



REPUBLIC OF NAURU

# Nauru Financial Intelligence Unit

## Standard Operating Procedures

---

# Contents

Introduction .....	4
Functions of FIU .....	4
Security .....	5
Initial processing of a SAR.....	8
Types of reports REs provide to the FIU .....	10
Sources of information to analyse the SAR.....	14
Gathering information .....	16
Analysing the information.....	16
Preparing a financial intelligence brief for an investigation.....	18
Rules for sharing of information.....	22
FIU's role in ensuring compliance.....	23

## **Table of Abbreviations**

AML/TFS ACT 2023 – Anti-Money Laundering and Targeted Financial Sanctions Act 2023

SARS Regulations – Anti-Money Laundering and Targeted Financial Sanctions (Suspicious Activity Report) Regulations 2023

BCR – Border Currency Report

CDD – Customer Due Diligence

DPP – Director of Public Prosecutions

FIU – Financial Intelligence Unit

FFIU – foreign financial intelligence unit

KYC – Know Your Customer

LEA – Law Enforcement Agency

NFMRA – Nauru Fisheries and Marine Resources Authority

NMPA – Nauru Maritime and Ports Authority

PEP – Politically Exposed Person

PFIC – Pacific Financial Intelligence Community

POCA 2004 – Proceeds of Crime Act 2004

Record Keeping Regulations – Anti-Money Laundering and Targeted Financial Sanctions (Record Keeping) Regulations 2023

RE – reporting entity(ies)

s – section

SMR - Suspicious Matter Report

SAR – Suspicious Activity Report

## Introduction

The purpose of this document is to describe the standard operating procedures to be followed by the Nauru FIU in performing its functions and in exercising related powers.

The FIU is the key operational unit in a reporting and monitoring system established by the AML/TFS ACT 2023. The purpose of the AML/TFS ACT 2023 is to improve Nauru's capability to detect and deter money laundering, terrorist financing and all serious crimes with appropriate sanctions. The POCA 2004 complements the AML/TFS ACT 2023 by providing for the confiscation of proceeds of serious offences and establishing provisions for enforcing border currency reporting.

The AML/TFS ACT 2023 and the system of reporting and monitoring, establishes general models and approaches used and endorsed internationally.

The Independence of the FIU is stipulated under s.74 of the AML-TFS Act 2023 with the FIU having its own budget. The FIU is established within the Department of Justice and Border Control reporting administratively to the Secretary for Justice.

The Minister for Justice is responsible for the appointment of the FIU Supervisor in consultation with the Cabinet under s.70 whilst the FIU officers are appointed in accordance with s.71 of the AML-TFS Act 2023. The FIU Supervisor makes the final determination on the appointment of the FIU Officers.

## Functions of FIU

The AML/TFS ACT 2023 (s.69) provides the FIU with the following functions.

*'(1) The FIU shall have the following functions:*

- (a) to enforce this Act;*
- (b) to supervise the compliance of reporting entities with this Act;*
- (c) to receive and analyse suspicious activity reports and other information available to it, whether by any means or under any law, in order to identify activity that may constitute or may relate to a financial crime or criminal conduct and to carry out any further investigations it considers necessary;*
- (d) to disseminate information derived from analysis and reports of information received under paragraph (c) to domestic and foreign law enforcement bodies or foreign intelligence bodies;*
- (e) to enquire into conduct that constitutes as or relates to financial crime or is suspected to do so;*

- (f) *to conduct related inquiries, investigations, analysis and oversight;*
- (g) *to identify, analyse and assess on an ongoing basis financial crime trends, patterns and risks of relevance to the Republic, including in relation to new technologies, business practices and products;*
- (h) *to coordinate with supervisory authorities and other authorities in the Republic that have a role in combatting financial crime or criminal conduct;*
- (i) *to engage in an arrangement, understanding or any mutual cooperation with similar foreign entities in other countries or international bodies on matters relating to financial crime or criminal conduct;*
- (j) *where necessary, may commence proceedings in any court established in the Republic for the purposes of enforcing any part of this Act or any other written law, in the performance of its functions;*
- (k) *to ensure that reporting entities, supervisory authorities, other competent authorities and the public at large are adequately informed about the trends, patterns and risks of financial crime and the appropriate responses; and*
- (l) *such other functions which may be given to the FIU by any written law, the Cabinet or the Minister.*

(2) *The Financial Intelligence Unit shall have all such powers that are necessary to give effect to or for carrying out its functions under subsection (1).'*

Under Division 2, Part 5 of the AML/TFS ACT 2023, the FIU has wide powers; Power relating to information exchange with domestic authorities (s.77); Power to conduct inspection (s.78); Power to require a RE to produce certain information (s.79); Power to require certain persons to produce information relating to business relationships, accounts and transactions (s.80); Powers to enforce compliance (ss.81-83).

