Republic of Nauru

VIRTUAL ASSET SERVICE PROVIDER POLICY

Registrar of Business Licences
Financial Intelligence Unit

Table of Contents

VIRTUAL ASSET SERVICE PROVIDER POLICY

TABLE OF REVISIONS

The Virtual Asset Service Provider Policy was published on 6 October 2023.

Revision Date	**Published**
22 February 2024	20 March 2024
10 April 2024	20 May 2024

Introduction

Nauru as a member of the Asia Pacific Group on Anti-Money Laundering is committed to the implementation of the 40 FATF Standards. *Recommendations 15* of the FATF standards, require the regulation of Virtual Assets Service Providers. These are financial institutions that provide the following:

- exchange between virtual assets and fiat currencies;
- exchange between one or more forms of virtual assets;
- transfer of virtual assets;
- safe keeping or administration of virtual assets or instruments enabling control over virtual assets; and
- participation in a provision of financial services relating to issuers, offers or sale of virtual assets.

Nauru currently does not have any financial institutions that provide the services referred to above. For this reason, this policy was developed to anticipate the establishment of such institutes in Nauru. One of the main objectives of this policy is to ensure, that the same transparency and accountability requirements applying to traditional and conventional financial institutes, also apply to VASPs. This must be done to ensure Nauru is protected from the abuse of electronic systems for laundering money for the financing of terrorism or proliferation financing.

This Policy provides for the requirements of *Recommendation 15* of the FATF Standards. It explains what a VASP is and how a VASP is regulated in Nauru under the current legislative framework. The Policy also identifies who is a Supervisor of VASP, how a Supervisor can identify illegal operators and what the mode of supervision is.

Further, in anticipation of VASPs being established in Nauru, the policy provides a guide as to how VASPs can identify AML/CFT Risk. The Policy has adopted the FATF-developed Red Flag Indicators of which there are 6, to establish a guide that VASPs can follow to meet their obligations under the *Anti-Money Laundering and Targeted Financial Sanctions Act 2023*

The Policy also sets out the obligations a VASP is to comply with where suspicious activities are detected. It explains how and to whom reports must be made. It further explains the offences and penalty schemes that are applicable to VASPs.

The Policy further explains other obligations of VASPs relating to customer due diligence, wire transfers and targeted financial sanctions. An explanation of international cooperation mechanisms in place is also included. It also explains the obligations of VASPs to keep records in accordance with the AML-TFS Act and in turn the FATF Standards.

It is anticipated, that should VASPs formally establish in Nauru, this Policy will aid its establishment and provide a clear guide on the requirements it must meet and obligations it must adhere to.

Key terms

The key terms used in this policy are set out below:

'AML/CFT' means anti-money laundering and combatting the financing of terrorism;

'AML-TFS Act 2023' means the *Anti-Money Laundering and Targeted Financial Sanctions Act 2023;*

'Banking Act' means the *Banking Act 1975;*

'BO' means a beneficial owner defined under the *Beneficial Ownership Act 2017;*

'BO Act 2017' means the *Beneficial Ownership Act 2017;*

'BLA 2017' means the *Business Licence Act 2017;*

'BNRA 2018' means *Business Names Registration Act 2018;*

'CO Act 1972' means the *Corporations Act 1972*;

'CTTOC' means the *Counter Terrorism and Transnational Organised Crime Act 2004;*

'FATF' means the Financial Action Task Force;

'FPPC' means fit and proper person criteria;

'POCA' means the *Proceeds of Crime Act 2004;*

'transfer' in the context of virtual assets 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;

[definition insrt; per FATF Standard 15.3(b) and footnote 123]

'VAs' or ***'virtual assets'*** means a digital representation of value that is digitally traded or transferred and that can be used for payment or investment purposes, but does not include digital representations of fiat currencies.

