funds (knowingly or unaware) in a corporate account with the bank. Despite these clear vulnerabilities, banks are deemed to pose medium risk rather than a high risk for three reasons:
    - They are well-versed in AML/CFT measures and have robust policies and procedures in place (essential for operating in Malta)
    - They have a clearly stated risk appetite (partially determined by correspondent banks) which will rule out the riskiest of virtual-asset related activities
    - The industry is mature and operates under clear regulatory and supervisory oversight
- The number of investment firms currently offering VFA related products in Malta is low. However, several firms have expressed interest in offering both crypto-based financial products (e.g. Bitcoin futures) as well as access to the underlying cryptocurrencies themselves to their clients. Despite muted interest to date from institutional clients, there has been clear appetite from retail investors, family offices, hedge funds etc. to gain exposure to virtual financial assets. As investment firms begin to service this demand, the sector will as a whole be very vulnerable to ML/FT risks. Sophisticated structuring of financial products has long been a way for complicit investment firms to launder illicit proceeds on behalf of criminals. This risk will remain the case with virtual asset related investments and the risks will arguably be greater given the general gap in understanding around the underlying technologies behind the products. This risk applies as much to customers as it does to the investment firms themselves. Furthermore, given their diminutive size relative to banks, investment firms are more likely to have less robust AML/CFT procedures in place. Their size and number also mean that it is far easier for a rogue operator to remain undetected for considerable periods of time.
- Gaming operators pose the highest risk in this category largely due to the size of the sector in Malta, the products and services offered, and the fact that many clients will be located abroad. The remote gaming operators are more vulnerable than their land-based counterparts because of the difficulties in identifying customers. There is no face-to-face interaction with the player (who is often located outside of Malta), and any identity checks have to be carried out via email or phone. This leaves them vulnerable to abuse (e.g. fraudulent account creation using falsified/stolen identification documents).

VFA agents, on the other hand, are particularly exposed. Accredited private firms will serve as "virtual financial asset" agents, carrying out much of the due diligence required to license businesses operating in the virtual financial asset space. Their role as a 'gatekeeper' leaves them open to exploitation and coercion by criminals looking to commit ML/FT offences. As a key part of the second-line of defence they would have to be complicit (either knowingly or otherwise) in any criminal activity. The fact that the virtual financial asset space is so technologically complex and subject to rapid change means that VFA agents need to be particularly well-qualified to carry out their role in the ecosystem.

4. Controls assessment

Findings of the assessment indicate that Malta has taken a proactive approach to regulating and supervising this fledgling space and has released three pieces of landmark legislation to address the virtual asset and DLT space (the VFA, MDIA, and ITAS acts). The assessment examined

the existing and proposed legislation and control framework for virtual financial asset issuers and service providers as well as innovative technology arrangement and service providers across four stages of classification, supervision (market entry and ongoing monitoring), preventative measures, and investigation, prosecution and recovery. Each of the three acts predominantly covers the supervisory mandates and processes that will govern market entry controls, with less emphasis given to ongoing supervision, investigation and prosecution.

From an AML/CFT perspective, the VFA Act goes well beyond 5AMLD and establishes that all VFA issuers (ICOs) and virtual asset service providers will be classified as subject persons (as defined in Malta's Prevention of Money Laundering act). The VFA Act also determines which assets should be classified as VFAs and applies certain criteria to distinguish VFAs from financial instruments (as defined in MiFID II), virtual tokens and e-money. It is to be noted that authorisations under the VFA and ITAS Acts are not mutually exclusive and a person may hold dual authorisation.

5. Recommendations from the Sectoral Risk Assessment

In the risk assessment, the recommendations that were made, centred around the fact that various observations were noted for potential expansion to the framework which, if implemented, would see Malta progress yet further in its aim to establish itself as the world's soundest regulatory regime in which to operate a DLT business. This includes determining necessary enhancements to core processes to incorporate the new demands of the VFA space, as well as building out clearer roles and responsibilities across the framework and training both public and private sector stakeholders to allow them to fulfil their role in the framework effectively.