As part of its functions under the AML-TFS Act 2023 stated above, the FIU will:

- a. continue to engage in evaluating and monitoring of Proliferation Financing activities on a risk-based approach in collaboration with all stakeholders; and
- b. Continue to monitor and follow up on all international requests for quality, timeliness and consistency similar to the approach to SAR's (refer to page 21).

## **Security**

### ***Protecting information and its sources***

The FIU cannot work without the close cooperation and effective compliance of REs. Information provided by REs to the FIU can be extremely sensitive. It is vital that REs have confidence in the security and proper handling of the

information they provide. The experience of other FIUs has shown that if REs are to cooperate with the FIU, they must trust the FIU not to disclose the source of the reports they provide it with, including either the name of the reporting officer or the name of the organisation. Improper disclosure of information may jeopardise the safety of staff in REs and harm their business. Such disclosure could also harm the reputation and effectiveness of the FIU. If it is perceived amongst REs that improper disclosure may occur, they may not report future suspicious transactions. The AML/TFS ACT 2023 makes this security requirement explicit in: Appointment of officers of the FIU at s.71(3); Limitations on compliance with request at s.99(1)(b); and resonated throughout the Act dealing with disclosures.

There are a number of measures, described below, that can and must be taken to ensure security is not breached and information is provided to the FIU via appropriate disclosure methods.

### ***Confidentiality Agreement***

All officers of the FIU shall undertake an oath of Secrecy as a mandatory requirement to fulfill his/her role within the ambits of the AML/TFS ACT 2023. (The oath is Annexed to this SOP as Attachment A.)

### ***Vetting Staff***

All officers of the FIU are vetted in accordance with the policies of the Government and in accordance with the Act.

Each officer of the FIU must report to the Head of the FIU (the FIU Supervisor) any change in their circumstances which could harm either the reputation or the effectiveness of the FIU. The FIU Supervisor shall report any change in his or her circumstances to the Chairperson of the Anti-Money Laundering Governance Council.

### ***Office security***

#### **Access to the FIU – Authorised Officers**

The FIU will be located within secure self-contained area and located within the department of Justice and Border Control. Normal access to any part of the premises is restricted to the FIU Supervisor and officers of the Financial Intelligence Unit.

The FIU office shall remain locked at all times when unattended, including short periods.

It is the responsibility of the last officer who leaves the office to ensure that it is secure. When unattended, all computers should be security locked (e.g. by logging out of the computer), and every computer must be shut down at the end of every day.

### **Visitor access to the FIU**

To gain entry to the FIU office, visitors must be on FIU business and must be accompanied at all times by the Supervisor or officers of the Financial Intelligence Unit. [REDACTED]

### **Secure information storage**

All reports from REs and related documentation [REDACTED]

All information received from [REDACTED]

The following items will be stored in the FIU [REDACTED]

- [REDACTED]

[REDACTED] This is to ensure no one else can access the folder.

The Supervisor must ensure that the FIU staff adhere to the ICT policy established for FIU to keep access to FIU computers and laptops secure. [REDACTED]

Printing of any confidential report and documentation is prohibited unless approved by the FIU Supervisor and shall be done for the purposes of manual record keeping obligations only if necessary.

### **Hours of Operation**

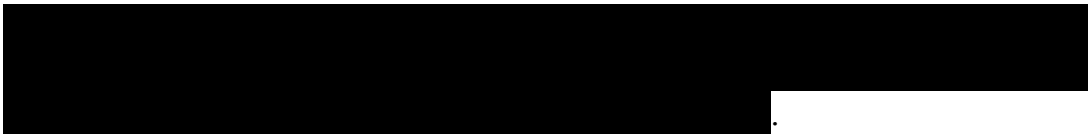
The FIU shall be open from 9.00 am to 5.00 pm, Monday to Friday as per the usual business hours. However, the FIU Supervisor may authorise any work to be undertaken after hours.

The AML/TFS ACT 2023 (s.59) obliges REs to report suspicious transactions to the FIU within 2 working days of the transaction occurring. REs or other stakeholders will often seek advice from the FIU about their reporting obligations which should be timely, reliable and easy to access. Some urgent requests – for example concerning customs or immigration border seizures – may occur out of regular office hours.

If the FIU is unattended for any reason, including weekends, the FIU supervisor must ensure arrangements are made to ensure that an officer can be contacted by alternative means and outside of official business hours by the relevant REs, remittance providers or government authorities – particularly Police, Customs and Immigration officials.

## **Initial processing of a SAR**

Upon receipt of a SAR, the following steps must be taken:

1. Assessment – is it urgent or has merit?
  - Need to monitor or restrain assets? Key issues that need to be considered include: whether you wish to request the RE to monitor activity in the account, and whether the situation appears serious enough to apply for an order to restrain particular assets.
2. Date the reports received manually or create sub folder under SAR. This will later assist with assessing the compliance of REs with reporting deadlines.
3. Assign file number and create file online.
4. 
5. Enter report into database.
6. Check report for completeness of information.
  - If necessary, request from the RE any information omitted from the report form.
  - Record any further information received on a file note. Note that officers must not use further information to fill in gaps in the submitted SAR



form<sup>1</sup>. Note the date when further information was provided and its completeness.