'VASPs' means virtual asset service providers which is also defined under the AML-TFS Act 2023 as a financial institution that provides services in relation to virtual assets including but not limited to:

(a) the exchange between virtual assets and fiat currencies;
(b) the exchange between one or more forms of virtual assets;
(c) the transfer of virtual assets;
(d) the safekeeping or administration of virtual assets or instruments enabling control over virtual assets; and
(e) the participation in the provision of financial services relating to issuers offer or sale of virtual assets;

FATF Recommendation 15

Recommendation 15 of the FATF Standards requires:

> *'Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise concerning:*
>
> *(a) the development of new products and new business practices, including new delivery mechanisms; and*
>
> *(b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.*
>
> *To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.'*

What is a VASP?

A VASP as defined by the FATF is mirrored in Nauru's AML-TFS Act 2023. The definition can be found in Section 4, definition of ***'financial institution'***; *paragraph (n)*. A VASP means:

> *'any natural person or legal entity engaged in the conduct of the following activities or operations:*
>
> *....*
>
> *(n) provision of services in relation to virtual assets, including, but not limited to:*
>
> *(i) exchange between virtual assets and fiat currencies;*
>
> *(ii) exchange between one or more forms of virtual assets;*
>
> *(iii) transfer of virtual assets;*
>
> *(iv) safekeeping 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 or sale of a virtual asset.'*

How are VASPs regulated under Nauru's written laws?

There are no known VASPs currently operating in Nauru. However, should a VASP intend to commence operations it would have to comply with the requirements set out below, before commencing operations.

(a) If a VASP is a legal entity

If:

(i) a VASP is established as a corporation, it has to be incorporated under the CO Act 1972;

(ii) a VASP is established as a partnership, it has to be established under the *Partnership Act 2017;* or

(iii) a trust establishes a VASP, the trust has to be created under the *Trusts Act 2018.*

It does not matter under which legislation it is established, it will need to obtain a business licence under the BLA 2017.

(b) Must register a business name

In addition to obtaining a business licence, a VASP will be required to register a business name under the BNRA 2018. A business cannot operate unless it has registered a business name under the BNRA 2018.

(c) Must obtain a business licence

Section 6 of the BLA 2017 does not allow a person to *'commence or carry on any business without a licence*' granted under that Act. *Section 2* of the Act also defines a business as *'any form of economic activity…carried on…for the purpose of generating revenue for gain.'* It is clear from the definition of a VASP, that it operates within the scope of the definition of a business. Therefore, a VASP will be required to obtain a business licence in order to operate in Nauru.

(d) Must register beneficial ownership

As a legal entity the VASP will be required to comply with the requirements of the BO Act 2017. The beneficial ownership details are contained in *Beneficial Ownership (Forms and Fees) Regulations 2017* and the *Beneficial Ownership (Identification) Regulations 2023.* It is important for any proprietor to understand the requirements for registration and if they need any clarification, they should seek assistance of the Authority.

Also, under the BO Act 2017, a legal entity would be required to appoint a nominated officer.

There is a Manual which provides detail on how beneficial ownership is to be registered. It is available on the website and a copy can be obtained from the Authority.

Who is a Supervisor of VASPs in Nauru?

The VASPs are not actually recognised as a separate operation in Nauru. However, since VASPs will be conducting businesses they will be subject to other laws as discussed above. As such the Supervisory Authority will be the Registrar of Corporations, Registrar of

Partnership, Registrar of Trusts, Registrar of Business Names and Registrar of Business Licences.

A VASP is subject to the requirements of *Recommendation 15* of the FATF Standards as such, the activities and operations will be subject to the requirements of the AML-TFS Act 2023. For that purpose the FIU will also supervise VASPs for AML/CFT activities.

The FIU will also be the responsible authority for assessing ML/TF risks associated with VASPs and as per Section 85(k) of the AML-TFS Act, will release guidance or other materials to inform stakeholders.

