FINANCIAL INTELLIGENCE CENTRE

P.O. BOX 2882, Windhoek

Tel: +264 61 283 5100 / 5216 / 5283, Fax +264 61 283 5259

Web address: www.fic.na

E-mail address: helpdesk@fic.na

DIRECTIVE NO 02 OF 2021

DATE ISSUED: 17 SEPTEMBER 2021

FINANCIAL INTELLIGENCE ACT, 2012 (FIA) COMPLIANCE REQUIREMENTS FOR VIRTUAL ASSETS SERVICE PROVIDERS (VASPs)

KEY DEFINITIONS AND SCOPE OF VASPs

Part A: Key definitions

1. ***Virtual Asset (VA):*** *VAs must be digital and must themselves be digitally traded or transferred and be capable of being used for payment or investment purposes. That is, they cannot be merely digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in Schedules 1 and 3 of the Financial Intelligence Act, 2012, without an inherent ability themselves to be electronically traded or transferred and the possibility to be used for payment or investment purposes.*

2. ***Virtual Asset Service Provider (VASP):*** *The definition of a VASP is broadly defined by the Financial Action Task Force (FATF), owing to the nature of virtual asset operations. Along such guidance, Namibia has adopted a functional approach and applies the following concepts underlying the definition to determine whether an entity is undertaking the functions of a VASP. A VASP is any natural or legal person who, 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 assets and fiat currencies;*
   - *ii. Exchange between one or more forms of virtual assets;*
   - *iii. Transfer[1] of virtual assets;*
   - *iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and*
   - *v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.*

Part B: Scope of VASPs

3. VA Exchange and transfer

The first part of the definition of VASP refers to any service in which VAs can be given in exchange for fiat currency or vice versa. If parties can pay for VAs using fiat currency or can pay using VAs for fiat currency, the offerer, provider, or facilitator of this service when acting as a business is a VASP. Similarly, in the second part or (ii), if parties can use one kind of VA as a means of exchange or form of payment for another VA, the offerer, provider or facilitator of this service when acting as a business is a VASP. It is emphasized that parts (i) and (ii) include the above

[1] In this context of virtual assets, transfer means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

activities, regardless of the role the service provider plays vis-à-vis its customers as a principal, as a central counterparty for clearing or settling transactions, as an executing facility or as another intermediary facilitating the transaction. A VASP does not have to provide every element of the exchange or transfer in order to qualify as a VASP, so long as it undertakes the exchange activity as a business on behalf of another natural or legal person. Part (iii) in the definition of VASP covers any service allowing users to transfer ownership, or control of a VA to another user. The FATF Recommendations define this to mean "conduct[ing] a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another." To help illustrate what this part covers in practice, it is useful to consider the current nature of the VA. If a new party has custody or ownership of the VA, has the ability to pass control of the VA to others, or has the ability to benefit from its use, then transfer has likely occurred. This control does not have to be unilateral and multi-signature[2] processes are not exempt (see limb (iv) below), where a VASP undertakes the activity as a business on behalf of another natural or legal person.

Where custodians need keys held by others to carry out transactions, these custodians still have control of the asset. A user, for example, who owns a VA, but cannot send it without the participation of others in a multi-signature transaction, likely still controls it for the purposes of this definition. Service providers who cannot complete transactions without a key held by another party are not disqualified from falling under the definition of a VASP, regardless of the numbers, controlling power and any other properties of the involved parties of the signature. The part is conceptually similar to what FATF Recommendation 14 on money and value transfer services (MVTS) covers for traditional financial assets. An example of a service covered by (iii) includes the function of facilitating or allowing users to send VAs to other individuals, as in a personal remittance payment, payment for nonfinancial goods or services, or payment of wages. A provider offering such a service will likely be a VASP.