- Enter further information provided into the database.

7. Note any significant omission of the information in the database.

- Note whether information was collected by the RE and not included or whether the RE had not collected the information. This will help when giving performance feedback and supervising compliance.

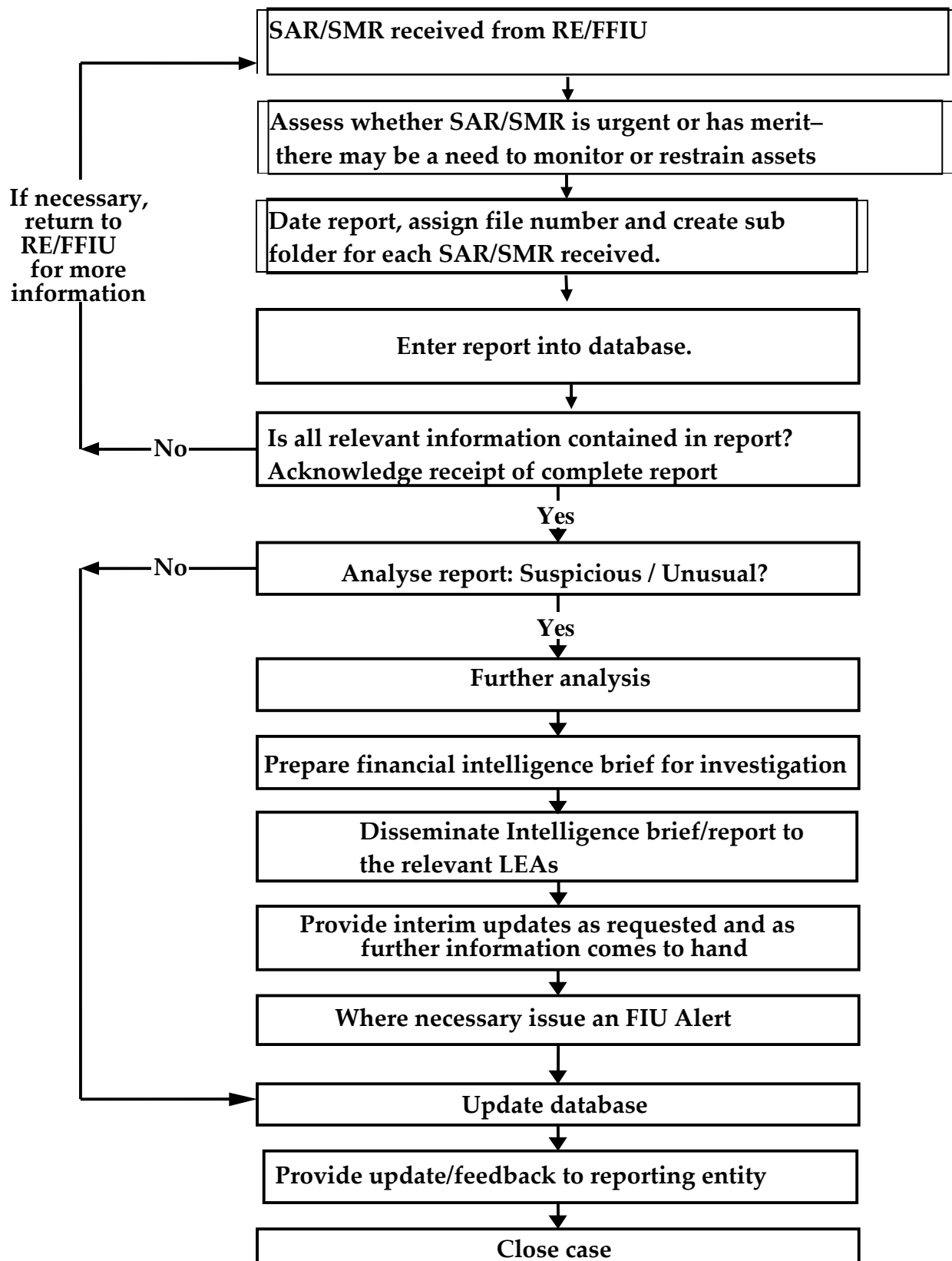
8. Complete acknowledgement letter/email for RE and send.

## **Overview of report (SAR/SMR) handling procedure**

The diagram below summarises the main steps from receipt of the SAR or SMR to potential completion of financial/intelligence analysis.

---

<sup>1</sup> This is to ensure the original report is not compromised.