[Am per FATF Standards IO 3 and 4 and R15, 22 Feb 2024]

How can a Supervisor of VASPs identify illegal operators of VASPS? [R15.5]

Under Nauruan law, the screening process for illegality will begin at the time when a VASP is found to be carrying on business. The obligation is on the VASP to have the requisite business licence and it must be established in accordance with the laws for registering a business. At this preliminary level, VASP will be caught in contravening the laws for which the administrative penalties as well as more severe penalties through prosecution in court will be imposed. These are contained in the BLA 2017 and the other Acts referred above. As soon as the illegality is detected other laws such as BO Act 2017 come into play.

Once illegality is traced, the VASP will be required to comply with the laws. In that case, whatever penalties and sanctions are applicable needs to be paid before the VASP will be able to rectify all illegality. In addition, the VASP operation can be shut down by the Registrars of various entities. Also, if it is a foreign operator the person's presence in Nauru will be declared unlawful and the natural person or any person responsible in Nauru will become a prohibited immigrant under the *Immigration Act 2014*.

Since Nauru does not have any such operators currently to its knowledge, there are no laws made for them. However, any such presence will certainly be met with a proper legislative framework which will have further sanctions consistent with the requirements of *Recommendation 15.5*. Those fines would be separate for individuals and corporations.

Mode of supervision (sole and joint with FIU) [R15.6]

Since VASP are not currently under any special legislation, it is only appropriate that they will be supervised by the FIU for most part on their operations. However, the normal requirements for business registration etc. will allow the Supervisors there to jointly work with the FIU.

Red flags to assist VASPs identify AML/CFT risks

The FATF have issued a guideline of Red Flag Indicators to assist not only countries supervisors and authorities in monitoring VASPs activities but also VASPs in identifying AML/CFT risks in their day to day operations. The Red Flag Indicators identified by the FATF are by no means exhaustive. However, for Nauru's purposes, the Red Flag Indicators are provided in this Policy for reference. There are 6 Red Flag Indicators set out below.

(a) Red Flag Indicators Related to Transactions

The rationale for identifying red flags relating to transactions is because they are frequently used by criminals to transfer funds. According to the FATF Guideline *'while VAs are not widely used by the public, their use has caught on among criminals'*[1].

In saying that, the FATF red flag indicator relating to transactions that VASPs must pay attention to is set out below:

'***Size and frequency of transactions***

- *Structuring VA transactions (e.g. exchange or transfer) in small amounts, or in amounts under record-keeping or reporting thresholds, similar to structuring cash transactions.*

- *Making multiple high-value transactions:*

    - *in short succession, such as within a 24-hour period;*

    - *in a staggered and regular pattern, with no further transactions recorded during a long period afterwards, which is particularly common in ransomware-related cases; or*

    - *to a newly created or to a previously inactive account.*

- *Transferring VAs immediately to multiple VASPs, especially to VASPs registered or operated in another jurisdiction where –*
    - *there is no relation to where the customer lives or conducts business; or*
    - *there is non-existent or weak AML/CFT regulation.*

- *Depositing VAs at an exchange and then often immediately:*

    - *withdrawing the VAs without additional exchange activity to other VAs, which is an unnecessary step and incurs transaction fees;*

[1] FATF Report: Virtual Assets – Red Flag Indicators of Money Laundering and Terrorist Financing, 2020; p5

- *converting the VAs to multiple types of VAs, again incurring additional transaction fees, but without logical business explanation (e.g. portfolio diversification); or*

- *withdrawing the VAs from a VASP immediately to a private wallet. This effectively turns the exchange/VASP into an ML mixer.*

- *Accepting funds suspected as stolen or fraudulent –*
  - *depositing funds from VA addresses that have been identified as holding stolen funds, or VA addresses linked to the holders of stolen funds.*'

(b) Red Flag Indicators Related to Transaction Patterns

The FATF red flag indicator relating to transaction patters are discussed under 2 subheadings which are *'Transactions concerning new users'* and *'Transactions concerning all users.'* The FATF red flag demonstrates to the VASP how VAs can be used for AML/CFT purposes by studying the transaction patterns of users.