Recommendations for the Competent Authorities

Specific enhancements for the public sector were grouped under broader thematic improvements which apply across the regulatory and supervisory framework.

Enhance legal and regulatory framework: Malta's legislation goes well beyond Europe's 5th AMLD but there is room to expand/clarify the scope. More specifically, it is not clear whether ATM providers, which are assessed to be highly vulnerable to ML/FT abuse, would fall under the proposed legislation. This point should be clarified in future guidelines. Miners are not currently covered by the VFA Act. In order to close this gap, the MFSA could update the VFA activity framework to include the creation of new coins via mining as a regulated activity. Privacy tokens are growing in popularity and they pose the highest level of ML/FT risk of any virtual asset. Malta should consider carrying out a feasibility assessment regarding the potential costs and benefits of an outright ban on privacy tokens.

Clarify roles and redefine organisational structure: the VFA Act and its guidelines establish clear divisions of responsibility for both private and public-sector entities across market entry elements of the framework. However, more clarity regarding governance and organisational structures could be provided for other parts of the framework. Greater accountability and clearer ownership should be applied to the MFSA, FIAU, MGA and ARB across the framework, but particularly in relation to ongoing supervision of the VFA sector. Authorities should review their governance mechanisms to ensure that they are able to respond to the

ML/FT risks posed by VFAs. Greater emphasis is required on the need to revise organisational structures to account for the new demands and obligations arising from the VFA sector.

Clarify key processes and enhance where required: specific processes need to be laid out for enforcement, investigation, prosecution and recovery of VFAs. The MFSA should improve its core processes (including data and technology) going forward and will need to automate the DD process as far as possible. The authority will also need to enhance the data available for assessments. In additional to these MFSA-specific issues, other processes need to be laid out for enforcement, investigation, prosecution and recovery of VFAs (e.g. the processes of the economic crime unit and the asset recovery bureau).

Upskill stakeholders and deliver necessary data and systems enhancements: the DLT and VFA space will require new skills across competent authorities in order to ensure the risks posed are appropriately mitigated. In order to meet the new challenges presented by the space, competent authorities will not only need to train existing employees on the intricacies of the VFA and DLT ecosystem but also in many cases will need to hire new competencies. Also, in investigating potential crimes, the economic crime unit will need new capabilities and tools. The same applies to the Asset Recovery Bureau, who will need extensive training and enhanced technological capabilities to store confiscated VFAs.

Recommendations for the Private Sector

This section outlines a number of areas for future enhancement and investment that need to be adopted by the private sector. VFAs have a wide range of use cases and give rise to various opportunities for new and existing businesses. Maltese private sector entities can benefit greatly from the emergence of these new business activities and the VFA presence in Malta.

The emergence of VFAs and DLT however also has several implications for the private sector. This risk assessment outlines implications for all Maltese entities as well as for VFA agents specifically. In addition to the actions arising from this risk assessment, the private sector should consider additional steps to mitigate the AML/CFT risks. This section describes these three sets of implications.

The private sector should take a number of actions based on the outcomes of the risk assessment. These implications apply to all Maltese entities, also those entities not currently looking to leverage virtual financial assets. Even though these entities may not be directly involved with VFAs, they may have customers or customers of customers that are. Therefore, all Maltese entities are recommended (in line with all subject persons) to:

- Inform their strategic agenda and decisions with this risk assessment and other sources of information available
- Include information on virtual financial assets in the assessment of clients and products that they are (considering) serving (i.e. as part of onboarding)
- Ensure their processes and controls are effective in preventing abuse through virtual financial assets and services for AML/CFT purposes
- For VFA agents this document serves as guidance to take the actions required to mitigate AML/CFT risks:
- Establish the required skillset to understand, assess and vet virtual asset and service providers through training and / or hiring new personnel
- Collaborate with competent authorities to understand and mitigate the AML/CFT risks of virtual financial assets to ensure that the right controls are in place.

In addition, the private sector should consider additional steps to mitigate the AML/CFT risks of virtual financial assets, specifically upskilling employees and establishing tools to understand, assess and manage virtual financial assets. Besides that, they should increase the collaboration with competent authorities to share first share first-hand insights, discuss good practices, file timely STRs, etc.