## Types of reports REs provide to the FIU

In brief, REs or supervisory authorities must report any transaction that they suspect may be related to the commission of a money laundering offence, a

financing of terrorism offence or an unlawful activity (s.59 AML/TFS ACT 2023) or where they have reasonable suspicion of such offences occurring. Customs and Immigration authorities must report any suspicion of the breach of the declaration requirements of cross-border movements of cash, precious stones or metals or bearer negotiable instruments in the value of more than \$5,000 (POCA 2004, s.9B).

REPORT TYPE	REPORTED WHEN	NOTES
<b>SARs</b>	A RE or supervisory authority has reasonable grounds to suspect that information that it has concerning the transaction may be relevant to the investigation or prosecution of a money laundering offence, a financing of terrorism offence or a criminal conduct (s.59, s.61 and s.62 AML/TFS ACT 2023).	<p>'criminal conduct' is defined by s.4 of the AML/TFS ACT 2023.</p> <p>'activity' is defined by s.4 of the AML/TFS ACT 2023.</p> <p>not including a law relating to non-payment or avoidance of any form of taxation.</p>
<b>Border Currency Reports</b>	<p>Customs and authorised officers who form the suspicion that a breach of the declaration requirements of cross-border movements of cash, precious stones or metals or bearer negotiable instruments in the value of more than \$5,000 (POCA 2004, s.9B).</p> <p><i>There are no services available in Nauru to convert foreign currency or realise BNI, bank cheques, personal cheques, traveler's cheques and money orders.</i></p>	<p>Section 97 of POCA 2004 refers to both Customs officers and 'authorised officers'.</p> <p>Examples of bearer negotiable instruments include bank cheques, personal cheques, traveler's cheques and money orders.</p>
<b>FFIU SARs/SMRs</b>	Where a FFIU forms a suspicion that there are reasonable grounds to suspect that information that it has concerning any Nauru related transactions/activity may be relevant to the investigation or prosecution of a money laundering offence, a financing of terrorism offence or a criminal conduct whether in or outside of Nauru (s.69(1)(c))	Some FFIU only report if there is an existing bilateral arrangement mechanism in place. That is, between Nauru FIU and the FFIU.

## Method of delivering reports to the FIU

REPORT TYPE	METHOD OF DELIVERY
Border Currency Reports (POCA 2004 s.96)	<ul style="list-style-type: none"> <li>The method of delivery should be through a secure channel. Electronic means (e.g. email) is the preferred option.</li> </ul>
SAR/SMR (AML/TFS ACT 2023 s.59, s.61 and s.62)	<p><b>Choosing the method of delivery</b></p> <p>The method of delivery of a SAR will depend on the circumstances of the report.</p> <ul style="list-style-type: none"> <li><b>Verbal Communication (including Phone):</b> Some SARs may refer to an imminent crime, or potential irrecoverable transfer of tainted funds (e.g. transfer out of Nauru), thus requiring rapid transmission to the FIU.</li> </ul> <p>For these reasons, advising the FIU of a suspicious transaction immediately is essential. REs must supply the FIU with an electronic copy of the SAR in the form in Attachment B. This must be submitted within 2 working days of forming the suspicion, whether they have previously spoken to the FIU or not. Where email access is not available, a paper SAR will suffice. (s.59 AML/TFS ACT 2023 and SARs Regulations)</p> <p><b>Methods of delivery</b></p> <p>Delivery of the reports must have regard to the likely delivery time, with preference given to that method of delivery which ensures the timely delivery of reports to the FIU, this may include:</p> <ul style="list-style-type: none"> <li><b>Hand collection or delivery:</b> REs in Nauru and FIU staff, may prefer to deliver or collect SARs in person given the sensitivity of the report and also, may want to discuss the context in which the report arose. The FIU Supervisor and officers may wish to collect such reports in person, but only where this is practical and would not compromise the confidentiality of the REs identity.</li> <li><b>Paper mail:</b> This may be an option where the SAR is not urgent and could be delivered within 2 working days via paper mail. REs should contact the FIU before using this option.</li> <li><b>Email:</b> This is the preferred option. In such cases it is essential that REs advise the FIU of the report by telephone or email prior to sending it electronically, as this will assist the FIU in maintaining the SAR</li> </ul>

confidential.

As far as applicable, REs should use the SAR form attached in Attachment B.

## **Feedback**

After handling and completing a task or information request ; or as in an ongoing case during information gathering process, the FIU shall continue to provide feedback to its stakeholders.

The feedback can be provided as follows:

- Verbally. This can be done at the time FIU meets with the stakeholders for meetings etc;
- Over the phone when the FIU is in discussions of the same matter or other matters;
- Via emails when responding to information requests or enquiries;
- Formally where the FIU is provided with a feedback form;
- Electronic means such as emails and monkey surveys; and
- In a manner preferred by the stakeholder.

The FIU may seek feedback from the stakeholders in the same manner as specified above.