'Transaction concerning new users

- *Conducting a large initial deposit to open a new relationship with a VASP, while the amount funded is inconsistent with the customer profile.*

- *Conducting a large initial deposit to open a new relationship with a VASP and funding the entire deposit the first day it is opened, and that the customer starts to trade the total amount or a large portion of the amount on that same day or the day after, or if the customer withdraws the whole amount the day after. As most VAs have a transactional limit for deposits, laundering in large amounts could also be done through over-the-counter-trading.*

- *A new user attempts to trade the entire balance of VAs, or withdraws the VAs and attempts to send the entire balance off the platform.*[2] '

'Transactions concerning all users

- *Transactions involving the use of multiple VAs, or multiple accounts, with no logical business explanation.*

- *Making frequent transfers in a certain period of time (e.g. a day, a week, a month, etc.) to the same VA account –*

  - *by more than one person;*

  - *from the same IP address by one or more persons; or*

[2] ibid; p7

- *concerning large amounts.*

- *Incoming transactions from many unrelated wallets in relatively small amounts (accumulation of funds) with subsequent transfer to another wallet or full exchange for fiat currency. Such transactions by a number of related accumulating accounts may initially use VAs instead of fiat currency.*

- *Conducting VA-fiat currency exchange at a potential loss (e.g. when the value of VA is fluctuating, or regardless of abnormally high commission fees as compared to industry standards, and especially when the transactions have no logical business explanation).*

- *Converting a large amount of fiat currency into VAs, or a large amount of one type of VA into other types of VAs, with no logical business explanation.*[3]*'*

(c) Red Flag Indicators Related to Anonymity

It is important to note that the red flag indicators relating to anonymity is not by itself a red flag. This red flag indicator must be considered in parallel with or *'in context of other characteristics about the customer and relationship or a logical business explanation.*[4]*'* The FATF red flag red indicators relating to anonymity that VASPs are set out below.

- '*Transactions by a customer involving more than one type of VA, despite additional transaction fees, and especially those VAs that provide higher anonymity, such as anonymity-enhanced cryptocurrency (AEC) or privacy coins.*

- *Moving a VA that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange and then immediately trading it for an AEC or privacy coin.*

- *Customers that operate as an unregistered/unlicensed VASP on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customers handle huge amount of VA transfers on its customer's behalf, and charge higher fees to its customer than transmission services offered by other exchanges. Use of bank accounts to facilitate these P2P transactions.*

- *Abnormal transactional activity (level and volume) of VAs cashed out at exchanges from P2P platform-associated wallets with no logical business explanation.*

[3] ibid; p8
[4] ibid; p9

- *VAs transferred to or from wallets that show previous patterns of activity associated with the use of VASPs that operate mixing or tumbling services or P2P platforms.*

- *Transactions making use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces.*

- *Funds deposited or withdrawn from a VA address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports.*

- *The use of decentralised/unhosted, hardware or paper wallets to transport VAs across borders.*

- *Users entering the VASP platform having registered their Internet domain names through proxies or using domain name registrars (DNS) that suppress or redact the owners of the domain names.*

- *Users entering the VASP platform using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs. Transactions between partners using various anonymous encrypted communication means (e.g. forums, chats, mobile applications, online games, etc.) instead of a VASP.*

- *A large number of seemingly unrelated VA wallets controlled from the same IP-address (or MAC-address), which may involve the use of shell wallets registered to different users to conceal their relation to each other.*

- *Use of VAs whose design is not adequately documented, or that are linked to possible fraud or other tools aimed at implementing fraudulent schemes, such as Ponzi schemes.*

- *Receiving funds from or sending funds to VASPs whose CDD or know-your customer (KYC) processes are demonstrably weak or non-existent.*

