VIRTUAL ASSETS
WORKING DOCUMENT

FEBRUARY 2023

COMPILED BY THE VIRTUAL ASSETS WORKING GROUP (VAWG)

Version 1.0

Table of Contents

LIST OF ACRONYMS

VASPs	Virtual Assets Service Providers
FATF	Financial Action Task Force
AML	Anti-money Laundering
CFT	Combating the Financing of Terrorism
VASPs	Virtual Asset Service Providers
CBDC s	Central Bank Digital Currencies
CDD	Customer Due Diligence
OTC	Over the Counter
DeFi	Decentralized Finance
NFTs	Non-Fungible Tokens
BoN	Bank of Namibia
FSC	Financial Services Commission
FIA	Financial Intelligence Authority
FSCA	Financial Services Conduct Authority
IFWG	Intergovernmental Fintech Working Group
CASPs	Crypto Asset Service Providers
SARS	South African Revenue Service
LEAs	Law Enforcement Agencies
CID	Criminal Investigations Directorate
IG	Inspectorate of Government
UWA	Uganda Wildlife Authority
URA	Uganda Revenue Authority
MLA	Mutual Legal Assistance
IMF	International Monetary Fund
UNODC	United Nations Office for Drugs and Crime
UNOCT	United Nations Office for Counter Terrorism
FITSPA	Financial Technologies Service Providers Association

Foreword

The Financial Action Task Force (FATF), a global inter-governmental body that sets international standards in combatting Money Laundering (ML) and Terrorist Financing (TF) made amendments to recommendation 15 that required Virtual Assets (VAs) and Virtual Assets Service Providers (VASPs) to comply with Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) obligations. The said amendment included guidance for the respective jurisdictions to register, license and/or regulate VASPs, and subject them to effective systems for monitoring or supervision by relevant authorities.

Consequently, the Republic of Uganda through the Minister of Finance, Planning and Economic Development amended the 2nd Schedule of the Anti-Money Laundering Act, 2013 in December 2020 to include VASPs as Accountable Persons.

In addition to this endeavour, the Financial Intelligence Authority (FIA) constituted an in-house Virtual Asset Working Group (VAWG) in October 2022 to study VAs, VASPs including other related emerging technologies and identify emerging threats in order to propose appropriate measures that will mitigate them. In recent years, relevant Law Enforcement Agencies and Regulatory Authorities in Uganda have noted that VAs have slowly gained acceptability, and many sector players including the general public have begun to diversify in opportunities for VA associated investments. Whereas this popularity and public adoption of VAs in Uganda may have created opportunities, FIA as a body mandated to combat ML/TF threats found it necessary to have its position known to all key stakeholders.

FIA through the VAWG has, in its quest to effectively execute its mandate developed a Working Guide/Document as an outline of the many interventions it needs to undertake, some in collaboration with regulatory bodies, or law enforcement agencies and/or accountable persons. In this regard, FIA commits to taking a center stage in preserving the financial integrity and improve Uganda's reputation and comply with FATF recommendation 15 as well as play a role in protecting its citizens from the threats posed by VAs.

I wish to express my sincere appreciation to all members of top management at FIA and members of the VAWG for their invaluable contribution to this working document, and further encourage them to uphold the same spirit towards this vital task of protecting the integrity of Uganda's financial system.

Mr. Cyrus K. Barigye CISM, CDPSE, CAMS
Chairperson, Virtual Assets Working Group, FIA

1.0 Background

The last decade has seen a phenomenal rise in the number of new digital instruments promising easier, faster, and cheaper global payments and transfers. These digital representations of value and contractual rights comprise a broad (and expanding) category of assets. Common market place terms referencing such new products include cryptocurrencies, digital currencies, crypto assets, virtual assets, all describing systems of storing/capturing value and rights in digital form. Some of the most well-known digital assets rely on cryptographic technology to secure transactions and control the creation of additional units, underpinned by distributed ledger technology (DLT), such as blockchain, to construct a ledger (or a database) that is maintained across a network. The first of these instruments— Bitcoin—was launched in 2009. Since then, thousands of cryptocurrencies have been issued, with varying degrees of success. As of September 19, 2021, with a capitalization of at least US$1.97 trillion (for the top 101 cryptocurrencies) and, for a dozen of them, a daily turnover of more than US$1 billion, cryptocurrencies now represent a small but not negligible portion of financial markets. This space is characterized by the speed at which different types of assets and business models are created, as well as their complexity. This includes stablecoins with the potential for mass adoption. In line with the terminology set by the Financial Action Task Force (FATF), the internationally recognized standard setter for anti-money laundering and combating the financing of terrorism (AML/CFT), this note refers to these new instruments as Virtual Assets (VA) and to the new actors as Virtual Asset Service Providers (VASPs). The FATF definition of VA explicitly excludes digital representation of fiat currencies, securities and other assets that are covered elsewhere in the FATF standards. For this reason, national digital currencies, including central bank digital currencies (CBDCs), while they may, in practice, share some similarities with VAs, are not discussed in this note.

VAs offer many potential benefits. As noted in the IMF's earlier publications, these include greater speed, lower cost and increased efficiency in making payments and transfers, including across borders, with the potential to improve financial inclusion. DLT offers potential benefits that go far beyond VAs. Many countries across the world are currently looking into leveraging this new technology to issue domestic "currency" in virtual form—CBDCs. At the same time, however, VAs are susceptible to criminal abuse. Some of their features—in particular their varying degrees of anonymity or pseudonymity— raise new challenges for competent authorities. Criminals have misused these features to facilitate fraud, theft, money laundering (ML) and terrorist financing (TF), amongst other crimes. Without strong mitigation, VAs can pose a significant threat to the integrity of the global financial system. ML, related predicate crimes, TF, and the financing of the proliferation of weapons of mass destruction (PF) can all be facilitated with VAs and can all have

1. See IMF Staff Discussion Note "Virtual Currencies and Beyond: Initial Considerations" (2016)
2. See https://coin.dance/stats and https://coinmarketcap.com/
3. The FATF is an inter-governmental body established in 1989 to set standards and promote effective implementation of legal, regulatory, and operational measures for combating ML, TF and PF.
4. The FATF standards comprise the 40 Recommendations, their Interpretive Notes, and the accompanying Glossary

serious economic consequences. Preserving the integrity of the global financial system is a necessary aspect of ensuring financial stability, sustainable growth and inclusive economic development. Effective anti-money laundering and combating the financing of terrorism (AML/CFT) frameworks are crucial in that respect.

In June 2019, the FATF finalized amendments to its global standards to clearly impose AML/CFT requirements on VAs and VASPs. In June 2020, it noted that while progress was being made in the implementation of its new standards by the public and private sector, considerably more effort was needed. The FATF conducted a second 12-month review of the implementation of its new standards in June 2021 and added new updates such as the travel rule guidance for VASPs.

This document explains why VAs are vulnerable for misuse for ML/TF/PF purposes and clarifies which assets and service providers should be subject to AML/CFT measures. It discusses the measures that Uganda should take, and the type of action necessary in instances of criminal misuse of VA.

5. On legal issues pertaining to CBDC: see Bossu, W., Itatani, M., Margulis, C., Rossi, R., Weenink. H., and Yoshinaga, A., Legal Issues of Central Bank Digital Currencies: Central Bank and Monetary Law Considerations, IMF, WP/xx/20.

6. See for example Bali Fintech Agenda, IMF Policy October 2018 and January 2016 Staff Discussion Note "virtual Currencies and Beyond: Some Initial Considerations" (SDN/16/03).