Law enforcement authorities must report AML/CFT related matters to the FIU. This should include risks identified, methods and trends.

## Sources of information to analyse the SAR

The information needed to help you decide if the transaction warrants investigation could come from a range of sources:

### 1. *The FIU database*

Using this database, you can cross-check details of the new reports with previous reports, including items such as:

- the personal and/or business names;
- account numbers;
- phone numbers and addresses;
- methodology; and
- structuring, etc.

If the new SAR details match any previous SAR that was referred for investigation, FIU shall advise the investigator or agency of the new SAR and to confirm whether or not the new SAR matches any previous SAR.

### 2. *Criminal history information from Police sources*

- Nauru Police Force;
- Interpol;
- Foreign Law Enforcement Agencies;
- FFIU; and
- Open Source (google etc.)

### 3. *Information from Customs or Immigration sources.*

Customs and Immigration officials may provide helpful information, and may wish to receive a report from the FIU, if the transaction relates to suspicious import or export of goods or funds.

- **Note:** Sections 97 and 98 of the POCA 2004 states that an 'authorised officer' may seize and detain, for up to 28 days, any currency, bearer negotiable instruments and precious metals or stones that is being imported into or exported from Nauru. That is if there are reasonable grounds for suspecting that it is derived from or intended to be used in a serious offence. A court may order continued detention of the funds (s 98).
- **Note:** 'serious offence' is defined under Section 3 of the POCA 2004.

### 4. *Other Nauru Government sources*

- Department of Justice and Border Control;
- Register of Business Names;
- Register of Business Licences;

- Register of Corporations;
- Register of Partnerships;
- Register of Beneficial Ownership;
- Register of Private Security;
- Register of Trusts;
- Register of Associations;
- Register of Import Licences;
- Bendigo Agency;
- Nauru Trustee Corporation;
- Nauru Maritime and Port Authority;
- Vehicle or ship registration details;
- Department of Finance;
- Nauru Fisheries and Marine Resources Authority; and
- Any other agency the FIU identifies.

**Note:** Section 77(b) of the AML/TFS ACT 2023 which provides the FIU with the authority to request information from any law enforcement agency, government institution or agency supervisory authority.

## ***5. Records of the RE***

Consider checking the previous business or transaction history of the customer at the RE, and whether there are related accounts.

REs will usually provide such information freely and willingly. However, in relation to coercive powers, Sections 77, 78, 79 and 80 of AML/TFS ACT 2023 explains the circumstances under which an officer of the FIU can be given access to the premises of a RE to inspect and copy records and reports.

**Note:** For the enforcement of the record keeping requirements, the FIU must after confirming a suspicion report the suspected breach by reporting entity to the relevant supervisory authority. Refer to regulation 5 of the Record Keeping Regulations.

**Note:** 'supervisory authority' is defined under Section 4 of the AML/TFS ACT 2023.

## ***6. The 'World Check' database.***

World-Check includes international data from many official sources on people with previous convictions for financial crime, and people wanted for terrorist activity. World-Check also enables you to check the validity of passport information.

## ***7. FFIUs***

FFIUs may also have information on the subject of the SAR, especially where transnational crime is suspected (e.g. the Solomon Islands, Australia, Kiribati, Vanuatu, and Fiji – In absence of being a member of EGMONT, the NFIU may enter into formal agreements such as letters of bilateral cooperation to share information. This is to be undertaken on a case by case basis.)

The NFIU is a member of the PFIC. The FIU is to actively participate in project work and information sharing with the members of the PFIC and contribute to the PFIC. The FIU shall promote a multi-lateral information sharing mechanism with PFIC to further strengthen information sharing with regional counterparts.

## **8. Google**

Google is a powerful intelligence gathering open source tool (<http://www.google.com/>). The advanced search function should be used, as you can search for an exact name, address, number or phrase, and avoid many irrelevant results.

## **Gathering information**

The key task of the FIU is to use all information sources to find out more about the SAR, until it can decide whether the SAR should be formally investigated, or closed on the database.

In verifying the information sources, check whether any of the key details on the SAR match with the information being searched. For example, but not limited to:

- the name of the person conducting the transaction;
- the recipient of the transaction;
- names of any other person associated with the sender or recipient;
- residential or business address, of either sender, recipient or associates;
- company titles (if any);
- telephone numbers; and
- bank account numbers.

## **Analysing the information**

Conducting the SAR check in the manner provided above, creates a better position to decide whether further action is necessary. The following analytical questions will help in making that decision.

