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 01 OF 2021

FIRST ISSUED: 17 SEPTEMBER 2021

REVISED AND UPDATED: 22 MARCH 2022

REQUIREMENTS RELATING TO THE INTRODUCTION OF NEW INNOVATIONS, PRODUCTS, SERVICES OR EXPANSIONS AND AMENDMENTS TO PRE-EXISTING ONES

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

[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.

when acting as a business is a VASP. It is emphasized that parts (i) and (ii) include the above 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—any type of distributed ledger (includes public, private and any other type of ledger/platform) 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:

a. *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;*

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

c. *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*

d. *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 part 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).

This Directive should be duly considered with all other prior FIC publications on risk management and compliance and in particular Revised Directive 01 of 2021, which was also updated in March 2022.

1.1 SUMMARY OF UPDATE/REVISION: MARCH 2022

Since its implementation on 17 September 2021, inputs were received from various stakeholders necessitating this revision. Below is a summary of the material revisions within this Directive:

a. *Scope of ledgers in VAs and VASPs:* the definition or scope of ledgers[6] described in the first version of the Directive referred to *public* ledgers only. Such definition now refers to ledgers broadly. This is necessary to include public, private and any other type of ledger that may be used and thus be vulnerable to ML/TF/PF;
b. *FIC's turnaround times:* avail context around the FIC's turnaround time/period after receiving institutional submissions for proposed products or services, before the eventual launching of same. This includes the turnaround time/period related to proposed amendments/expansions that institutions plan to effect on products or services already in the market. Such period is generally within 30 days but may be deviated from should the need arise;
c. *Nature of information required* to demonstrate compliance with this Directive: Depending on the nature of proposed operations, products and services (or

[5] the Financial Intelligence Act, 2012 (Act No. 13 of 2012) (FIA), as amended, section 9(1) (f) and (g).
[6] See definition of Decentralized or distributed application (DApp) on pages 3 - 4 above.

amendments thereto), unless otherwise specified[7], it is an applying institution's prerogative to decide on the most suitable type, nature and form of information to submit which best demonstrates compliance with the requirements herein. The FIC however reserves the right to request for any type of information (in any reasonable format) which may support its due diligence activities in this regard;

d. *Nature of amendments for which FIC consent is required:* The revised Directive now provides that FIC consent is only required for proposed amendments or expansions to existing products, services and operations where such amendments would have an impact on ML/TF/PF risk mitigation; and
e. *Physical presence in Namibia:* In ensuring effective risk based supervision and access to records by relevant AML/CFT/CPF combatting authorities, the FIC may require a foreign based applicant (or such relevant service provider) to have a physical presence in Namibia, as stated in the Revised Directive 02 of 2021.

2. OBJECTIVE

This Directive serves to ensure effective institutional and regulatory considerations are made with regards to the introduction of new products and services which could affect the financial system. This includes all types of electronic transfers of money or value as stated in Item 13 of Schedule 1[8] such as electronic money (e-money), the various forms of Virtual Assets (VAs)[9] or authorised online business activities including gambling.[10] This scope similarly applies to considerations to amend or expand pre-existing products and services.

International AML/CFT/CPF treaties and standards mandate that institutions participating in the financial system who introduce, amend or expand products and services, must duly:

[7] e.g by prudential authorities in other relevant FIC publications.
[8] of the FIA. Any entity that avails products and services within the scope of Item 13 of FIA Schedule 1, is an Accountable Institution which falls within the AML/CFT/CPF regulatory and supervisory framework.
[9] In some spheres referred to as Crypto assets (including crypto currencies).
[10] Any services wherein electronic movement of value is expected.

a. conduct comprehensive identification (or assessment) of potential Money Laundering (ML), Terrorism Financing (TF) and Proliferation Financing (PF) risks[11] that could emanate from the proposed new products or services, including amendments to pre-existing ones; and
b. use their understanding of such risks to duly guide the implementation of relevant control measures (in mitigating such risks).

At the discretion of the FIC, as per powers within the FIA, the FIC may require that Reporting Institutions (such as insurance service providers), listed in Schedule 3 of the FIA also comply with this Directive. It is thus not entirely limited to Accountable Institutions.[12]

The Directive, if complied with, not only ensures Namibia remains compliant with international AML/CFT/CPF obligations and standards but enables the relevant institutions to proactively employ necessary measures to practically manage risks of potential abuse. In the same vein, it enables the FIC, as regulatory body, to have an in depth understanding of risks associated with new products, services as well as amendments to existing products and services and to guide the prevention and combating framework accordingly.

3. AUTHORITY AND RATIONALE

As said above, persons availing services that facilitate the electronic transfers of money or value are required to comply with the FIA.