- *Using VA ATMs/kiosks –*

    - *despite the higher transaction fees and including those commonly used by mules or scam victims; or*

    - *in high-risk locations where increased criminal activities occur.*

A single use of an ATM/kiosk is not enough in and of itself to constitute a red flag, but would if it was coupled with the machine being in a high-risk area, or was used for repeated small transactions (or other additional factors).[5] *'*

(d) Red Flag Indicators about Senders or Recipients

This FATF-developed red flag indicator helps the VASP to assess the profile and any out of the ordinary behavior of a sender or a recipient of a transaction. The red flag indicators for senders or recipients are discussed under three different headings which are '*irregularities observed during account creation*', *'irregularities observed during CDD process'* and *'profile'* The FATF-developed red flag indicators are set out below:

'Irregularities observed during account creation

- *Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by VASPs.*
- *Transactions initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious.*
- *Trying to open an account frequently within the same VASP from the same IP address.*
- *Regarding merchants/corporate users, their Internet domain registrations are in a different jurisdiction than their jurisdiction of establishment or in a jurisdiction with a weak process for domain registration.*[6] *'*

'Irregularities observed during CDD process

- *Incomplete or insufficient KYC information or a customer declines requests for KYC documents or inquiries regarding the source of funds.*
- *Sender / recipient lacking knowledge or providing inaccurate information about the transaction, the source of funds, or the relationship with the counterparty.*
- *Customer has provided forged documents or has edited photographs and/or identification documents as part of the onboarding process.*[7] *'*

'Profile

- *A customer provides identification or account credentials (e.g. a non-standard IP address, or flash cookies) shared by another account.*

[5] ibid; pp9 - 10
[6] ibid; p12
[7] ibid; p12

- *Discrepancies arise between IP addresses associated with the customer's profile and the IP addresses from which transactions are being initiated.*

- *A customer's VA address appears on public forums associated with illegal activity.*

- *A customer is known via publicly available information to law enforcement due to previous criminal association.*[8] *'*

'Profile of potential mule or scam victims

- *The sender does not appear to be familiar with VA technology or online custodial wallet solutions. Such persons could be money mules recruited by professional money launderers, or scam victims turned mules who are deceived into transferring illicit proceeds without knowledge of their origins.*

- *A customer significantly older than the average age of platform users opens an account and engages in large numbers of transactions, suggesting their potential role as a VA money mule or a victim of elder financial exploitation.*

- *A customer being a financially vulnerable person, who is often used by drug dealers to assist them in their trafficking business.*

- *Customer purchases large amounts of VA not substantiated by available wealth or consistent with his or her historical financial profile, which may indicate money laundering, a money mule, or a scam victim.*[9] *'*

'Other unusual behaviour

- *A customer frequently changes his or her identification information, including email addresses, IP addresses, or financial information, which may also indicate account takeover against a customer.*

- *A customer tries to enter into one or more VASPs from different IP addresses frequently over the course of a day.*

- *Use of language in VA message fields indicative of the transactions being conducted in support of illicit activity or in the purchase of illicit goods, such as drugs or stolen credit card information.*

- *A customer repeatedly conducts transactions with a subset of individuals at significant profit or loss. This could indicate potential account takeover and*

[8] ibid; p13
[9] ibid; p14

attempted extraction of victim balances via trade, or ML scheme to obfuscate funds flow with a VASP infrastructure.[10] *'*

(e) Red Flag Indicators in the Source of Funds or Wealth

The FATF developed red flag indicators to assist VASP in flagging unusual transactions where the source of funds or wealth are questionable or suspicious. These red flag indicators are set out below:

- *'Transacting with VA addresses or bank cards that are connected to known fraud, extortion, or ransomware schemes, sanctioned addresses, darknet marketplaces, or other illicit websites.*