### **1. Does the transaction still appear suspicious?**



- Review the reasons given for suspicion in the SAR form. Do they still seem credible? Are the transactions consistent with the nature of business?
  - Is the transaction consistent with what is known now about the sender, receiver and any associates?
  - Are these subjects (Persons of Interest or entities) engaged in a business or activity consistent with the transaction?
  - What is known about their previous conduct? What is known about them and their reputation in their locality?
2. *What type of offence(s) is suspected to have generated the funds in the transaction?*
- What did the receiver of the money provide in return? For example, if it is an unusual payment to a public official, could it be a bribe?
  - Could the suspected offence amount to criminal conduct or a financial crime?
  - **Note:** 'criminal conduct' and 'financial crime' are defined under Section 4 of the AML/TFS ACT.
3. *Could there be a genuine explanation for the transaction?*
- Do the people involved have access to legitimate sources of this amount of cash?
  - Could there be both legitimate and illegitimate purposes for the transaction – e.g. payment for tobacco and cannabis?
4. *Is financial or other monitoring necessary?*
5. *Have there been similar transactions previously? Is another suspicious transaction likely?*

*Next steps following analysis:*

- 1) *No suspicious activity indicated, or insufficient information to draw any conclusions*
- Endorse comments with steps undertaken & enquiries conducted.
  - Update database and sub-folder for relevant SAR.
  - Complete advice to reporting institution (email/phone).

- Close case

*Note: If there is more than 1 SAR received against a person or body, a single file should be created if the facts are the same. However, if the facts and circumstances are different, then a different file should be created.*

**OR**

***2) Analysis reveals a possible (more probable than not) case of criminal conduct, financial crime or other offences which can only be determined by a formal investigation***

- Create a financial intelligence brief for investigation.
- Forward the financial intelligence brief to the relevant law enforcement agency.
- Conduct interim updates as requested and when further information comes to hand.
- Upon receipt of the completed investigation report or brief, update the FIU database and the SAR sub-folder.
- Close case.

***3) Making a Request for Information***

Where there is a need to make a request for additional information or a new request in any matter whether domestic or international, the following rules must be applied:-

- Ensure complete and accurate information is provided.
- A brief description of the case.
- Indicate whether the request is urgent.
- Consider any other information that is important to the particular request.

This is to ensure that there is a clear indication on the urgency of the request so that the request can be executed in a timely and efficient manner.

## **Preparing a financial intelligence brief for an investigation**

### **1. Summary of the SAR**

*Brief description of the suspicious activity*

- For example: “A customer of a supermarket, Harold Ronaldo, used its alternative remittance service to send three large sums of money overseas during a two-month period – a total of \$37,000. This is inconsistent with both Mr. Ronaldo’s occupation as a Government clerk, and his history with the supermarket (he had never previously used its alternative remittance services).”

### *Transaction details*

- Names (including any businesses involved), addresses and phone numbers.
- Type of transaction.
- Account names and numbers (if applicable) – sender and receivers.
- Bank branch (if applicable).
- Amounts.
- Dates.

## **2. Explanation of the transfer**

### *RE’s reasons for suspicion*

- List any other reasons provided by the RE for suspecting the transaction may be associated with proceeds of crime – for example:
  - Unrealistic wealth compared to client’s occupation or business.
  - Other – “Mr. Ronaldo appeared anxious when sending the remittances. On the most recent transfer, he was accompanied by people who waited outside the supermarket. Combined with his small income, this suggested he may have been making the transactions for other people.”
- List any ‘know your customer’ (KYC) information provided by the RE – e.g. alternative names, identification presented, other account signatories, known sources of income or business activity.

### *Results of FIU information gathering and analysis*

- *Information sources:* List the checks made by the FIU – including the results – positive or negative – of any database searches or other enquiries.
- *Potential criminal activity:* Describe any results from FIU information gathering and analysis. For example, “One of the ideal issues to be explored further is that the transaction may involve stolen government funds or proceeds from bribes. When the FIU checked the details of the receiver with AUSTRAC, the Australian FIU, it was discovered that the receiver is a company suspected of involvement in money laundering. One

of its Directors is a Nauruan citizen, Mr. X, who is listed in the World Check database as having a conviction for fraud. Mr. X is a family relation of a senior Nauru Government official (a Politically Exposed Person, or PEP).”

- *Associates*: list suspects and people of interest, describing:
  - who they are – role, and apparent connection to suspicious transaction or activity;
  - any legitimate sources of income – occupation and business activities;
  - any known criminal history; and
  - residential and business addresses and contact details.

### **3. Alternative explanation for the transfer**

- List any plausible alternative explanations for the activity.

### **4. Recommendations**

- *Further information gathering*: identify potential further enquiries, particularly interviews, with people, REs, or government agencies, and provide contact details. Identify any accounts or people or assets that should be monitored. Note any additional enquires the FIU could undertake if necessary (e.g. further contact with other FIUs).
- *Further information dissemination*: Note any information that may be relevant to other Nauru government agencies – e.g. Customs, Immigration authorities, statutory agencies (NFRMA, NMPA etc.) or RE’s where necessary.
- *Identify any higher priority activities*: In cases that may involve flight/escape of suspects or assets, identify any potential use of the asset restraint or forfeiture provisions of the AML / TFS ACT 2023 (Section 97) and POCA (Part 3).