6. Additional recommendations

Furthermore, given that the in October 2018 the FATF adopted a series of changes to Recommendation 15, which led to the adoption of a revised Interpretative Note in June 2019 and, in an effort to better set out how the FATF expects jurisdictions to comply therewith, it also issued a revised version of its Guidance for a Risk Based Approach to VAs and VASP ("RBA Guidance"), this section proposes a series of recommended actions to ensure that the domestic framework is better aligned with the said recommendations.

- Determine to what extent, if any, VFA issuers are captured by the FATF's definition of a VASP.
- Consider whether there are any additional services that should be subjected to the current regulatory framework so as to ensure adherence with the definition of VASP provided by the FATF, and in particular with respect to services that fall to be considered as involving a transfer of VFAs. The MFSA has already expressed its intention to look further into the possible extension of the VFA Act to also cover VFA payment services.
- Ensure that the reasons justifying exclusions provided in relation to virtual tokens, private placements etc. are duly documented, bearing in mind possible regulatory changes there may be in relation to the same.
- Consider the challenges that competent authorities and other entities may face in eventually carrying out their functions in relation to this new sector. Law enforcement, prosecution and asset seizure agencies are very likely to face difficulties and in this context recommendations should be made as to any necessary legislative amendments and resources required to ensure that all competent authorities are in a position to exercise their role in as an effective manner as possible.
- Determine on what basis specific exemptions were allowed for under the current legislative and regulatory regime and document the reasons for as much.
- Ensure that the findings of the said document are, to the extent that they may be relevant thereto and allow for dissemination, communicated to the private sector in a manner that is both timely and allows them to make use of the same.
- Set out the necessary policies and procedures to bring to the attention of all competent authorities any developments in this area that may somehow influence the national AML/CFT framework, allowing all the said authorities to consider how any such development will influence their functions at law, and limit as much as possible the ability of the different authorities to take independent action.
- Guidance provided to VFA service providers and issuers be revised to ensure that it makes reference to any additional risk factors referred to in the RBA Guidance. In drafting any additional sector specific Implementing Procedures, the FIAU should ensure that it considers to what extent the sector is exposed to VFAs and, on that basis, provide guidance as to possible risk factors associated with VFAs to which the sector may be exposed to.

- Clear criteria should be set out specific to VFA service providers as to what it entails to have a foreign legal person established in Malta and also as to what is meant to have a VFA service provider offering services in or from Malta or an issuer conducting an offer in or from Malta;
- Set out as a matter of policy how on-going monitoring of the fit and properness test is to be carried out by the responsible authority;
- To the extent that a VFA issuer is determined to be included within the definition of a VASP, it may become necessary to see whether the current application of the fit and properness test is sufficient or whether it requires further streamlining or additional changes;
- Carry out a monitoring exercise to seek data and information as to the possible incidence of entities registered in Malta carrying out VFA services not in or from Malta and, on the basis of the said conclusions, determine whether the situations requiring licensing by the MFSA need to be revised. The same is to be done with regards to issuers of VFAs;
- Ensure that the authorities have the necessary resources and tools to detect the carrying out of unlicensed or unauthorised VFA activity, and are effectively able to sanction for the same;
- Conduct a post-mortem examination of how the MFSA went about enforcing the transitory regime provided for under Article 62 of the VFA Act;
- Finalise the amendments to the VFA Act to ensure that a licence to provide a VFA service or the authorisation to carry out an offer to the public is withdrawn or suspended in the event of AML/CFT breaches or of significant AML/CFT concerns and consider what additional amendments, if any, are required with respect to the VFA Act.
- The FIAU clarifies in more detail what information may be required to be collected and held by a VFA service provider to reconstruct a transaction involving a transfer of funds;
- The authorities continue their engagement with service providers to identify possible solutions that may be used by VFA service providers to comply with the Travel Rule;
- Consider (i) whether action should be taken at the national level to introduce legislation extending the obligations under the Funds Transfer Regulation to VFA service providers as well or if this should be delayed pending action at the EU level; and (ii) what may be the implications of so doing on other regulated service providers due to possible changes to the definition of 'funds';
- It be clarified that any AML/CFT guidance relative to AML/CFT aspects within the VFA area is to be also applicable to anyone carrying out the said activity, even if exempt from licensing, to the extent that the activity is being carried out by way of business to service third parties;
- Highlight as much as possible any ML/FT high risk factors whenever VFAs are used in the context of relevant financial business or relevant activity.
- Initiate a dialogue between the MFSA, the MGA and the FIAU with respect to gaming companies that may be interested in conducting an offer of assets that may be considered either virtual tokens or VFAs, in particular in view of the Sandbox Approach launched by the MGA.
- The creation of a standing sub-committee focusing on the risks and challenges presented by VFAs may be a possible future development to consider. As discussed hereunder, the authorities that may have an interest in this area may be much wider than the spectrum of authorities that was involved in the consultation process carried out prior to the launching of the DLT and VFA legislative and regulatory framework. Through the NCC it would have been possible to carry out the said process in a more structured and focused manner when considering the ML/FT aspect.

- Maltese law does not impose any particular threshold for there to be an occasional transaction in the context of the PMLFTR. Thus, AML/CFT obligations are triggered independently of the amounts involved in, or the value of, a VFA transaction. This decision was taken on the basis that there may arise situations in a VFA-to-VFA transaction where it would not be possible to actually determine the values involved:
    - A VFA might not be listed on an exchange; and
    - Even if listed on an exchange, it is close to impossible to determine the basis on which the value of the VFA concerned is to be determined. Even if an average value is to be taken, the question will arise as to how many valuations is one to consider and whether any criteria are to be met for an exchange's valuation to be taken into consideration.

  Given the above, it is still considered possible to argue that the decision taken by the Maltese authorities is risk-based as it takes into account the possible inabilities to determine the necessary values to trigger the application of AML/CFT requirements – it is not viable to introduce requirements which prove impracticable to implement. Moreover, one has to remark that in the context of funding of terrorism any amount can be problematic and even a USD/EUR 1,000 threshold can be considered as too high, especially in a context where (pseudo) anonymity is especially high.
- A more thorough analysis be conducted as to whether the characterisation of any transaction carried outside of a business relationship as an occasional transaction is justified, or if a threshold should actually be introduced, at least limitedly to transactions involving a VFA-FIAT-VFA exchange;
- Ensure that VFA transfer services are also subject to regulation in terms of licensing and supervision.
- Ensure that the Implementing Procedures – Part II addressed to the VFA sector provide the necessary guidance to subject persons as to how to comply with their obligations at law and include any additional risk factor that may be referred to in the RBA Guidance to ensure that subject persons have as much guidance as possible when it comes to assessing the risks they are exposed to when carrying out their particular activity.
- In terms of the reporting of suspicious transactions or activity, consider whether it would be sufficient to address the issue identified with respect to Regulation 15(3) of the PMLFTR by providing guidance in the Implementing Procedures – Part II to the effect that the term 'funds' is, in the context of VFAs, to be interpreted so as to also include VFAs. The Suspicious Transaction Report template form should also be examined to determine whether any changes are necessary to ensure that it adequately caters also for the VFA sector.

7. Concluding remarks

Malta is thoroughly committed to combating all forms of ML/FT and this document is intended to develop a deeper understanding of the specific risks posed by this new sector. The country has undertaken a comprehensive risk assessment of the VA sector to ensure it remains best-equipped to mitigate ML/FT risks while at the same time embracing the opportunities presented by recent technical advancements. The key results document has the objective of advancing this assessment to enhance the risk-based approach to regulation, supervision and enforcement, and mitigate the ML/FT risks within this rapidly growing part of the economy. Further to presenting the key results document the NCC will be working on the action plan and this will involve a comprehensive exercise involving all the entities. Subsequently, the NCC will

continue to assess whether there was an effective execution of the action plan in order to address the highlighted risks and will continue with its outreach initiatives in order for the entities to be knowledgeable and have a holistic picture of the risks that are ever changing in nature.