- *VA transactions originating from or destined to online gambling services.*

- *The use of one or multiple credit and/or debit cards that are linked to a VA wallet to withdraw large amounts of fiat currency (crypto-to-plastic), or funds for purchasing VAs are sourced from cash deposits into credit cards.*

- *Deposits into an account or a VA address are significantly higher than ordinary with an unknown source of funds, followed by conversion to fiat currency, which may indicate theft of funds.*

- *Lack of transparency or insufficient information on the origin and owners of the funds, such as those involving the use of shell companies or those funds placed in an Initial Coin Offering (ICO) where personal data of investors may not be available or incoming transactions from online payments system through credit/pre-paid cards followed by instant withdrawal.*

- *A customer's funds which are sourced directly from third-party mixing services or wallet tumblers.*

- *Bulk of a customer's source of wealth is derived from investments in VAs, ICOs, or fraudulent ICOs, etc.*

- *A customer's source of wealth is disproportionately drawn from VAs originating from other VASPs that lack AML/CFT controls.*[11]*'*

(f) Red Flag Indicators related to Geographical Risks

The red flag indicators developed by the FATF relating to geographical risks help VASPs identify suspicious or questionable transactions related to countries or places that are considered to be high risk. These red flag indicators are set out below.

[10] ibid; p15
[11] ibid; p15

- '*Customer's funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located.*

- *Customer utilises a VA exchange or foreign-located MVTS in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for VA entities, including inadequate CDD or KYC measures.*

- *Customer sends funds to VASPs operating in jurisdictions that have no VA regulation, or have not implemented AML/CFT controls.*

- *Customer sets up offices in or moves offices to jurisdictions that have no regulation or have not implemented regulations governing VAs, or sets up new offices in jurisdictions where there is no clear business rationale to do so.*[12]'

Reporting of suspicious activities to Supervisor or FIU

As a reporting entity, a VASP may use the red flag indicators set out above, to generate a Suspicious Activity Report which is required under *Section 59* of the AML-TFS Act 2023. The Suspicious Activity Report is to be provided to the FIU Supervisor.

Additionally, as business or corporation operating in Nauru, the VASPs would also be required to use the red flag indicators to generate a report of suspicious activities to the relevant supervisors. These are the:

- Registrar of Businesses for the operation of a business;
- Registrar of Corporations if the VASP is a corporation; and
- FIU Supervisor.

Sanctions [R15.8]

The AML-TFS Act 2023 makes provision for proportionate and dissuasive sanctions. *Section 48, 58, 67, 78, 79 and 80(5)* of the AML-TFS Act 2023 applies to VASPs.

Under *Section 17* of the AML-TFS Act 2023, it provides that the same penalties for the legal entities apply to Senior Management of the VASP.

It is important for every operator to realise that it must comply with the laws of Nauru. The financial penalty in Nauru is very severe. The separation of the penalty from the legal entity needs to be understood. If the legal entity by which the VASP is operating contravenes any laws, the entity itself will be prosecuted. In addition to the entity, the Senior Management staff or team may also be prosecuted. The Board of the legal entity may also be prosecuted if it knowingly allowed the VASP to operate without complying with all the legal requirements in Nauru.

If VASP is involved with operations that may amount to money laundering or for that matter funding any terrorist organisation or proliferation financing, the penalties are very severe

[12] ibid; p17

which includes life imprisonment. The relevant laws which apply for these offences are CTTOC and AML-TFS Act 2023.

In addition to these requirements Nauru very strongly follows and requires all entities to comply with the requirements of AML/CFT.

Customer due diligence

Depending on the nature of business the VASP is undertaking, it is a requirement under *Recommendation 15.9 for VASPs* to undertake customer due diligence for its customers. Customer due diligence require a VASP to comply with Part 4 of the AML-TFS Act 2023. In summary this requires on certain occasions *simplified due diligence* (for regular customers), and *enhanced customer due diligence* (for first time customers and in many cases where the nature of business the customer undertakes is complex and involves a substantial sum of money).

In undertaking customer due diligence if any suspicious activity is made known to the VASP it must immediately report the same to the FIU.

Under *Section* 59 of the AML-TFS ACT 2023, all reporting entities are required to report any suspicious activity. In any event any transactions beyond $10,000 AUD must be subject to customer due diligence, including occasional transactions. In the case of a VASP, the obligation is also for VASP to ensure to undertake CDD for an occasional transaction which is in excess AUD 1,500 or its equivalent value in any other currency or virtual currency.

[para rev per; FATF Standards; Criterion 15.9(a)]

The VASP is also required to provide details of how it conducts customer due diligence, to its customers. It must develop a policy which should be readily available for customers' inspection.

Wire Transfers

Recommendation 15.9(b) specifically requires VASPs to comply with *Recommendation 16* of FATF Standards. This Recommendation deals with wire transfers. For the purposes of wire transfers, the VASP will be required to keep and maintain records of the following:

(a) originating VASPs are to obtain and hold required and accurate originator information, beneficiary information on all virtual asset transfers, financial institutions;

(b) beneficiary VASPs must obtain and hold all required originator information and required and accurate beneficiary information on virtual asset transfers and make it available to the FIU;

(c) requirements of any freezing action or prohibition action with designated persons or entities; and

(d) the obligations which apply to financial institutions when sending or receiving transfers on behalf of a customer.

The records are to be kept in accordance with the requirements of the records referred to later in this Policy.

Targeted Financial Sanctions

Nauru has recently passed the targeted financial sanctions in the AML-TFS Act 2023. Also, regulations have been made under the CTTOC. *The CTTOC (Targeted Financial Sanctions) Regulations 2023* have domesticated all the United Nations Security Council resolutions in respect of terrorists, terrorist groups and terrorist activities. Together with the requirements under the AML-TFS Act 2023, VASPs will be required to comply with the requirements for *Criteria 6.5(d); 6.5(e), 6.6(g), 7.2(d). 7.2(e). 7.3 and 7.4(d).*

In essence this requires the VASP to monitor all the communications mechanisms, reporting obligations and monitoring for terrorist activities.

If the VASP is involved in stock exchange, it is important that the sale of stocks on market is carefully monitored.

Range of international cooperation

This is available under various laws. The AML-TFS Act provides for mechanisms of international cooperation. Equally the same is provided for in more detailed procedures under the *Mutual Assistance in Criminal Matters Act 2004 and POCA.*

Records

Nauruan law requires all business and entities to keep and maintain their records during the currency of the business. The reference to '*keep and maintain'* means that the information kept must be recorded properly and when new information is available it must be updated on a regular basis.

It is a requirement that updated information is to be provided to the relevant supervising authority which includes the Registrars of various businesses, Registrar of Business licence and in this case also the FIU.

Additionally, FATF *Recommendation 11* requires that all records of the entities are to be kept for 5 years even if the VASP be wound up, dissolved or ceases operation. Nauru requires that all records are to be kept for a period of 7 years. The limitation period under the *Limitations Act 2017* has a limitation period of 6 years.

Beneficial ownership information is to be kept for 7 years as well. It is anticipated that this information will be kept by the nominated officer. However, if the nominated officer is to leave Nauru, such information is to be provided to the Authority.

In case of VASP, the information, VASPs are required to keep the following information:

(a) originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities;

(b) beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers, and make it available on request to appropriate authorities;

(c) other requirements of R.16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis as set out in R.16; and

(d) the same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.

[para insrt; per Criterion 15.9 of FATF Standards; 9 Apr 2024]

Contact

This Policy is issued jointly by the Registrar of Business Licences and the Supervisor of the FIU. The contact persons are:

(a) Wiley Detenamo: Deputy Registrar – wdetenamo@gmail.com

(b) Rajas Swamy: FIU Supervisor – rajasswamy@gmail.com