### **5. Documents enclosed with the report**

- Attach any reports that may assist the investigation – e.g. copies of results of database searches.
- Note: The SAR dissemination report shall not be used as a disclosure or as evidence under any circumstances, including, investigation or in court. Only use the information on the SAR to develop the brief. The identity of

the RE must be protected at all times. For investigation purposes, the police officers conducting the investigation shall obtain relevant documents from the institution concerned:

- through their normal procedures for a search warrant

## **6. Law Enforcement & Other Requests**

- The FIU is authorised to receive requests from local and foreign law enforcement agencies (includes FFIUs) and supervisory authorities.
- Depending on the nature of requests, all requests shall be processed in the same manner as defined above for processing of SARs.
- Any variation or when conducting a due diligence on behalf of the Republic shall be approved by the FIU Supervisor.

**Note:** *The FIU may refuse to provide any request for assistance received if in the opinion of the FIU the requesting foreign government or international organisation is not adequately able to protect the confidentiality of any information that has been requested. This approval shall come from the FIU Supervisor and the grounds of such refusal must be communicated to the requesting agency, unless it is in the national interest not do so. (s.89 AML/TFS ACT 2023)*

## **7. Assessment of quality and consistency of information received**

- When receiving information pertaining to requests made (both domestic and international bodies), the FIU must confirm the following:
  - the information received is specifically related to the request made;
  - all the information requested has been received;
  - whether there are any restrictions applying to the information provided; and
  - where a request has been refused – whether the reason for such refusal has been provided.

## **8. Method of Dissemination**

- The preferred method is via a dedicated, protected and secure channel which would be via email (preferred).
- Ensure the report and attachments are protected documents (password secured).
- The password to be sent via a separate email, phone or verbally disclosed to the recipients.

- However, where it is deemed that sending reports via emails is a potential risk, the report and attachments shall be hand delivered in a sealed envelope.

## **Rules for sharing of information**

1. The FIU must not disclose to anyone the original reports received in accordance with the AML/TFS ACT 2023. However, the contents of such reports, may be used to generate an investigation brief by the FIU.
2. The FIU must not disclose the source of information received, relating to AML/CFT contravening activities unless so directed under a court order.
3. Information may be shared with domestic and foreign or international bodies. The rules prescribed in the AML-TFS Act 2023 must be adhered to. In particular, such information sharing must be done with the required confidentiality and non-disclosure requirements.
4. Where information to be shared is **intelligence**, it must be shared in a timely manner even if the **intelligence** is not of use to the FIU but may be useful to another LEA.
5. The FIU may share information/reports arising out of operational and strategic analysis with all stakeholders. This will ensure that stakeholders are aware of the methods and crime trends in the Republic.

**The strategic analysis reports may be made available on the FIU Website.**

## **FIU's role in ensuring compliance**

The AML/TFS ACT 2023 creates a number of legal obligations for REs, including: making SARs, conducting CDD measures and ensuring appropriate records are kept. The FIU is tasked with ensuring REs fulfil these obligations. In doing so, the FIU has powers under the AML/TFS ACT 2023 to monitor (ss.77 - 79), issue guidelines (s.85) and provide training to REs (s.85).

### ***The Compliance Role of the FIU***

#### **Education**

One of the functions of the FIU is to raise awareness of money laundering and financing of terrorism offences and the obligations people have under the relevant legislation. This includes the following tasks:

- Issuing guidelines (s.85) and providing training to REs in relation to customer identification KYC, CDD, record keeping, reporting obligations and identification of suspicious transactions (s.85(d));
- Providing periodic feedback to REs and other relevant agencies regarding outcomes relating to the reports or information given under the Act (s.8(e)); and
- Educating the public and creating awareness on matters relating to money laundering and financing of terrorism including relevant legislation and international requirements (s.85(k)).

#### **Compliance and monitoring**

In order to ensure that REs comply with the AML/TFS ACT 2023, the FIU has functions (s.69) and powers (ss.77-79) to:

- examine the records and inquire into the business risk assessment, internal controls and obligations of any RE (s.78(2)); and
- instruct REs to take appropriate steps in order to ensure compliance with the AML/TFS ACT 2023 (s.69).

REs in turn must provide FIU officers 'all reasonable assistance' and any information they may reasonably require for compliance purposes under the AML/TFS ACT 2023 (s.78(5)).

Where a RE fails to comply with a directive issued by the FIU to ensure compliance with the Act, the FIU may report the non-compliance to the relevant supervisory authority or under s.81 apply to the court for an order against any or all officers or employees of a RE.