7. These are the underlying offenses that generate illegal proceeds to be laundered. Pursuant to the FATF standards, the ML offense should apply to all serious offenses, with a view to including the widest range of predicate offenses. At a minimum, it should apply to the 21 categories of offenses in the FATF glossary (e.g., fraud, drug trafficking, corruption and bribery, and tax crimes)

8. See https://www.imf.org/en/Publications/Policy-Papers/Issues/2019/02/04/pp101718-2018-review-of-the-funds-aml-strategy

2.0 VA AND VASP DEFINITION

2.1 Virtual Assets (VAs)

According to the FATF, the term 'Virtual Asset' refers to "any digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes." VAs do not include digital representations of fiat currencies, securities, and other financial assets.

VAs have technological properties that enable pseudo-anonymous and anonymous transactions, fast cross-border value transfer and non-face-to-face business relationships. Those properties have the potential to improve multiple financial products and services such as trade financing, cross-border payments and financial instrument settlement.

International typologies related to VAs show that organised crime organisations may use them to access 'clean cash' (paying in and paying out). Not only cybercriminals use VAs – other organised crime groups such as drug traffickers use them to move and launder the proceeds of crime. VAs allow such groups to access cash anonymously and obscure the transaction trail. Criminals may acquire private keys for e-wallets or withdraw cash from cashpoint machines.

VAs, such as Monero, are designed as privacy coins to obfuscate the identities of the sender, the recipient, and the transaction itself. These VAs directly confront customer due diligence (CDD) measures and therefore are particularly appealing to criminals. Transactions using mixing and tumbling services, infer attempts to obscure illicit funds flows between wallet addresses and darknet markets.

9. There are instances where anonymity can be introduced e.g. through the use of private wallets / privacy coins, this is an exception rather than the norm. In instances where private wallets are not used, the beneficiary / sender can be identified through aspects like the Travel Rule. Also, all transactions are recorded on the blockchain, which means they can be traced using the appropriate tools

2.1.1 Types of Virtual Assets (VAs)

Type of VA	Category	Description
Utility Tokens	VAs that grant digital access to specific digital platforms and to current or planned products or services. Typically, only accepted by the issuer or other users of a particular digital platform. Examples: Filecoin (FIL), Civic (CVC)	Utility tokens may resemble vouchers and typically only offer holders access to certain platforms or products, meaning that these types of tokens are not easily traded. Utility tokens are not considered to provide an efficient mechanism to exchange or realise value, making them unattractive to criminals to launder illicit funds or fund terrorism.
Payment/exchange tokens	VAs that can be used as digital means of payment or exchange, subcategories include:	
	Pseudo-anonymous: used as a means of exchange or potentially as a store of value. Transactions are linked to a specific sender. Examples: Bitcoin (BTC), Litecoin (LTC)	Transactions with pseudo-anonymous VAs are linked to a wallet address; however, the address may not be linked to an individual. Given that transactions with pseudo-anonymous VAs are stored in the blockchain and provide a full audit trail of VA movements (where other anonymisation techniques are not employed), these types of VAs present a medium risk of ML/TF.
	Anonymous (privacy coins): VAs with inbuilt anonymity features. Used as a means of exchange or potentially as a store of value. Transactions are not linked to a specific sender. Examples: Monero, Dash, ZCash	Privacy coins prevent third parties from linking a VA wallet to an identity. Although privacy features are not always sought to undertake illicit activity, criminals favour anonymous VAs which make their exposure to ML/TF higher than other types of VAs.
	Platform: used to access digital marketplaces and platforms. Also used as a means of exchange and potentially as a store of value. Examples: Ethereum (ETH), ERC20 tokens	

	Asset-backed tokens (also known as stablecoins): VAs that purport to maintain a stable value by referencing more than one fiat currency, a commodity, or a basket of commodities and fiat currencies. Examples: Tether Gold (XURt)	Transactions with platform tokens are linked to a wallet address which is normally linked to an individual. These types of VAs present higher levels of usability than other VAs as they can facilitate transactions between platforms, and, as a result, offer higher liquidity.
	Fiat-backed tokens (also known as stablecoins): VAs that purport to maintain a stable value by referencing a single fiat currency. Examples: Tether (USDt)	Stablecoins offer high usability when compared to other VAs, which makes them attractive from an ML/TF perspective as they can be exchanged and transferred more easily than other tokens. Some stablecoins also have the potential for mass adoption, increasing their exposure to ML/TF risks.
Closed-loop tokens	VAs used as a means of exchange within a closed system. Examples: World of Warcraft gold (video games)	Closed-loop tokens can only be used within a specific virtual community and cannot be exchanged for other virtual assets or fiat. Their limited usability makes them unattractive as a means to launder illicit funds or to pay for illegal goods.

2.2 Virtual Asset Service Providers (VASPs)

In exercise of the powers conferred on the Minister responsible for Finance, Planning and Economic Development by section 139 of the Anti-Money Laundering Act, 2013, and in consultation with the Financial Intelligence Authority Board, and the approval of Parliament, the Second Schedule to the Anti-Money Laundering Act, 2013 was amended by Parliament on November 20, 2020 to include Virtual Asset Service Providers (VASPs) as Accountable Persons. The Statutory Instrument was published in the National Gazette, vide Vol. CX111 No.77 on November 27, 2020.

In the amendment, Virtual Asset Service Providers, are defined to include, a natural or legal person who conducts one or more of the following activities for or on behalf of another natural or legal person;

(i) The exchange between virtual assets and fiat currencies;

(ii) The transfer of virtual assets;

(iii) The safekeeping or administration of virtual assets or instruments enabling control over virtual assets; and

(iv) The participation in or provision of financial services related to an insurer's offer or sale of a virtual asset.

Based on the above description, peer-to-peer transactions are also included in the scope of VASPs since one peer (natural person) may exchange VAs or fiat with another peer (natural person).

2.2.1 Types of VASPs

Type of VASP	Category	Description
Wallet providers/ custodians	Service providers enabling the storage of public and private keys	VA custodians are most vulnerable to ML/TF risks at the time of deposits and withdrawals in VAs as it is often challenging to verify that the assets are being deposited or withdrawn from addresses owned or controlled by the customer. Nevertheless, custody services alone do not offer an effective means to transfer illicit funds, for which the inherent risk stemming from this service has been rated as low risk.

Exchanges	Service providers facilitating virtual asset transfers and exchanges (VA - fiat / fiat - VA / VA - VA).	Centrally operated exchanges offering fiat-VA, VA - fiat or VA - VA exchange services are exposed to ML/TF risks as criminals may attempt to use these platforms to place, layer, and integrate the proceeds of crime. Nevertheless, the volumes exchanged through centralised exchanges tend to be small or medium, and in most cases, trading is done using an orderbook, which minimises opportunities for coordination between criminals.
Payment processors & brokers, including orderbook exchanges & OTC desks	Service providers conducting payment processing / arranging transactions.	**Payment processors and brokers**, including orderbook exchanges: Trades against order books tend to be smaller when compared to trades via OTC desks and fiat deposits and withdrawals are normally only accepted from/to a bank account in the customer's name. Deposits and withdrawals in VAs present a higher risk, but given that transaction amounts tend to be smaller, the ML risk presented by these types of entities is usually low.
		OTC desks: Volumes traded on OTC desks tend to be higher than those traded using an order book. With higher liquidity levels and a wider range of VAs available to trade, institutional investors, hedge funds, and other large players trade using OTC desks rather than exchanges. OTC desks also offer higher anonymity and may facilitate one-off transactions that do not require the establishment of a business relationship.