4. Decentralized or distributed application (DApp)

Exchange or transfer services may also occur through so-called decentralized exchanges or platforms. The Decentralized or distributed application (DApp), refers to a software program that operates on a P2P[3] network of computers running a blockchain protocol—a type of distributed public ledger that allows the development of other applications. These applications or platforms are often run on a distributed ledger but still usually have a central party with some measure of involvement, such as creating and launching an asset, setting parameters, holding an administrative "key" or collecting fees. Often, a DApp user pays a fee to the DApp, which is commonly paid in VAs, for the ultimate benefit of the owner/operator/developer/community in order to develop/run/maintain the software.

[2] In a multi-signature process or model, a person needs several digital signatures (and therefore several private keys) to perform a transaction from a wallet.
[3] Refers to direct Peer-to-Peer (P2P) remittances or movement of value without the conventional facilitation of a centralized exchange platform.

DApps can facilitate or conduct the exchange or transfer of VAs. Under the FATF Recommendations, a DApp itself (i.e the software program) is not a VASP, as the Recommendations do not apply to underlying software or technology. However, entities involved with the DApp may be VASPs as per definition herein and in line with the FATF. For example, the owner/operator(s) of the DApp likely fall under the definition of a VASP, as they are conducting the exchange or transfer of VAs as a business on behalf of a customer. The owner/operator is likely to be a VASP, even if other parties play a role in the service or portions of the process are automated. Likewise, a person that conducts business development for a DApp may be a VASP when they engage as a business in facilitating or conducting the activities previously described on behalf of another natural or legal person. The decentralization of any individual element of operations does not eliminate VASP coverage if the elements of any part of the VASP definition remain in place.

5. Other common VA services or business models

Other similar services or business models may also constitute exchange or transfer activities based on parts (i), (ii), and (iii) of the VASP definition, and the natural or legal persons behind such services or models would therefore be VASPs if they conduct or facilitate the activity as a business on behalf of another person. These can include:

1. *VA escrow services, including services involving smart contract technology, that VA buyers use to send or transfer fiat currency in exchange for VAs, when the entity providing the service has custody over the funds;*

2. *brokerage services that facilitate the issuance and trading of VAs on behalf of a natural or legal person's customers;*

3. *order-book exchange services, which brings together orders for buyers and sellers, typically by enabling users to find counterparties, discover prices, and trade, potentially through the use of a matching engine that matches the buy and sell orders from users (although a platform which is a pure-matching service for buyers and sellers of VAs and does not undertake any of the services in the definition of a VASP would not be a VASP); and*

4. *advanced trading services, which may allow users to access more sophisticated trading techniques, such as trading on margin or algorithm-based trading.*

6. P2P platforms

For P2P platforms, the approach in considering their scope within the VASP definition is centred around the underlying activity, and not the label or business model. Where the platform facilitates the exchange, transfer, safekeeping or other financial activity involving VAs (as described in parts (i)-(v) of the VASP definition), then the platform is necessarily a VASP conducting exchange and/or transfer activity as a business on behalf of its customers. Launching a service as a

business that offers a qualifying function, such as transfer of assets, may qualify an entity as a VASP even if that entity gives up control after launching it, consistent with the discussion of the lifecycle of VASPs above. Some kinds of "matching" or "finding" services may also qualify as VASPs even if not interposed in the transaction.

The definition (based on FATF expectations) takes an expansive view of the definitions of VA and VASP and considers most arrangements currently in operation, even if they self-categorize as P2P platforms, may have at least some party involved at some stage of the product's development and launch that constitutes a VASP. Automating a process that has been designed to provide covered services does not relieve the controlling party of FIA obligations.

7. Regulatory sandbox

"A regulatory sandbox is a regulatory approach, typically summarized in writing and published, that allows live, time-bound testing of innovations under a regulator's oversight. Novel financial products, technologies, and business models can be tested under a set of rules, supervision requirements, and appropriate safeguards. A sandbox creates a conducive and contained space where incumbents and challengers experiment with innovations at the edge or even outside of the existing regulatory framework. A regulatory sandbox brings the cost of innovation down, reduces barriers to entry, and allows regulators to collect important insights before deciding if further regulatory action is necessary. A successful test may result in several outcomes, including full-fledged or tailored authorization of the innovation, changes in regulation, or a cease-and desist order."[4]

8. Products and Services

Refers to the actual product or service which the service provider will provide upon licensing or regulatory approval.

9. Technologies or Innovations

These terms are used herein to the extent that the technology or innovation avails a platform for financial products or services. References to such terms is not necessarily intended to regulate conventional technology or innovation.

---

[4] *Source: United Nations Secretary-General's Special Advocate for Inclusive Finance for Development. Via: https://www.unsgsa.org/sites/default/files/resources-files/2020-09/Fintech_Briefing_Paper_Regulatory_Sandboxes.pdf#:~:text=A%20regulatory%20sandbox%20is%20a%20regulatory%20approach%2C%20typically,set%20of%20rules%2C%20supervision%20requirements%2C%20and%20appropriate%20safeguards.*

1. INTRODUCTION

The Financial Intelligence Centre (FIC) is tasked with the coordination of Namibia's Anti-Money Laundering, Combatting the Financing of Terrorism and Proliferation (AML/CFT/CPF) activities[5]. In furtherance of this mandate, the FIC's responsibility includes supervision of various sectors that deal in specified services as per Schedules 1 and 3 of the Financial Intelligence Act, 2012 (Act No 13 of 2012) as amended (FIA).

The global emergence of Virtual Assets (VAs), often referred to as crypto or digital assets (or currencies), has resulted in the creation of an avenue where electronic value is moved with minimal regulatory oversight and interventions. While such regulatory oversight and interventions may not always be desired by persons preferring the use of VAs, the VA platforms, like any other, are vulnerable to Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) abuse. The absence of relevant AML/CFT/CPF controls on any platform enhances its exposure to ML/TF/PF vulnerabilities.

Persons that avail products and services within the scope of Item 13 of FIA Schedule 1, are Accountable Institutions (AIs) and therefore fall within the Namibian AML/CFT/CPF regulatory and supervisory framework.

1.1 Virtual Asset (VA)

A VA is a cryptographic or digital representation of value that can be used for payment or investment purposes. Regardless of its use, a VA does not meet the criteria for consideration as a fiat currency in Namibia, but it can be readily exchanged for funds, goods or for other VAs amongst parties who choose to do so. Most include a private key of a cryptographic nature or system that enables persons to have access to a digital representation of value.

[5] the Financial Intelligence Act, 2012 (Act No. 13 of 2012) (FIA), as amended, section 9(1) (f) and (g).

1.2 Scope of Virtual Asset Service Providers (VASPs)

A VASP is a person who carries out one or more of the five categories of activity or operation described in the VASP definition on pages 2 – 5 (i.e "exchange" of virtual/fiat, "exchange" of virtual/virtual, "transfer," "safekeeping and/or administration," and "participation in and provision of financial services related to an issuer's offer and/or sale").

In terms of this definition, a VASP includes persons availing certain services within the VA value chain. These include but are not limited to exchange houses; agents; brokers; mixers; traders; virtual asset managers; persons providing for trade, clearance and settlement services of VAs; persons facilitating the exchange of fiat currencies for any type of VA (and vice-versa), crypto fund managers and distributors of crypto funds, businesses or persons accepting VAs as forms of payment for their products and services etc. These are activities that are inherently vulnerable to ML/TF/PF abuse and excludes persons offering certain services which merely support the administration or functioning of technologies/platforms on which VAs operate, such as Bitcoinminers, provided that such are not involved in any of the activities mentioned above.

1.3 Namibian AML/CFT/CPF regulatory scope: Domestic and foreign VASPs

By their very nature, VAs have no jurisdictional limitations. It is thus common that VASPs avail services to persons regardless of jurisdictional origin or regulatory frameworks. In furtherance of risk mitigation in such spheres, AML/CFT/CPF frameworks are aligned accordingly.

It is hereby directed, in terms of FIA sections 9(2) and 54(2) that both domestic and certain[6] foreign based VASPs fall within the Namibian AML/CFT/CPF regulatory

[6] As per section 1.3.2 below.

framework as entities involved in the movement of electronic values as per Item 13 of FIA Schedule 1.

1.3.1 Domestic VASPs

Domestic VASPs as persons that perform any of the abovementioned services and:

a. are incorporated in Namibia;
b. have physical location(s) or place of business in Namibia; or
c. have employees, agents or branches that advance their VA trading activities in Namibia.

1.3.2 Foreign VASPs

Foreign VASPs that meet the criteria below fall within the Namibian AML/CFT/CPF framework and are thus required to register with the FIC (as per Directive No. 02 of 2020[7]) and duly implement measures to comply with the FIA. The foreign VASPs which must ensure FIA compliance are those that:

a. perform one or more of the services listed above; and/or
b. have no Namibian abode, but as part of their business activities, target Namibian residents and directs services at them (e.g using a *.na* domain, or markets and advertises for, or in any other way targets a Namibian audience).

2. COMPLIANCE DIRECTIVES

All persons who meet the definition of VASPs (domestic and foreign) are directed to take the following steps to ensure compliance with the FIA.

2.1 Step 1: Conduct a risk assessment

[7] https://www.fic.na/index.php?page=2020-directives

The aim of such assessment is to identify ways in which the specific services to be offered (or currently offered) can be abused by those advancing ML/TF/PF activities. In furtherance of this, VASPs, like all other Accountable Institutions under the FIA, are **required to undertake a ML/TF/PF risk assessment**[8], the comprehensiveness of which should be aligned to the nature, complexity and risk exposure of proposed (or current) products or services. Directive No 01 of 2021 (https://www.fic.na/index.php?page=2021-directives) avails detailed information on key variables that ought to be considered as part of such assessment. Outcomes of such risk assessment should be used to craft or inform the VASPs' AML/CFT/CPF compliance framework (program) as per below.

2.2 Step 2: create (and implement[9]) an AML/CFT/CPF compliance framework (program)[10]

VASPs are expected, in terms of sections 39(3), read with sections 39(4), 39(5) and 39(7) of the FIA, to develop programmes, policies, procedures and controls to effectively mitigate and manage ML/TF/PF risks. These programmes, policies, procedures and controls should be aimed at outlining how the VASP will comply with its obligations as mandated in the FIA. These sets of controls are collectively referred to as the FIA Compliance Program, which is a crucial guide for the implementation of an effective AML/CFT/CPF control framework. Such a FIA Compliance Program should be approved by the relevant senior/executive management of the VASP as per FIA section 39(4). VASPs with branches, agents, brokers, other third parties that helps in its compliance with the FIA, should ensure such FIA Compliance Framework outlines the responsibilities of all parties in preventing and combatting ML/TF/PF risks (both in and outside Namibia).

[8] FIA section 39(1) read with FIA section 23 requires that an accountable institution, on a regular basis, must conduct ML/TF/PF activities risk assessments taking into account the scope and nature of its clients, products and services, as well as the geographical area from where its clients and business dealings originate. Persons much measure, rank or rate (e.g low, medium and high) their level of risk for relevant elements of the services they aim to provide. You should rank each service as low, medium or high risk. The control measures should describe how the entity will reduce each level of risk, especially the medium and higher risk rated levels. The FIC may, in its interpretation however disagree with ratings not duly informed and request reconsiderations accordingly.

[9] For existing VASPs or those that have received regulatory approval/consent to proceed with commencement of operations.

[10] See Guidance Note No 04 of 2009 on the FIC website under "Publications" on how to create a compliance program. The FIC can be engaged for guidance in the regard.

The VASP's AML/CFT/CPF framework or program, as informed by an understanding of ML/TF/PF risks that the VASP is exposed to, should, at a minimum, provide for the following:

a. **Identify clients in terms of the FIA:** FIA section 21 requires identification of clients when a business relationship is established or a single transaction is concluded. The FIA Regulations further guide how such identification should be undertaken. This needs to be understood and implemented within the risk profile of such clients as stated in FIA section 23[11]. In this regard, VASPs should consider Guidance Notes No. 01 and 03 of 2015[12] on general customer identification and Guidance Note No. 01 of 2019 on CDD related to Politically Exposed Persons (PEPs).[13] In due time, the FIC will study the practical operations of local VASPs and issue an industry specific guidance for VASPs;

b. **Monitoring controls to detect suspicious transactions/activities:** As per section 23 of the FIA, implement appropriate risk management and monitoring systems to identify clients or beneficial owners whose activities may pose a risk of ML/TF/PF. If detected, such should be analysed and if found suspicious for ML/TF/PF purposes, need to be reported to the FIC as per section 33 of the FIA. Consider Guidance Note 06 of 2015[14] on STR and SAR reporting as well as Guidance Note No. 04 of 2017[15];

c. **Ensure mandatory reporting of transactions:** reporting transactions that fall within the prescribed parameters: In terms of section 32 of the FIA, VASPs, along with all other Accountable Institutions are required to report, within a five-day period, all cash transactions above NAD 99,999.99 to the FIC in the prescribed form and manner. This applies to physical cash brought to the VASP and excludes payments made directly to the bank account of a VASP. Considering the said financial threshold, VASPs are

[11] to have appropriate risk management and monitoring systems in place to identify clients or beneficial owners whose activities may pose a risk of ML/TF/PF.
[12] FIC website: https://www.fic.na/index.php?page=2015-guidance-notes
[13] FIC website: https://www.fic.na/index.php?page=2019-guidance-notes
[14] FIC website: https://www.fic.na/index.php?page=2015-guidance-notes
[15] FIC website: https://www.fic.na/index.php?page=2017-guidance-notes

required to put mechanisms in place to detect transactions structured in a manner to avoid the reporting threshold. If related transactions occur within a reasonably shorter period of each other and collectively exceed the prescribed threshold, then same must be reported to the FIC as a CTR. See Revised Circular 03 of 2015[16]. Consider Guidance Note 06 of 2015[17] on STR, SAR, CTR, EFT reporting guidelines;

Important: *The FIC herewith directs that all obligations that apply to Banks and Money Value Transfer Services (MVTs)/Authorised Dealers with Limited Authority (ADLAs) as per Revised Circular 03 of 2015[18] similarly apply to VASPs. Therefore, VASPs, Banks and ADLAs should file IFTs & EFTs with the FIC.*

d. **Implement measures to screen clients against United Nations Security Council (UNSC) sanctions lists:** In terms of FIA,[19] ensure implementation of controls which ensure the screening of all clients or potential clients against the UNSC sanctions lists, before availing services to such clients, for purposes of combating TF and PF activities;

e. **Effective record keeping:** The primary goal of record keeping in AML/CFT/CPF is to ensure such records are adequate or fit for purpose. For customer due diligence, records need to enable the creation of an adequate customer profile which can assist in monitoring. Another object of record keeping is transaction reconstruction for use by competent authorities (e.g to provide reliable evidence for civil proceedings or criminal prosecution). Records ought to be reliable and be kept in a manner that enables timely access to such. In terms of FIA sections 26 and 27, read with FIA Directive 02 of 2017[20], VASPs, like all other Accountable Institutions, are required to keep records in the prescribed manner and form. Such records include the identity of clients, manner in which such identities are/were established and all transactional

[16] FIC website: https://www.fic.na/index.php?page=2015-circulars
[17] FIC website: https://www.fic.na/index.php?page=2015-guidance-notes
[18] FIC website: https://www.fic.na/index.php?page=2015-circulars
[19] FIA Regulation 1 read with Regulation 15 read with section 25 of the Prevention and Combating of Terrorist and Proliferation Activities Act, 2014 (Act No. 4 of 2014) (PACOTPAA).
[20] FIC website: https://www.fic.na/index.php?page=2017-directives

records for a minimum period of five years. If any mandatory reports (CTRs, EFTs, STRs etc) are reported to the FIC, VASPs should equally keep records of such, for five years. Records within the VASP's reach/domain, which are beyond the conventional financial systems (e.g blockchain) should be maintained to enable inspections as per FIA section 53 and access (or tracing) by competent authorities as per relevant sections of the FIA. Records on the trading, exchange or such other similar platforms should be maintained to the extent that the VASPs can reconstruct all transactions it facilitated;

f. **Staff training:** Create provision for training relevant staff members to execute their functions in terms of FIA section 39(5)(b). There is a need to ensure that on-going training programs are implemented for relevant staff members on their duties and responsibilities relating to FIA compliance;

g. **Subject the entire AML/CFT/CPF program/controls to independent reviews (audit):** Section 39(8) of the FIA requires institutions to subject their AML/CFT/CPF compliance programs, processes and control measures to an independent audit review. The aim of such is to evaluate the adequacy and effectiveness of AML/CFT/CPF policies, procedures and controls to provide the VASPs' management with reasonable assurance that such controls are working efficiently and effectively. This needs to occur periodically, especially when there are changes in risks or other AML/CFT/CPF considerations; and

h. **Duly designate or appoint an AML Compliance Officer:** in terms of section 39(6) of the FIA, such Compliance Officer should be at management level. Such must be skilled and operationally independent from the execution of high risk operations within the entity charged. This person shall be tasked with ensuring the day-to-day execution of the AML/CFT/CPF activities as set out above.

2.3 Step 4: Register with the FIC

Upon registration with the FIC, it is required that registering persons avail documents which detail the VASPs' AML/CFT/CPF compliance framework (referred to above).

All pre-existing VASP service providers should ensure registration with the FIC before or on **30 September 2021**. All other persons desiring to operate as VASPs after such date need to ensure prior FIC registration (and any prudential regulations that may arise at the time), before commencement of any such VASP related operations or businesses.

Directive 03 of 2020 (https://www.fic.na/index.php?page=2020-directives) directs persons on registration procedures to follow.

3. DIRECTIVES ON OPERATIONAL ARRANGEMENTS

In furtherance of the need to advance FIA objectives as per section 9(2), and the effective execution of FIA compliance related inspections (as per section 53), VASPs are further directed to ensure the following:

a. Conducting all VA trading activities under a single legal entity. This ensures the ease with which VA related transactions can be traced for assessment, monitoring and any other regulatory purposes. Deviations need prior FIC written consent;
b. Using the Namibian Dollar as a standard for measuring, comparing or estimating the value of all forms of VAs (e.g for currency or related conversion); and
c. Ensure compliance of its VA trading activities and operations with all other applicable laws emanating from prudential or such other relevant authorities.

4. CONCLUSION

With due consideration to ML/TF/PF vulnerabilities within various components of the VASP value chain, persons that conduct business and transactions for their customers will be regulated if they: (a) exchange digital currencies for fiat currencies; or (b) exchange

between VAs. As per the definition and context herein, the AML/CFT/CPF framework primarily applies to both domestic and relevant foreign VASPs such as: custodial wallet service providers who hold customers' private keys (including exchanges, VA brokers), as their services are susceptible to ML/TF/PF risks.

5. NON-COMPLIANCE WITH THE PROVISIONS OF THIS DIRECTIVE

For persons to duly comply with the FIA, FIC registration is an essential starting point. The consequence of failure to register with the FIC undermines the ability to ensure effective supervision in terms of the FIA. Such failure not only hampers the effective functioning of the entire AML/CFT/CPF framework but may result in such entities being subjected to enforcement considerations as per the FIA.

6. GENERAL

This Directive may contain statements of policy which reflect the FIC's administration of the legislation in carrying out its statutory functions. The Directive is issued without prejudice to the FIA and its complementing Regulations. The information contained herein is intended to only provide a summary on these matters and is not intended to be comprehensive.

The Directive can be accessed at https://www.fic.na/index.php?page=2021-directives

DIRECTOR: FINANCIAL INTELLIGENCE CENTRE