[11] Guide: consideration of all threats and vulnerabilities. Vulnerabilities refer to control shortcomings within the product or services that could be abused while threats would be those illicit activities that would undermine or take advantage of such shortcomings.

[12] Reporting Institutions (as per Schedule 3 of the FIA) such as insurance service providers have in the past approached the FIC with proposals to amend current service delivery frameworks of their pre-existing products/services, by, amongst others, introducing or making use of e-KYC mechanisms which enhances non-face-to-face engagements in customer relationships. All FATF publications indicate that non-face-to-face platforms are inherently more vulnerable to abuse as there is reduced effective due diligence. The context of expanding this requirement beyond Accountable Institutions will be at the discretion of the FIC, as per its appreciation of risks in each case before it.

This Directive is issued in terms of sections 9(2) read with the provision of section 54(2) of the FIA. The objective of the Directive is to ensure products and services or amendments to existing ones remain aligned to the national AML/CFT/CPF prevention and combatting framework. In furtherance of this, the Directive serves to ensure new products and services (or expansions or amendments to existing products and services) duly align to expectations in FIA sections 21; 22; 23; 24; 25[13]; 26; 27; 28; 32; 33 and 39, amongst others. Affected institutions are thus required to ensure that proposed control measures are aligned with all the relevant sections of the FIA.

4. SPECIFIC DIRECTIVES

4.1 Prudential licensing and regulation

4.1.1 General licensing and regulation requirements

Unless otherwise provided for in such other relevant laws, all financial services should be licensed by relevant prudential authorities such as the Bank of Namibia or Namibia Financial Institutions Supervisory Authority (NAMFISA).

The governance framework established in institutions, consequential to prudential regulations creates the needed foundation on which sound AML/CFT/CPF controls are build. It is for this reason that prudential licensing is a pre-requisite[14] for all proposed financial services seeking FIC consent as per this Directive. FIC's role as supervisory and regulatory body (in all aspects including position on new innovations and services) is limited to AML/CFT/CPF or compliance with the FIA and does not replace relevant prudential licensing and regulation.

At the time of Revising this Directive, regulatory engagements geared towards considerations of creating a local prudential regulatory framework for VASPs are ongoing.

[13] Where applicable.
[14] This position is also aligned to FATF Recommendation 26, sub-item 26.2.

When a position is taken on prudential regulation, VASPs registered with the FIC will be further directed to ensure compliance with such relevant legal frameworks that may arise. This Directive may therefore be revised if prudential positions so require.

4.1.2 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”).

The VASP definition includes persons availing certain services within the VA value chain. These include 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[15]. 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,[16] such as Bitcoin miners, provided that such are not involved in any of the activities mentioned above.

In ensuring effective risk based supervision and access to records by relevant AML/CFT/CPF combatting authorities, the FIC may[17] require a foreign based applicant (or such relevant service provider) to have a physical presence in Namibia, as stated in the Revised Directive 02 of 2021.

[15] The FIC may, when need be, amend the scope of this definition, depending on changes in risk exposure, in the advancement of its regulatory objectives as per section 9(2) of the FIA (and powers provided therein).
[16] If such persons however part take in selling and buying, brokering, agency or such other related services, they would be required to comply with the FIA.
[17] FIC discretion depending on various factors deemed necessary to advance risk management, supervisory and combatting objectives.

4.2 Conducting risk assessments and adopting effective controls

Accountable Institutions best understand their pre-existing and proposed products and services. These institutions are therefore best placed to identify and assess the level of ML/TF/PF risks they may be exposed to resulting from offering of their products and services. Equally, they have an obligation to ensure their proposed operations duly comply with the FIA. It is therefore required that such institutions:

a. **undertake a ML/TF/PF risk assessment**[18], the comprehensiveness of which should be aligned to the nature, complexity and risk exposure of their proposed products, services (or amendments thereto). The three main elements institutions are directed to consider, in addition to others that may arise are:

   i. *the **risk profiles of customers** to be served by such new products or proposed amendments, especially if some are Politically Exposed Persons (PEPs)*[19]*, foreign nationals or other such type of persons whose Customer Due Diligence (CDD) information cannot be effectively or readily verified. In the case of foreign customers, understand reliability of national identification systems in such country, the effectiveness of AML/CFT/CPF systems in such country etc.;*

   ii. ***description of products or services and relevant vulnerabilities of same:** such should be in so far as it relates to the ML/TF/PF vulnerabilities of such products and services. e.g if there are no direct or face-to-face*

[18] FIA section 39(1) read with FIA section 23: 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. Accountable Institutions must measure, rank or rate (e.g low, medium and high) their level of risk for relevant elements of the products, services, delivery channels, and clients they aim to provide. The control measures should describe how the entity will duly reduce (or mitigate) each level of inherent risk, especially the medium and higher risk rated levels. To ensure controls do not unduly undermine financial inclusion objects, institutions should duly explain the nature, type and extent of simplified due diligence measures they will subject low risk clients, products and services to (as per FIC sectoral Guidance Note 01 of 2022, *draft availed to FIC registered VASPs and finalised Guidance to be issued in April 2022*). The FIC may, in its interpretation however disagree with ratings not duly informed and request reconsiderations accordingly.

[19] See FIC Directive No. 02 of 2020 on PEPs as well as Guidance Note No. 01 of 2019 on the definition and due diligence required for PEPs: Both documents are available on the FIC Website under the “Publications” folder.

engagements, customer identification efficiency might not always be similar to face-to-face identifications; and

iii. ***delivery channels*** *(how you provide those products or services): for example, face-to-face, online customer engagements or a mixture of both. Cross border delivery channels could enhance domestic ML/TF/PF risk exposure, especially if the entity does not gain assurance that relevant AML/CFT/CPF frameworks in such other foreign jurisdictions are effective and reliable, relative to the proposed products or services.*

b. **Role of key stakeholders in the service provision or product delivery, if any:** if the operations as proposed would entail inputs from other stakeholders (different to the Accountable Institution or entity proposing same to the FIC), ensure that there is clarity around responsibilities to duly implement AML/CFT/CPF requirements as per the FIA. Matters such as availability of records[20], as and when where required by the institution (for timely and effective due diligence) or competent authorities,[21] are worth considering;

c. **Description of the nature of operations:** demonstrate to the FIC, the type, nature and extend of proposed controls to be implemented to reduce inherent[22] risks to tolerable or acceptable levels. The FIC must be satisfied, upon such presentation, that such residual[23] risk levels are tolerable or acceptable to the national AML/CFT/CPF framework;

d. **Aligning of controls:** for institutions already operating within the AML/CFT/CPF framework, should ensure such new products and services are aligned to the

[20] As per FIA record keeping obligations.
[21] As defined by the FIA.

[22] **Inherent** risks refer to the level of (original) risks prior to the implementation of controls to reduce the likelihood and impact of such risks.

[23] **Residual** risk refers to the level of exposure that exists after controls have been implemented. The remaining risk that the institution can tolerate. Consideration of impact and likelihood are essential in this regard.

approved internal AML/CFT/CPF program or policies.[24] As a matter of principle, compliance programs should dictate that the higher the risk, the more such should be subjected to enhanced or extensive risk management measures. This naturally implies that simplified due diligence should be applied to lower risk clients, products and services, as per FIC sectoral Guidance Note 01 of 2022. The existing program may be amended if the introduction of such (or proposed amendments) so require. Institutions are directed to ensure that at all times, the AML/CFT/CPF program in use is approved by relevant governance and accountable bodies (board or executive management) and such is at all times in compliance with the FIA; and

e. **Periodic review of controls:** if newly proposed control measures are implemented, institutions are directed to periodically review such AML/CFT/CPF controls[25] within the context of internal control framework (program), in line with evolving risks and update same when need be. The frequency of reviews should

[24] Overall principles of FIA section 23: Accountable institutions must 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. When developing customer identification and verification procedures, institutions must also: consider the risk posed by the beneficial owner/s of such customers; whether such customers or their beneficial owners are PEPs; the customers' financial profiles (source of income, wealth); the nature and purpose of the Accountable Institution's business relationship with such customers; the control structure of customers who are not individuals, such as companies and trusts. Consider Industry Guidance Note No.1 of 2015 on Identification and Verification of Beneficial Ownership Information. Available on the FIC website under "Publications": https://www.fic.na/index.php?page=2015-guidance-notes.
FIA section 39(3): Accountable and reporting institutions must develop, adopt and implement a customer acceptance policy, internal rules, programmes, policies, procedures and controls as prescribed to effectively manage and mitigate risks of money laundering and financing of terrorism activities.
FIA section 39(4): A customer acceptance policy, internal rules, programmes, policies, procedures referred to must be approved by directors, partners, or senior management of accountable or reporting institution and must be consistent with national requirements and guidance, and should be able to protect the accountable or reporting institution's systems against any money laundering and financing of terrorism activities taking into account the results of any risk-assessment conducted under subsection. For new entities/persons, ensure to duly designate or appoint a AML Compliance Officer in terms of section 39(6). Such Compliance Officer should be at management level and must be a skilled and independent individual within the entity charged with ensuring the day-to-day execution of the AML/CFT/CPF framework.

[25] Overall message in FIA section [read with 24 FIA section 39(1)]: On-going and enhanced due diligence: An accountable institution must exercise on-going due diligence in respect of all its business relationships which must, at a minimum, include - (a) maintaining adequate current and up-to-date information and records relating to the client and beneficial owner; (b) monitoring the transactions carried out by the client in order to ensure that such transactions are consistent with the accountable or reporting institution's knowledge of the client, the client's commercial or personal activities and risk profile; and (c) ensuring the obligations relating to high risk clients, as prescribed in FIA section 23, and correspondent banking relationships are fulfilled. This suggests effective simplified due diligence measures for low risk clients, products and services are implemented to ensure financial inclusion related interests are not unduly undermined.

be guided by changes in risks, internal control frameworks or such other relevant factors.

4.3 Registration

All VASPs, as defined herein, are hereby directed to ensure registration with the FIC before or on **30 September 2021**. FIC Directive No. 03 of 2020 avails more information in this regard and can be accessed on the FIC website, under Publications (https://www.fic.na/index.php?page=2020-directives).

Registration with the FIC does not amount to compliance with prudential regulations, nor does such registration imply compliance with all FIA provisions, as highlighted in Revised Directive 01 of 2021 on obtaining FIC consent before launching new products, services, or amending such existing ones. Accountable and Reporting institutions should thus ensure separately presenting their proposed products and services to the FIC, as stated herein, even if they are duly registered with the FIC.

4.4 Presentations to the FIC and measures post presentation

4.4.1 Prudential licensing and FIC consent

Conventionally, prudential compliance and licencing is required prior to FIC consent. This Directive will be amended to reflect same, if and when prudential licensing frameworks for VASPs are created domestically. All other non-VASP proposals are required to demonstrate having met relevant prior prudential compliance and licensing before FIC consent can be considered.

In ensuring that risks do not unduly undermine or expose the AML/CFT/CPF framework, the FIC has authority to only consent to the introduction or advancement of products and services that do not expose the financial system to ML/TF/PF risks as per the FIA. Thus, while prudential licensing is required to commence operations or the introduction of new

products and services, the FIC's powers and mandate to protect the financial system from ML/TF/PF abuse as per the FIA necessitates its consent for all such products and services. In order to facilitate the obtaining of FIC consent, all persons intending to introduce new products, services or amend pre-existing ones are directed to present information stated in section 4.2 above, and any other which may be additionally requested by the FIC.

4.4.2 Further exploratory exercises

With an enhanced understanding of relevant AML/CTF/CPF measures, the FIC may, in certain circumstances direct that the introduction or launch of new (or amended/expanded) products and service *first* be tried (operationalised) in a Regulatory Sandbox, within parameters preferred by the FIC and the relevant prudential regulators (if need be).

Note however that a sandbox is not the only regulatory tool that could be applied. Other options include a *test-and-learn* approach to try out new innovations under *ad-hoc* circumstances in a live environment or a *wait-and-see* strategy that allows for informal monitoring of new trends before any formal intervention is considered (e.g., P2P lending, cryptocurrencies). The *test-and-learn* as well as *wait-and-see* approaches would equally be expected to be executed within relevant prudential regulatory parameters.

With these different approaches, Regulatory Sandboxes are more structured, objective-driven and publicized, but also more formalistic, potentially costly and resource-intensive. The exploratory exercises cited herein are to be concluded as agreed between the applicant or service provider and the relevant regulator(s).

4.4.3 FIC turnaround time/period

The FIC's due diligence activities cited herein are generally additional to the activities of the licensing or prudential authorities. Therefore, considerations around planning for effective product or service launches should be considerate of such.
Generally, the FIC would be in a position to avail or express its position on proposed new products, services or such amendments to existing ones, within a period of 30 days, depending on various factors. The period required to complete such FIC due diligence depends on the nature and type of due diligence that is required, given the type of submission at hand. The FIC will communicate when more time is required (beyond the 30 days).

Institutions proposing to introduce new products and services or amending such existing ones should engage the FIC when shorter or different turnaround periods may be required. Based on circumstances of each submission, risk exposure, prudential regulatory positions etc., the FIC may reconsider its turnaround period.

5. INFORMATION TO BE SUBMITTED

Depending on the nature of operations, products and services at hand, it is an institution's prerogative to decide on the most suitable type, nature and form of information to submit which best demonstrates compliance with the requirements herein to the FIC and such other prudential authorities. The FIC reserves the right to request for any type of information (in any reasonable format) which may support its due diligence activities in this regard.

6. NON-COMPLIANCE WITH PROVISIONS OF THIS DIRECTIVE

The consequence of failure to register with the FIC or obtain such consent prior to the introduction of new products and services (including amendments to pre-existing ones)

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 also result in enforcement considerations as per the FIA.

7. GENERAL

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

8. QUERIES

Queries related to this Directive may be communicated with the FIC as per contact details on the cover page.

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

DIRECTOR: FINANCIAL INTELLIGENCE CENTRE