Asset management providers	Entities offering fund management / fund distribution.	Asset managers may facilitate access to VA investments as part of their fund management services. Asset managers will not be classified as VASPs unless they offer any of the five activities defined by the FATF as VASP services and who are not covered elsewhere in the regulatory regime. In terms of exposure to VAs, these types of entities are a step removed in the value chain, as they will typically access VAs via a VASP.
		Investing in funds may not be an attractive option to launder the proceeds of illicit activity as they tend to be longer-term strategies that do not offer an effective mechanism for criminals to layer funds and access them immediately. Where those strategies are not longer-term, the risk of this structuring being attractive or utilised to launder the proceeds of illicit activity may not be managed as effectively. There is a risk that asset managers may purchase VAs from unregulated exchanges, or exchanges with lax customer due diligence requirements. Also, one-off large transactions may increase the risk of ML; however, regulated asset managers are more likely to only deal with regulated exchanges.

Issuers	Entities issuing and selling VAs to the public.	Although newly issued tokens may not offer a practical means to launder illicit proceeds, weak controls or lacking AML/CFT processes by issuers may allow criminals to purchase these tokens using criminal proceeds and hold them as a speculative investment. Newly issued tokens that are not easily converted into fiat or other VAs may not be attractive to criminals.
Investment/trading platforms	Entities enabling investment in or the purchase of VAs via a managed investment scheme or a derivatives issuer providing VA options, or via a private equity vehicle that invests in VAs.	Investment/trading platforms acting as an intermediary between their customers and either financial institutions (such as asset managers), or VASPs (such as exchanges or VA trading platform operators) are exposed to a low risk of ML/TF. Deposits by customers of these types of entities are normally only accepted if made from bank accounts under the customer's name, meaning that the funds reaching the investment/trading platform have already gone through AML/CFT checks by the bank. As with asset managers, the degree of separation between these types of entities and the VAs also decreases their exposure to ML/TF risks presented by the VAs they enable investment in.
Not covered by FATF Recommendations		
Miners/validators/pool operators	Entities that validate and confirm transactions on a distributed ledger. Although not usually captured by the VASP definition, if they hold sufficient control/validation power, they could be considered VASPs	These types of entities present a low risk of ML/TF given that these activities do not provide an effective mechanism to launder the proceeds of crime or fund terrorist activities. It should be noted that there are reports of State actors trying to use VA mining as a means to evade international sanctions.

Technology and ancillary service providers	Entities offering mixing services, blockchain explorers, web administration, mining hosting services, information providers	Technology and ancillary service providers are exposed to a low risk of ML/TF given that they are not involved in VA fund flows.

The FATF has highlighted that the wide range of providers in the virtual assets space and their presence across several jurisdictions can increase the ML/TF risks associated with VAs and VA financial activities due to potential gaps in customer and transaction information. This is a particular concern when the following risk elements are present:

a) Transactions are cross-border;

b) There is a lack of clarity on which entities or persons (natural or legal) involved in the transaction are subject to AML/CFT measures;

c) There is a lack of clarity regarding which countries are responsible for regulating (including licensing and/or registering) and supervising or monitoring those entities for compliance with their AML/CFT obligations; and

d) Lack of a well aligned legal framework and regulations in countries as this introduces the risk of consumer protection, as well as exchange control regulation.

Further, if a VA achieves sufficient global adoption by customers such that it is used as a medium of exchange and store of value without the use of a VASP or other regulated financial institution, the lack of AML/CFT controls and compliance monitoring could mean the VA is at high risk of ML/TF abuse.

2.3 Highlights of the FATF Interpretative Notes

2.3.1 VASPs should be treated like general Financial Institutions

- VASPs should complete risk assessments of their client base to determine risk;
- VASPs should have suitable policies and procedures for:
    - Know Your Customer (KYC)
    - Anti-Money Laundering (AML)
    - Countering the Financing of Terrorism (CFT)
- Increasing due diligence will provide greater access to the financial system as virtual assets become more mainstream.

2.3.2 Financial Institutions (FIs) can manage the risk of VASPs

- FIs must complete due diligence on VASPs as well as any parent companies or ultimate beneficiary owners;
- FIs must also review the VASPs screening and onboarding process as well as put in place transaction monitoring and regulatory reporting processes and controls.;
- FIs should treat VASPs like correspondent banking clients

2.3.3 It is essential to implement appropriate technology controls

- Monitor digital identities (comprised of devices like computers and phones);
- Authenticate physical IDs (e.g. passports);
- Comply with AML/CFT legislation requirements;
- Screen identities for risk related to sanctions, enforcements and PEP status; and
- Continuous monitoring of customers' risk profile and real-time risk-based authentication throughout the customer life cycle.

3.0 INTERFACE BETWEEN VIRTUAL ASSETS AND TRADITIONAL FINANCIAL SYSTEM

For the purposes of this document, it is important to understand the interface between virtual assets and the traditional financial system. As mentioned above, secondary markets for non-convertible virtual assets exist. The primary source of non-convertible currencies is the central administrating authority for the particular virtual currency in question. Secondary markets for non-convertible currencies, such as online auction sites, may accept a wide range of funding sources, including convertible virtual assets. The purpose of this section, however, is to focus on the ways in which primary trade in convertible virtual assets is funded. In other words, the ways in which it is possible to convert between virtual assets and fiat currencies, goods, services or other representations of value.

3.1 Virtual Asset Exchanges

Convertible virtual currencies are commonly traded on virtual currency exchanges, with different exchanges available for trading different virtual currencies. A mix of fixed fee and percentage commission pricing structures are used by the virtual currency exchange for their exchange services. Additional fees may be charged for depositing and/or withdrawing funds from the virtual exchange account. The range of available funding sources and withdrawal destinations for virtual currency exchanges vary but some examples include; Bank transfer, Money Service Business, Payment card, Cash, and other online payment operators such as PayPal.

Considering the relatively unregulated nature of this market, a risk exists that virtual currency exchanges do not properly identify the source of cash or third-party funding used

to purchase virtual currencies. In the recent past, several countries have announced plans to regulate virtual asset intermediaries, such as currency exchanges, to combat the risks of money-laundering associated with them.

3.2 Financial Institutions

As mentioned above in Section 3.1, a bank account can act as a funding source for purchasing virtual asset or as a destination for exchanging virtual assets for fiat currency. As such, all of the typical regulatory and supervisory measures that are in place relating to the use of bank accounts would be applicable. However, as highlighted elsewhere, the use of money mules to facilitate laundering of crime proceeds using various techniques on the Internet, including virtual assets, can present challenges.

Virtual asset exchanges themselves will also interface with the financial system to hold and/or transfer fiat currency. The legal and regulatory implications of this fact continue to evolve.

3.3 Cash/ATMs

The use of cash has always been attractive in the laundering of crime proceeds. Therefore, the interface between virtual currencies and cash warrants particular attention. The awareness and popularity of virtual asset has substantially increased in recent years, particularly with the advent of Bitcoin. Following on from this growing popularity, novel business models have emerged in the case of Bitcoin that offer possibilities were not historically available with other virtual currencies. For example, Bitcoin ATMs are available in a number of countries as near as Kenya. Such ATMs allow buying and selling of bitcoins for cash.

3.4 Merchants Accepting Virtual Assets

Another effect of the increasing popularity of VAs is that an increasing number of merchants/businesses are accepting payments in virtual assets, most notably with bitcoins. VAs is an attractive option for merchants for the following reasons;

a) Once confirmed, VA transactions are irreversible therefore there is limited possibility of chargebacks or other fraud losses that can occur when using payment cards.

b) The fees associated with processing VAs are lower than payment card acquiring fees.

As well as merchants accepting VAs, there is a growing ecosystem of merchant services that are available to assist small businesses to configure and accept VA payments.

4.0 THREATS AND VULNERABILITIES ASSOCIATED WITH VAs

While generally used for legitimate purposes, VAs have also been misused to serve nefarious goals. Some cases of large-scale fraud, theft, ML, and other crimes using VAs have involved millions of U.S. dollars' worth of illegal proceeds. The exact extent of misuse of VAs around the globe is unclear, but so far appears to be smaller in volume and frequency than misuse of traditional financial services. Some firm-specific estimates as well as estimates issued by some regional agencies indicate that criminals still favor traditional assets. But they also reveal that the misuse of VAs is not negligible and is rapidly increasing. Several factors make VAs potentially attractive to criminals. They notably include the following:

4.1 Potential for greater anonymity and availability of anonymity enhancing features.

In many cases (e.g., Bitcoin), transactions are visible online and traceable from one wallet to another. But linking a particular address or wallet to a specific individual is challenging. This challenge is compounded by the availability of mechanisms designed specifically to hinder the traceability of flows. They include anonymity enhancing features (such as mixers and multiple layers of encryption, stealth addresses and ring signatures) that limit the information available, including regarding the value and counterparties of a transaction. Some also obfuscate identification through secondary information (e.g., by preventing the identification of the IP addresses, geolocation data, device identifiers, and transaction hashes).

It is important to note that VASPs are responsible for identifying their customers and for linking wallet addresses to customers, and the introduction of the Travel Rule by FATF significantly mitigates the risk of anonymity. Furthermore, tools such as Chainalysis assist in identifying mixers which could lead to risk-based decision making. Although the risk of anonymity is present, there are mitigating factors that can be implemented by the industry. Also, tools are available to manage the risk of geolocation such as GeoComply which enables the identification of VPNs and can provide additional information (over and above IPs), like GSM, GPS and Wifi location.

10. For example, the Silk Road Case, AlphaBay, and the Wannacry ransomeware attack. While these cases ultimately resulted in successful law enforcement action, success remains rare.

11. 12-month Review of The Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, FATF, 2020

4.2 Non-face-to-face activities.

VAs-related activities are conducted online and are generally not in the same physical location. This complicates the identification of the customer during the onboarding process or at the time of transactions and increases the risk of forged or inaccurate identification information being provided. Although some conventional financial services also allow non-face-to-face onboarding and transactions, the anonymity feature of VA activities could exacerbate these challenges.

4.3 Potential for decentralization and fragmentation of near instant global services.

The fast-moving nature of VAs provides an opportunity to quickly exchange between different VAs for a more sophisticated disguise of the origins of funds in a cross-border context. VASPs can have a physical presence in one jurisdiction, be registered in another, place their server in yet another (or multiple others), and provide services globally without the need for a central center of command. This complicates the prevention of illegal transactions and the analysis of financial intelligence derived from suspicious trans action reports as case information can be fragmented across different countries. It also complicates law enforcement action as there is generally no single entity to investigate and target.

4.4 Uneven application of domestic AML/CFT measures.

Most countries are still in the early stages of implementation of the relevant FATF standards, which creates significant potential for regulatory arbitrage, thus providing opportunities for criminals to exploit VASPs domiciled or operated in countries with nonexistent or minimal VA and VASPs AML/ CFT regulations.

Ultimately, the factors highlighted above pose significant challenges to domestic authorities as well as to VASPs. They hinder the effective implementation of the AML/CFT preventive framework, and of law enforcement action.

12. For example, a VPN or an anonymized overlay network (e.g., Tor), which encrypts and routes communications through multiple computers can be used to mask Internet activity. Software to emulate an operating system within a user's operating system, with operations of the virtual machine encrypted, is also available.

5.0 LEGAL AND PRACTICAL CONSIDERATIONS FOR AN EFFECTIVE VAs AML/CFT SYSTEM

5.1 Milestones by FATF in Virtual Assets Regulation

In 2018 and 2019, the FATF adopted changes to its standards to explicitly apply them to the virtual context and provided additional tailoring where necessary. As is the case with traditional assets, the mitigation of the ML/TF/PF risks related to VAs therefore requires several steps, starting with a risk assessment as well as a review and commensurate tailoring of the existing legal and institutional framework. Mitigation also requires the active, ongoing participation of the private sector (VASPs, in particular and unless VA activities are prohibited, but also financial institutions and DNFBPs as defined by the FATF) and of a range of governmental agencies (e.g., policy makers, AML/ CFT supervisors, financial intelligence units, FIUs, and law enforcement agencies, LEAs).

In June 2022, FATF produced a targeted update on implementation of its Standards on VAs and VASPs, with a focus on FATF's Travel Rule. The report places a specific focus on FATF's Travel Rule to respond to FATF's June 2021 findings that countries and private sector face particular challenges in this area. Further, the report includes relevant emerging risks and market developments, including on Decentralized Finance (DeFi), Non-Fungible Tokens (NFTs) and unhosted wallets.

The report finds a continued need for many countries to strengthen understanding of ML/TF risks of the VA and VASP sector, and to rapidly implement FATF's R.15/INR.15 to mitigate such risks. In particular, FATF's Travel Rule requires VASPs and other financial institutions to share relevant originator and beneficiary information alongside virtual asset transactions, therefore helping to prevent criminal and terrorist misuse.

The report finds that jurisdictions have made only limited progress in implementing this requirement. Of the 98 jurisdictions that responded to FATF's March 2022 survey, only 29 jurisdictions have passed relevant Travel Rule laws, and a small subset of these jurisdictions have started enforcement. This demonstrates an urgent need for Uganda to accelerate implementation and enforcement to mitigate criminal and terrorist misuse of VAs.

5.2 Milestones by ESAAMLG Countries in Virtual Assets Regulation

5.2.1 Republic of Namibia

As at October 2022, the Bank of Namibia (BoN) included virtual assets and virtual asset service providers under its fintech innovations regulatory framework. There are plans to amend applicable laws and regulations. According to the central bank's governor, there is an ongoing "battle between regulated and unregulated money on the one hand and sovereign versus non-sovereign money on the other." BoN believes that while cryptocurrencies have

13. Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins, FATF, 2020.

no legal tender status in the country, it has now brought "virtual assets (VA) and virtual assets service providers (VASP) under its Fintech Innovations Regulatory Framework in a phased approach, through its innovation hub." BoN is also considering amending "applicable laws and regulations diligently in consultation with other relevant authorities."

BoN also clarified that even though privately issued digital currencies are still not legally recognized, merchants and traders can accept payment in this form provided they are "willing to participate in such an exchange or trade."

5.2.2 Republic of Mauritius

In September 2018, via a guidance note, the Financial Services Commission (FSC) of Mauritius recognised digital assets as an asset-class for investment by sophisticated and expert investors.

In the first quarter of 2019, the FSC published the Financial Services (Custodian services (digital asset)) Rules 2019 (CDA Rules 2019) to regulate the safekeeping of digital assets. Following queries from stakeholders requesting clarification on the regulatory approach in relation to security token offerings, a second guidance note was issued by the FSC.

In mid-2020, a third guidance note was issued by the FSC outlining a common set of standards for Security Token Offerings and providing for the licensing of Security Token Trading Systems.

In February 2021 the FSC issued a consultation paper on the introduction of a regulatory landscape for the Fintech Service Provider (FSP) licence to establish a supervisory regime for providers of technology services looking to establish a commercial presence and operate in or from Mauritius.

These developments culminated in Parliament passing the Virtual Asset and Initial Token Offering Services Act 2021 (Act), at the end of 2021. The Act was prepared in line with international standards to strengthen the development of key sectors and encourage innovation in fintech and regtech. The Act provides a comprehensive legislative framework for virtual asset service providers (VASPs) and issuers of initial token offerings (ITOs). It was passed by the Mauritius National Assembly on 10 December 2021, was gazetted on 16 December 2021 and came into force by proclamation on 7 February 2022.

It is also relevant to note that, as a safeguard against risks associated with fast evolving technologies involving virtual assets and initial token offerings, the Act, in compliance with the Financial Action Task Force's standards, includes provisions to mitigate the risk of money laundering, financing of terrorism and the proliferation of such related risks.

5.2.3 Republic of South Africa

The crypto regulatory landscape in South Africa is still in a state of uncertainty. While the Financial Services Conduct Authority (FSCA) is yet to implement any regulations, the regulator's sentiment towards crypto regulations has evolved to the point that we can now expect some regulatory framework in the not so distant future. This movement has been bolstered by the growing concern of customer protection in the wake of South Africa's $4 billion in crypto scams.

The Intergovernmental Fintech Working Group (IFWG) published a position paper on crypto assets on 11 June 2021, confirming that crypto assets will be brought into the SA regulatory purview. The paper provides 25 recommendations in relation to the following three pillars of regulation:

- Implementation Anti-money laundering (AML) and counter-terrorism financing framework'
- A framework for monitoring cross-border financial flows; and
- The application of financial sector laws.

Attention around looming crypto regulations in South Africa has recently been brought to the fore by South Africa's leading crypto exchange, Luno. Experts are likely to see an amendment to the FIC Act to bring crypto service providers into the purview of the Act, and it is a much-needed regulatory step to ensure consumer protection with a robust licence regime. The position paper shares a similar sentiment, and has highlighted the following five recommendations that are likely to be implemented within the next 12 months.

- Crypto asset service providers will be regarded as CASPs.
- Schedule 1 of the FIC Act is to be amended by adding CASPs to the list of accountable institutions. This means CASPs will need to register with the Financial Intelligence Centre.
- Crypto assets will be declared as a "financial product" under the FAIS Act.
- Certain crypto asset services will be included in the relevant licensing activities under the CoFi Bill and included in the definition of "financial service" in the Financial Sector Regulation Act (FSRA).
- The pooling of crypto for distribution should be treated as an alternative investment fund that should be incorporated within the relevant licensing activities in terms of the Conduct of Financial Institutions Bill. Collective investment schemes and pension funds should not be allowed to have exposure to crypto assets. Also, the issuing and listing of derivative instruments or other securities that reference crypto assets as the underlying assets should not be permitted.

The position paper identified that one of the objectives of regulating crypto assets is to combat tax evasion and impermissible tax avoidance arrangements. The South African Revenue Service (SARS) has confirmed that normal income tax rules apply to crypto and taxpayers need to submit their crypto gains or losses as part of their taxable income. A crypto asset can also be subject to capital gains if it is held and disposed of with capital intent.

There is also a clear stance on VAT in that the dealing in crypto assets itself does not give rise to VAT. However, services related to such dealings may well give rise to VAT if the VAT registration threshold is met.

The 2022 Budget Review referred to crypto assets in the financial sector update. A project is underway that is seeking to clarify the relevant operational, legal and policy questions around a potential change to the adoption of a digital central bank digital currencies (CBDCs) and crypto asset regulations. The project findings are expected to be released in April 2022.

The review also indicated that the national treasury continues to modernise South Africa's capital flows management framework. In this context, a reform is proposed to enhance the monitoring and reporting of crypto asset transactions to comply with the exchange Control regulations of 1961. The process to include crypto assets in the regulations is underway.

South Africa's mission towards implementing crypto regulations remains a slow and uncertain journey. Regulation in the crypto industry is essential to ensure that this new technology goes mainstream. Amongst the many benefits, the most noteworthy is customer protection. For cryptocurrency platforms, regulation is also important because it lays the foundation to develop key relationships, such as with banking institutions.

5.3 Areas Uganda needs to Focus on within the Virtual Assets Space

In light of the often cross-border nature of VA-related activities, including criminal activities, it also requires extensive dialogue and cooperation with foreign counterparts. Some action is required from all countries. Ultimately, countries are free to regulate or prohibit activities in VAs. But all must take some action. Even if Uganda prohibits the activities of VASPs within the regulated sectors, it must still assess the ML/TF/ PF risks associated with VAs, and undertake corresponding measures, as well as act to enforce that prohibition. It must also adopt risk mitigation strategies that account for the cross-border element of VA activities, and cooperate with other countries as needed. The following focuses on those actions that Uganda should consider;

5.3.1 Risk Assessment

5.3.2 Legal Foundation

Adapting to a world in which VAs exist may require updating a country's legal framework. The need for updates will vary on a case-by-case basis and will require a number of steps:

(i) An ex ante (future) policy discussion of the type of approach that a country wishes to implement to mitigate the risks. Some countries have taken a decision to ban VA-related activities (e.g., due to a lack of appropriate resources to regulate the sector); others have opted to regulate AML/CFT activities.

(ii) Regardless of the option chosen, a review of the legal framework is necessary to establish the breadth of the legal and regulatory changes needed (e.g., a ban would need to be in law or other enforceable means to ensure that unauthorized activities can be detected and sanctioned).

(iii) Further, a review of the criminal law framework is necessary to ensure that it allows for effective enforcement action (both of a ban and of criminal misuse of VAs). Regardless of their extent, effectively implementing the amendments to the legal framework, requires countries to adopt practical measures and take necessary policy considerations (e.g., to identify and address misuse of VAs and illegal activities of VASPS, the ability to freeze and seize VAs as discussed further below).

5.3.3 Legal Framework for Preventing and Sanctioning ML and TF

Uganda's legal framework should adequately criminalize ML and TF activities that involve VAs. Given that VAs are just another representation of value, they should be captured to the same extent as traditional assets. As a result, both the ML offense and the TF offence should apply, regardless of whether traditional assets or VAs are involved. This applies in all cases, including when Uganda has chosen to ban or restrict VA activities within its territory. In many countries, it is likely that the ML and TF offenses already apply, but in others, this may require amendments to the relevant criminal laws.

Further legal or regulatory changes may be needed to facilitate enforcement actions. Examples of such changes include a broadening of provisions related to customs declarations, international cooperation, or LEA's ability to conduct investigations (e.g., to provide for additional investigative powers specific to VAs), as well as provisions related to freezing/seizing, including in the context of implementation of targeted financial sanctions, confiscating, and management of proceeds of crime, among others.

14. This is notably due to the fact that the FATF standards have long required that the ML and TF offenses also apply to "incorporeal assets" and to "funds and other assets" which should include VAs.

5.3.4 Financial Intelligence

Some adjustments to existing practices may be needed to ensure appropriate receipt and analysis of financial intelligence. The Financial Intelligence Authority may wish to revise its templates for reporting to capture additional transaction and customer information specific to virtual asset transactions (e.g., wallet account information), transaction details (including transaction hash and information on the originator and the recipient), login information (including IP addresses), and mobile device information. These features are available in the goAML system. FIA will also need to have a solid understanding of how transactions operate in the virtual asset space, including in instances where enhanced anonymity features are involved, and the diversity of different types of VAs used for criminal purposes.

In addition, FIA will need to be able to conduct operational and strategic analysis based on the information received from VASPs and other reporting entities, thereby building networks of potential subjects and identifying financial transactions that may be indicative of ML/TF/PF activity for sharing with appropriate law enforcement authorities to facilitate investigation. Acquisition of an automated investigative tool such as Chain Analysis is vital.

5.3.5 Investigations and Prosecution of Criminal Activities in the Virtual Assets Space

LEAs particularly CID, IG, UWA, and URA need to be able to pursue investigations related to VAs and VASPs. Responsibilities and powers of investigation should notably include compulsory measures for the production of records held by VASPs and for the freezing or seizing of VAs. While many traditional investigative skills remain useful, they may not be entirely sufficient to deal with VAs, and LEAs may need to develop new skill sets related to conducting investigations online (e.g., ability to use monitoring/ screening tools to trace VA transactions, searches of cell phones and computers, where permitted).

As a starting point, Uganda should consider whether they have adequate expertise (e.g., investigators specialized in cybercrimes or Vas, among others). In many instances, specific training will be useful (e.g., on conducting investigations online, with a focus on identifying VAs and related transactions on the blockchain, and simulation trainings to understand the use of the darknet). In many cases, this might require strengthening interagency cooperation, developing special units with the relevant tech expertise, and ensuring adequate dialogue with foreign counterparts. Some technological solutions can assist with investigations. In addition to having a solid understanding of VAs, the DLT and the measures used to obfuscate the traceability of VA transactions (e.g., mixers), LEAs should also be aware of the new analysis tools available. For example, blockchain explorers are proving useful to investigators as they facilitate blockchain analysis by enabling searches related to addresses, transactions and other details on the basis of records maintained by the DLT. Certain firms now specialize in collecting and analyzing transaction data across VA networks. LEAs may therefore consider deploying additional technological

solutions to help with their analysis. Prosecutors and judges will also need to develop their understanding of VAs and VA-related activities. In most instances, given the specific nature of VAs and manner in which VASPs operate, this will most likely require enhanced training of prosecutors and the judiciary to ensure that they are able to understand the technological evidence and legal framework for VAs and VASPs in order to handle cases appropriately.

5.3.6 Seizing, Freezing, Confiscation, and Management of VAs

Where warranted, tainted VAs should be subject to freezing or seizing and confiscation. The circumstances that lead to such measures are likely to be the same as for traditional assets, but the modalities may need to be tailored to the virtual asset space.

5.3.6.1 Seizing/Freezing

In order to seize VAs, LEAs typically need to identify both the public and private keys related to VAs and have applications that manage the keys, recovery seeds, and/or VA wallet files. This may require specialist investigative skills and the use of different types of technologies. Given the highly mobile nature of VAs (e.g., any individual with knowledge of a subject's private keys or recovery seed can access the VA wallet despite law enforcement's seizure of wallet), seizure should ideally apply almost instantaneously (e.g., by moving VAs immediately into a LEA-controlled wallet). This may require adjusting some legal requirements and practices (e.g., freezing/seizing orders to be issued by a court) to allow for sufficient speed. Uganda may therefore need to establish the relevant framework to allow such possible seizure, as well as to enable LEAs to locate the associated instruments of the wallet or access private keys and/or recovery seeds.

5.3.6.2 Management of seized VAs.

Competent authorities could choose to either

(i) Convert VAs into fiat currency and manage the seized monies in a traditional fashion or

(ii) Manage the VAs in their existing form (i.e., creating a wallet, held and managed by LEA or a wallet service provider, into which seized VAs can be moved), which may require new policies and procedures (e.g., maintain records of private keys, recovery seeds). LEAs in some jurisdictions have opted to indicate the quantity of the virtual assets at the point of seizure instead of value to mitigate the volatile nature of the VAs.

Additional considerations arise from the high-price volatility of VAs, especially in light of potentially lengthy criminal procedures, and cyber security related risks. Decisions will need to be taken as to the value at which the VAs should be held (e.g., the price at the time the enforcement measure was taken or the price at the end of the criminal law process), as this can have implications following the adjudication and final outcome of the case. Efforts must also be made to secure the official wallets, commensurate with the cyber risks of the different types of wallet (e.g., cold storage is likely to be less prone to cyberattacks).

15. Examples of such firms include Elliptic, Chainalysis, CipherTrace, Coinfirm, Scorechain, Merkle Science and TRM Labs

5.3.6.3 Confiscation.

Competent Authorities should establish how to handle the confiscated VAs. They can choose to hold VAs or convert them to fiat. This may include similar considerations as seizing assets as noted earlier, and may require adjusting the legal framework.

5.3.7 International Cooperation

In light of the highly mobile nature of VAs, close and swift cooperation between countries is key. There needs to be a clear legal basis for exchanging information and cooperating, even for countries that have restricted or banned VA-related activities. In some instances, traditional processes such as mutual legal assistance (MLA) requests may be too slow and thus ineffective in a virtual asset context. Therefore, there may be a greater need to build up informal cooperation channels with different authorities (for instance, police and tax authorities) who would have the ability to take swift, conservatory action, including for freezing/ seizing of wallets, until more formal international cooperation processes have been initiated. Where MLA depends on dual criminality, additional issues may arise when other countries' criminal justice frameworks do not properly capture VAs. Finally, good domestic coordination is also useful since different authorities may have different channels for communication with their foreign counterparts.

6.0 CONCLUSION

The new FATF standards provide much needed clarity on ML/TF/PF risk mitigation in the virtual asset space. By explicitly addressing VAs in its standards, the FATF has facilitated the transposition of those standards into the domestic legal and regulatory frameworks. This is key in guiding country authorities / FIUs in the necessary legal and regulatory adjustments that might be needed, and in ensuring greater consistency in countries' approaches to mitigating the financial integrity risks of VAs. By addressing VAs in broadly the same way as other types of assets, the FATF ensured that VAs are treated adequately taking into account their intrinsic characteristics.

The main challenges to mitigation include keeping up with the technology and increasing dialogue amongst stakeholders. For the foreseeable future, VAs are here to stay and they are likely to be used increasingly in cross-border transactions. In particular, broad use of the stable coins would require rapid and coordinated actions across the globe to manage the associated financial integrity risks. A solid understanding of VAs' underpinnings and operating models is therefore a necessity for all AML/CFT stakeholders. In most instances, this will require building up the expertise and capacity of the relevant domestic authorities: policy makers, AML/CFT supervisors, FIA, competent authorities, and the judiciary.

Close dialogue with the VASP industry can be particularly helpful in that respect. Given the cross-border nature of the virtual assets space, close and prompt cooperation among jurisdictions is key to any effective mitigation strategy.

16. Cold storage refers to offline wallets that are not connected to the internet, and can include information stored in paper wallets (which are pieces of paper with information related to keys) and hardware wallets (which can be a remote device with relevant information on keys, which can be connected to a computer as required (e.g., USB sticks)).

Finally, a good understanding of the potential that technology offers to support the implementation of the AML/CFT framework would also be beneficial.

More broadly, the AML/CFT community, including the FATF and international organizations such as the IMF, UNODC, UNOCT, etc., will need to continue their engagement. Uganda is likely to face ongoing challenges in their mitigation of the risks in light of the rapidly evolving nature of VAs. The international community will need to support Uganda in its efforts to address the challenge. This support should include continued monitoring of developments in the virtual assets space and continued efforts to facilitate the effective implementation of the FATF standards. This should include the provision of advice and capacity development activities.

7.0 RECOMMENDATIONS

These recommendations are intended to guide in broad approaches that are necessary to protect citizens and the global economy from the risks of abuse of virtual assets.

7.1 Ensure compliance with FATF Recommendation 15

Uganda is currently rated Partially Compliant (PC) with FATF recommendation 15 on new technologies, and there is need for the Country to take steps to ensure compliance. This recommendation has 11 criterions of which only 2 are currently complaint. The VAWG has a major role in ensuring compliance of the outstanding 9 criterion such as;

(i) Coordinating a country level ML/TF risk assessment on new technologies that will address criterion 15.1 to 15.3.

(ii) Working hand in hand with industry players such as the self-regulating bodies e.g. FITSPA, Blockchain Association of Uganda, etc. to address criterion 15.5 - 15.11.

(iii) Preparation of draft regulations and guidelines specific to VASPs that will ensure compliance of the AML/CFT regime.

7.2 Capacity Building

Invest massively in capacity building, especially for those in law enforcement and the private sector in a position to detect virtual assets-based money laundering. Building capacity is not only about training existing staff, but about changing hiring practices to attract those already skilled in the cyber sphere. The virtual assets industry is expanding and evolving at an incredible rate. Capacity building should be widespread, with a particular focus on:

a) Strengthening the capabilities of specialised law enforcement units to address virtual asset related threats. These units are well placed to transfer skills within their own agencies (see next point) through in-house capacity building and awareness-raising.

b) Accelerating the training of "front-line" staff in a position to detect virtual asset related crimes. In law enforcement, this means first responders and those involved in investigating serious organised crime, corruption and other financial crimes. In the private

sector, AML compliance professionals in particular need to quickly upskill. Early detection aids investigation and the timely freezing of suspect funds before they can be dissipated or hidden.

c) Ensuring judicial authorities have the required knowledge and capabilities to act fast when warranties, summons and judicial requests are made.

d) Ensuring AML supervisors correctly understand new business models, their associated risks and how to address them. Both law enforcement and the private sector need to attract talented "digital natives" with high levels of technical expertise.

e) FIA should utilize the EGMONT group of FIU's facility to improve the expertise and capabilities of staff through FIU staff exchanges and technical support.

7.3 Harmonised Regulation and Its Effective Implementation

a) Ensure smart, harmonised laws and regulations that draws on wide-ranging expertise and looks ahead to future challenges. It is essential that all national authorities implement international regulations effectively, to prevent ML/TF/PF activity simply moving to jurisdictions with weak and poorly enforced regulations.

b) Regulation of VAs is challenging because they do not easily fall into traditional categories of AML regulation such as e-money, securities or financial instruments. The nature of VAs makes it difficult to impose regulatory requirements on the asset itself. This makes VAs highly vulnerable to use for illicit purposes and ML/TF/PF.

c) There is a strong need for specific regulations in order to set the parameters for market participants and establish a framework for investigators to approach bad actors in the system. Standards need to be harmonised internationally, to prevent criminals from engaging in regulatory arbitrage by simply moving their operations to jurisdictions with weak and poorly enforced regulations on virtual assets-based money laundering.

d) All DLT-based services that have elements of centralisation should be subject to anti-money laundering and counter financing of terrorism (AML/CFT) regulations like any other reporting entities. Given the cross-border nature of crypto assets and increased use of privacy mechanisms to conceal the source of funds or wealth, VASPs will be expected to apply a risk-based approach in evaluating the appropriate due diligence for each customer, product, transaction and asset type. Additional effort may be required to bring DeFi platforms under supervisory control, relying on the presence of centralised features such as the ability of a natural person or legal entity to modify smart contract features over time.

e) Recent regulatory developments address some of the risks associated with the use of virtual assets. However, competent authorities still need to speed up implementation of international standards, especially of the so-called travel rule, and address consumer protection and other regulatory risks.

f) A forward-looking approach is also needed to address challenges around the corner, such as arising from NFTs, the metaverse and the gaming industry. Competent authorities should closely monitor developments in this area, and consult widely with industry and law enforcement stakeholders to more fully understand the impacts of certain policies, which may be different to those one might expect in traditional financial markets.

7.4 International Cooperation and Mutual Legal Assistance

a) Make existing channels of international cooperation stronger, faster and more proactive, to counter the lightning-fast and hyperglobal nature of virtual assets. This includes efforts to strengthen both formal and informal cooperation between law enforcement agencies and judicial authorities, as well as between law enforcement and VASPs based in other jurisdictions.

The virtual assets industry is hyperglobal, and criminals can operate crypto-enabled crime schemes or launder illicit funds on the other side of the world just as easily as they can at home. Transactions take place at lightning speed and are often irreversible.

b) Law Enforcement Agencies should maximise the use of existing channels of both informal and formal cooperation to exchange information that can help to identify, investigate and prosecute those using virtual assets for illicit purposes. This includes the global cooperation mechanisms provided by EGMONT, INTERPOL and Europol, such as the Secure Information Exchange Network Application channel and the network of National Central Bureaus (NCBs), as well as bilateral and multilateral channels with VASPs based in different jurisdictions (see Recommendation 3). For example, in cases of serious and organised crimes, it should be standard practice to check names, telephone numbers and cryptocurrency addresses with Europol to crosscheck with other investigations.

c) Speeding up information exchange and the sending, receiving and actioning of judicial requests should be a priority, particularly where funds need to be frozen before they are dissipated or disappear. The hyper-speed nature of virtual assets means that all and any efforts in this area will result in significantly improved outcomes for investigations, prosecution and asset recovery.

d) When resources (new techniques, best practices, new strategies) are developed that could be useful for all law enforcement authorities, these should be shared widely to prevent duplication of work and ensure a consistent and harmonised response.

e) International cooperation should extend to developing standards and best practices in tackling virtual assets-based money laundering, as well as sharing emerging modi-operandi and investigative techniques. Conferences, workshops and knowledge-sharing sessions are key to this effort, as well as to building the trust and relationships that are foundational for effective international cooperation.

f) Virtual Assets are cloud based and facilitate unregulated cross border and transnational transactions. They therefore pose a very high risk for regulatory arbitrage to Uganda. International cooperation against the criminal misuse of VAs should therefore take a unified front at Regional level. i.e ESAAMLG and the East African Community.

7.5 Research and Development

R&D is key to FIA given that VAs and VASPs is an ever-evolving space. It is important because it provides powerful knowledge and insights, leads to improvements to existing processes, typologies, practices, positions, where efficiency can be increased.

7.6 Domestic Collaboration

a) Make existing channels of domestic cooperation stronger, faster and more proactive, to counter the lightning-fast nature of VAs. This includes efforts to strengthen both formal and informal cooperation between law enforcement agencies and judicial authorities, as well as between law enforcement and VASPs based in Uganda.

b) Law Enforcement Agencies should maximise the use of existing channels of both informal and formal cooperation to exchange information that can help to identify, investigate and prosecute those using virtual assets for illicit purposes.

7.7 Public-Private Cooperation

a) Establish trust and effective mechanisms for public-private cooperation to address virtual assets-based money laundering, especially between law enforcement and VASPs. Cooperation can be bilateral, multilateral or through public-private partnerships, and should cover both operational and strategic information sharing.

Combating virtual assets-based money laundering is a major ongoing challenge and requires all stakeholders to pool their expertise, information and resources.

b) VASPs like all financial institutions, have information and technical capabilities that can support law enforcement investigations and asset recovery, including tools for data analysis and transaction monitoring. They also have the ability to blacklist users, lock accounts and contact suspects to refund stolen funds. Close cooperation, including via joint investigations where appropriate, can help law enforcement agencies to do more with fewer in-house resources.

c) Speed is another benefit of public-private cooperation. For example, transaction monitoring tools developed by exchanges can help them to identify transactions potentially linked to illegal activity. Leads can then be referred to the law enforcement agency, which can quickly send and receive the relevant information through formal legal channels. Custom follow-up is also possible in this scenario, instead of automated blocking or off-boarding by the exchange acting alone. In the case of high-priority incidents, exchanges can take immediate action.

d) Information sharing at the strategic level, for example about hacking attempts, fraudulent activity, money laundering modi operandi, devices used, newly discovered trends, suspects and victims can help exchanges and other VASPs to improve their defences and detection algorithms. This in turn means that law enforcement can better focus their investigations and contributes to prevention, awareness and capacity building on both sides. Collaboration on capacity building can also help specialist law enforcement units to stay at the cutting edge of developments in the virtual assets industry.

Additionally, in the spirit of information sharing and collaboration, the industry players can establish blacklists / grey-lists. Occasionally, if a VASP identifies an illicit actor, the exit / off-boarding of that actor could lead to the individual moving to another VASP, just to repeat the modus operandi. A shared industry blacklist / grey-list can enable effective mitigation and protection to the industry to prevent illicit actors from re-entering the system.

e) Both operational and strategic information sharing are facilitated where VASPs have dedicated departments for cooperating with law enforcement and other government bodies, including internationally. Contact details for such departments should be made available to all law enforcement authorities to facilitate subpoenas and requests from investigators to VASPs.

A regulatory framework would have to be in place to protect industry players for sharing customer information e.g. formal and regulated channels to receive requests for information to ensure legal protection and also to ensure the admissibility of evidence in court procedures.

f) Law enforcement agencies need to be proactive about directly approaching VASPs and building mechanisms for cooperation and information sharing. Europol and INTERPOL can support these efforts by facilitating initial contacts. Stakeholders can also consider using existing public-private partnerships as a platform for exchanging information and building trust, such as the Europol Financial Intelligence Public Private Partnership (EFIPPP).

7.8 Multidisciplinary approach, including through Specialized Law Enforcement Units

a) Combine the expertise of financial investigators, IT/forensics experts and cybercrime specialists to tackle cases of virtual assets-based money laundering and related crypto-enabled crimes. In a law enforcement context, this means increasing intra-agency cooperation between different units. Where feasible, specialist teams could also be established to lead complex cases and provide in-house support to other units.

b) A multidisciplinary approach is increasingly recognized as essential to tackling complex crimes, including those of a financial nature. In the crypto sphere, this is multiplied by the high level of specialized expertise required in IT, cybercrime and financial investigation.

c) Increasing numbers of law enforcement authorities have set up multidisciplinary units focused on crypto-enabled crimes. However, they remain small and insufficiently resourced when one considers the relative sizes of the physical and digital domains. This is true even now, and will be even more so in the future as the digital sphere grows.

d) Specialized units have the ability to move fast, conduct their own investigations and support investigations led by other law enforcement units. They can and do also cooperate efficiently with central government authorities as well as internationally. An effective and integrated multidisciplinary approach also requires the support of specialized judicial authorities.

e) Where resources do not exist for dedicated specialized units in law enforcement agencies, it is recommended to introduce measures to increase intra-agency and inter-agency coordination. These could include multidisciplinary working groups, task forces or joint investigation teams.

7.9 Investigative techniques and technologies

a) Rapidly develop, adapt and evolve investigative technologies and techniques to keep up with the criminals. In this effort, it is helpful to leverage the innovation capacity of the private sector.

As a broad modus operandi, virtual assets-based money laundering is evolving fast. Law enforcement should recognise the potential for money laundering through new forms of cryptocurrencies and other virtual assets, such as NFTs, and develop procedures to address such use.

b) Traditional investigative techniques such as undercover investigations and controlled delivery need to be adapted to the current scenario. Crypto tracing and other techniques such as tactical surveillance and analysis of transaction and tax information (financial investigation) should also be applied.

c) The private sector can be a powerful partner to law enforcement in developing and using new technologies for tracing funds held in VAs. For example, blockchain analytics firms are responding to the challenges of tracing funds exchanged on decentralized platforms by innovating fast; new screening tools for technologies such as oracles, liquidity pools and smart contracts are already being developed.

d) VASPs also hold information that can help to develop new investigative techniques to address emerging technologies in the crypto sphere. Training and joint workshops or conferences can help to transfer this vital knowledge. Examples are those organised by the EFIPPP, the Europol Platform for Experts (EPE) and the Tripartite Working Group on Criminal Finances and Cryptocurrencies, as well as Europol's Virtual Currency Conference.

It is not only law enforcement that needs to adapt investigative techniques; judicial authorities also need to develop new strategies to address virtual assets-based money laundering.

7.10 Virtual Asset Recovery

a) Treat VAs like traditional assets such as jewelry or artwork to facilitate their freezing and confiscation. Easing the recovery of VAs helps not only to return stolen funds, but also to deter future crypto-enabled crimes and virtual assets-based money laundering.

b) Cryptocurrencies and other virtual assets should be regarded like any other assets in terms of implementing tried-and-testing asset recovery best practice. Recognised strategies such as pre-seizure planning and public-private collaboration have been pivotal in many jurisdictions. Approaching virtual assets like a complex asset has enabled agencies to recover significant amounts of crypto assets and convert them into fiat currencies through exchanges or auctions.

However, some jurisdictions have not yet taken this best practice on board in their laws and procedures. As a result, they miss opportunities to disrupt criminality, identify illicit financial flows and recover assets for the benefit of victims and wider society.

c) As the quantity of illicit assets held in the form of VAs grows, failure to implement international best practice will be an increasing obstacle to countries' efforts to fight financial crime. This is because asset recovery is not only about returning criminal proceeds to victims and governments, but about preventing and deterring corruption, organised crime and other illicit activity. Recovering illicit assets raises the risk and cost of crime, reduces the potential reward and helps ensure that crime does not pay.

d) All stakeholders should actively engage in developing and applying emerging international best practices in virtual asset recovery. This includes sharing knowledge on ways to freeze and seize virtual assets, to manage them effectively in order to retain their value while criminal proceedings are underway, to overcome issues of volatility, and to convert them into fiat currency following the confiscation order. A good example of this is the subgroup on virtual currencies within the Asset Recovery Office (ARO) platform hosted by the European Commission, in which Europol and EU AROs participate.

This document was compiled by the Financial Intelligence Authority, Virtual Assets Working Group (FIA VAWG) composed of:

NO.	MEMBER NAME	MEMBER POSITION
1.	CYRUS BARIGYE	CHAIRPERSON
2.	LAZARUS MUKASA	CO-CHAIRPERSON
3.	SHERIFAH TUMUSIIME	SECRETARY
4.	EDWARD AMANYIRE	COORDINATOR
5.	IVAN BWIRE	MEMBER
6.	GLADYS ATIM	MEMBER
7.	VINCENT KALULE	MEMBER
8.	MARGARET NABUKEERA	MEMBER
9.	BRIGHT BESIGYE	MEMBER