## **Correspondent banking relationships**

The AML/TFS ACT 2023 requires REs to perform various due diligence measures when establishing cross-border correspondent banking relationships (S.46(2)). These include:

- obtaining sufficient information about the respondent entity to understand fully the nature of its business;
- determining from publicly available information, the reputation of the respondent entity, the quality of the supervision to which it is subject and whether it has been subject to investigation or regulatory action in respect of financial crime; and
- assess the respondent entity's financial crime controls and ascertain whether they are adequate and effective.

## **Record Keeping**

REs are required by the AML/TFS ACT 2023 and the Record Keeping Regulations to fulfil various record keeping obligations. Records of all transactions carried out by it should be detailed enough to enable the FIU or law enforcement authorities to reconstruct any transaction and use the details as evidence in court. They should include:

- the name, address and business/occupation of client;
- how the RE verified the identity of the person;
- the nature and date of the transaction;
- the type of currency and amount involved;
- the type and account numbers of any accounts involved; and
- the name of the employee who conducted the transaction.

In addition, documents that have been used to verify the identity of a customer needs to be kept. Records of all reports to the FIU and any enquiries made by the FIU to the RE should also be kept by REs.

Records must be kept for a minimum period of 7 years under the AML/TFS ACT 2023 (s.29).



Sources of technical advice and support:

- Basel Committee ‘Core Principles Methodology’ and criteria to assess the adequacy of ‘KYC policies and procedures’ (<https://www.bis.org/bcbs/>)
- [www.worldcheck.com](http://www.worldcheck.com)
- Asia Pacific Group on Money Laundering ([www.apgml.org](http://www.apgml.org))
- Egmont Group of FIUs (<https://egmontgroup.org>)
- Financial Action Task Force (<https://www.fatf-gafi.org/>)
- Australian Transaction Reports and Analysis Centre (<https://www.austrac.gov.au>)
- Pacific Financial Intelligence Community (<https://www.austrac.gov.au>)
- <https://www.moneylaundering.com>

**Review**

This SOP has been reviewed to remove references to the Repealed *Anti-Money Laundering Act 2008* and updated to refer to the new *Anti-Money Laundering and Targeted Financial Sanctions Act 2023* and the *Proceeds of Crime Act 2004* as amended by the *Proceeds of Crime (Amendment) Act 2023*.

Person responsible for SOP:	<b>FIU Supervisor</b>
Effective Date	04.05. 2018
Review Date	04.05.2022
Review Date	13.09.2023
Date for next review	14.09.2024

# Attachment A



**REPUBLIC OF NAURU**

**FINANCIAL INTELLIGENCE UNIT**

## **OATH OF SECRECY**

I, **(name)**, do solemnly swear that I will faithfully, truly and to the best of my knowledge, judgement and ability, execute and perform the duties required of me as a **Supervisor /Staff** of the Nauru Financial Intelligence Unit. Except in the course of judicial proceedings where so required under a court order, I will not disclose, communicate or convey or allow to be disclosed, communicated, or conveyed directly or indirectly to any person, any private or confidential information whatsoever obtained by me or in or about the performance of my duties or by virtue of my position.

I hereby swear that I will not allow any person or persons to inspect or have access to any written statement, FIU reports, records, emails, correspondence or any other information over which I have any control and I will conscientiously endeavour to prevent any person from inspecting or having access to any such information as aforesaid. Whatever I see or hear of a confidential nature or that is confided to me in my official capacity will be kept ever secret unless revelation is necessary in the performance of my duty.

**Dated this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_\_.**

\_\_\_\_\_  
**PRINT NAME**

\_\_\_\_\_  
**SIGNATURE**

\_\_\_\_\_  
**WITNESS (PRINT NAME)**

\_\_\_\_\_  
**WITNESS SIGNATURE**







<b>PART F - DETAILS OF REPORTING ENTITY</b>	
<b>36. Full name of business</b> (including branch where applicable):	<b>37. Business address</b> (physical address/Postal address):
<b>38. Details of Reporting Officer</b> (eg. Financial crime compliance officer) Full name (including title): _____ Phone number: _____  Job title: _____ Fax number: _____	
<b>39. Financial institutions internal reference number</b> (if applicable):	<b>Send completed marked as 'CONFIDENTIAL' forms to:</b>
	<b>Supervisor-Nauru Financial Intelligence Unit</b> Government Buildings, Yaren District, Nauru
<b>40.</b> This statement is made pursuant to the requirement to report suspicious activities under the laws of Nauru on the grounds detailed in Division 5 of Part 4 of the Anti-Money Laundering and Targeted Financial Sanctions Act 2023.  Signature of authorised person (eg. Financial crime compliance officer): _____  Date (day/month/year): _____	<b>For assistance contact:</b>
	<b>Nauru Financial Intelligence Unit</b>
	Phone:5573388 Fax: Email: rajasswamy@gmail.com
	<b>Nauru Financial Intelligence Unit Use Only</b>
	Report Number: Authorisation: