



# GUIDELINES FOR SUSPICIOUS TRANSACTION REPORTING

# **Table of Contents**

Dog	cument Information	2
Dod	cument Review History	2
Def	initions	3
Acr	onyms and Abbreviations	4
1.	Scope and Application of These Guidelines	5
2.	Introduction	6
3.	Money Laundering	6
4.	Terrorist financing and Proliferation financing	7
6.	Why Submit an STR	8
7.	When to Submit the STR	8
8.	Who Submits the STR	9
9.	How to Identify a Suspicious Transaction or Activity	. 11
	9.1. Indicators of Suspicious Transactions or Activity	. 11
10.	How to complete the STR form	. 12
11.	How to Submit a STR	. 14
12.	Receipt of STR by the FIU	. 15
13.	Feedback on STRs	. 15
14.	Further Requests for Information	. 15
15.	Rejection of STRs	. 15
16.	Failure to Submit STR	. 16
17.	Tipping Off	. 16
18.	Protection for Persons Reporting STRs	. 17
19.	Record Keeping	. 17
	Annexure 1.0: Indicators of suspicious transaction/activity	. 18
	Annexure 2.0 Industry specific indicators	. 19
	Annexure 3.0 Steps on how to complete the STR form	. 23
	Annexure 4.0 High Quality versus low quality STR	. 27

# **Document Information**

Document Owner	Financial Intelligence Unit
Creation Date	December 2021
Version	V1.0

# **Document Review History**

Date	Version	Document Amendments/Insertion
December 16 <sup>th</sup> , 2021	V1.0	Document Creation

#### **Definitions**

**AML/CFT Act 2020** means the Anti-Money Laundering and Countering the Financing of Terrorism Act, 2020.

**Cash** includes notes and coins of Seychelles or of any other country which is a legal tender and accepted as a medium of exchange in the country of its issue, postal orders, bearer cheques which passes title thereto upon delivery including travelers' cheques, bank drafts and bearer bonds.

**Cash Transaction Threshold Reports** means a report which reporting entities ("REs") are required to file with the FIU for executing cash transactions above the prescribed threshold in terms of section 5 of the AML/CFT Act.

**Financial Intelligence Unit** means the unit established under section 10 of the AML/CFT Act.

**Proliferation Financing** means the act of providing funds or financial assistance or service, which may, in whole or in part, be used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and due use goods used for non-legitimate purposes), in contravention of the Laws of Seychelles, where applicable, and international obligations as per section 20B of the Prevention of Terrorism Act, 2004 as amended.

**Reporter** means a compliance officer ("CO") or an alternate compliance officer ("ACO") appointed in terms of section 34(1) and 34(3) of the AML/CFT Act and who shall be responsible for submitting STR to the FIU.

**Reporting Entities** means an entity or persons specified in the First Schedule of the AML/CFT Act (see Annexure 1.0).

**Suspicious Transaction Report ("STR")** means a report on an activity or a transaction or series of transactions made, to be made or attempted to be

made, by a RE under section 48 of the AML/CFT Act.

**Terrorist Financing activities** means the provisioning of material support in the form of funds to terrorist acts, terrorist and terrorist organizations and covered under section 5 of the Prevention of Terrorism Act, 2004 as amended.

**Transaction** includes an attempted transaction, regardless of the amount of the transaction.

Wire Transfer Threshold Report ("WTTR") means a report that REs are required to submit to the FIU in line with section 5 of the AML/CFT Act for executing wire transfers above the prescribed threshold.

# **Acronyms and Abbreviations**

ACO	Alternate Compliance Officer			
AML/CFT ACT 2020	Anti-Money Laundering and Countering the Financing of			
	Terrorism Act 2020			
СО	Compliance Officer			
CTTR	Cash Transaction Threshold Report			
DNFBPs	Designated Non-Financial Businesses and Professions			
FI	Financial Institution			
FIU	Financial Intelligence Unit			
ML	Money Laundering			
PF	Proliferation Financing			
RE	Reporting Entity			
STR	Suspicious Transaction Report			
TF	Terrorist Financing			
WTTR	Wire Transfer Threshold Report			

#### 1. Scope and Application of These Guidelines

- 1.1 These guidelines provide practical assistance and comprehensive approach for REs of all sizes and across all sectors in recognizing suspicious transactions and meeting their reporting obligation under section 48 of the AML/CFT Act, to the Financial Intelligence Unit ("FIU").
- 1.2 These guidelines are issued by the FIU pursuant to section 27 (1) (j) of the AML/CFT Act. It aims to assist REs specified under the First Schedule of the AML/CFT Act, to meet their Suspicious Transaction Reporting obligations in terms of section 48 (1) of the AML/CFT Act.
- 1.3 These guidelines provide a general guidance on the reporting obligation and procedures for submitting Suspicious Transaction Reports to the FIU in line with section 48 of the AML/CFT Act. In particular, it explains reporting timelines, the information that must be included in the Suspicious Transaction Report ("STR") and the procedure for submitting reports electronically to the FIU.
- 1.4 The FIU emphasises that the contents of these guidelines are to provide general information and guidance only, as such do not represent all the requirements of the law. It is also not intended to act as a substitute to the reader's own assessment, nor relieve the user of this guideline from the responsibility to exercise their own skill, knowledge and due care in relation to the specific circumstances of the transaction/activity. As such, these guidelines are not intended to constitute legal advice from the FIU nor is it intended to replace the AML/CFT Act.
- 1.5 It is important that REs do not confuse STR with the currency transaction threshold report such as the Cash Transaction Threshold Report ("CTTR") and Wire Transfer Threshold Report ("WTTR"). CTTR and WTTR are merely threshold reports and the transaction(s) may not

necessarily involve criminal conduct. If the RE suspects that any service or transaction may be related to the commission of a criminal conduct, including an offence of money laundering or terrorist financing activities, it shall submit an STR to the FIU, in line with the requirements under section 48 of the AML/ CFT Act and related Regulations.

#### 2. Introduction

Money Laundering and Terrorist Financing ("ML/TF") is an ever-evolving process and individuals involved in such activities are continuously attempting to exploit services and products offered by REs in an effort to disguise the true nature of their illicit proceeds. As such having a robust regime for reporting on suspicious transactions is regarded as an essential element of the Anti-Money Laundering and Combating the Financing of Terrorism framework for every jurisdiction.

#### 3. Money Laundering

Money laundering is the processing of criminal proceeds to disguise its illegal origin. Therefore, through money laundering, criminals can make illicit proceeds appear legitimate.

There are three stages involved in the money laundering process:



Placement - The introduction of illegal proceeds into the financial system

Layering – This involves a series of conversions or movements of funds to distance them from their source

Integration - The laundered funds are entered into the legitimate economy.

#### 4. Terrorist financing and Proliferation financing

Terrorists use money to plan and execute their attacks but also to grow as an organisation. They need access to funds to acquire weapons, fund trainings, for travelling and accommodation purposes. It is important to note that terrorism financing can originate from legitimate as well as criminal sources. To fight terrorism, we have to disrupt and prevent these terrorism-related financial flows and transactions. The stages of TF are illustrated below.



Similarly, to TF, PF allows the development and movement of weapons of mass destruction which eventually leads to loss of life. Below is an illustration of the stages of PF.

# Raise Obscure Procure

REs are also required to submit an STR when they detect transactions and activities that relate to TF or PF. Refer to annexure 1.0 for the list of indicators to TF and PF transactions. These indicators are offered as a guide and it is not an exhaustive list of every possible indicator.

# 5. The Legal Obligation to submit a STR

A RE must submit an STR to the FIU, if a transaction or activity has been conducted or attempted by or through its institution and it knows or suspects that the transaction or activity may relate to ML/TF activities. The requirement to report suspicious transactions applies to all types of transactions or activities regardless of whether cash is involved or not. Thus, non-cash transactions, such as wire transfers or other activities, that may appear suspicious should also be reported.

- 5.1. The obligation to report in terms of section 48 (1) (a)(i) and (ii) of the AML/CFT Act, arises where a RE has;
  - reasonable grounds to suspect that any activity, or transaction may be related to the commission of criminal conduct including an offense of ML/TF activities or to money or property that is or represents the benefit of criminal conduct;
  - (ii) information that may be-
  - (A.) relevant to an act preparatory to an offence or to money or property referred to in paragraph (a) (i) of the AML/CFT Act;
  - (B.) relevant to an investigation or prosecution of a person for an offence referred to in paragraph (a) (i) of the AML/CFT Act; or
  - (C.) of assistance in the enforcement of this Act or the Proceeds of Crime Civil Confiscation Act.

#### 6. Why Submit an STR

Through the submission of an STR, the RE is helping in the detection and disruption of illicit flow of funds. The reporting of suspicious transactions is a major function of an effective AML/ CFT program of a reporting entity. Therefore, it is of utmost importance that REs develop good knowledge and understanding of their customers, their business and the related transactions. This will ensure that REs detect suspicious activities/ transactions and submit STRs which are of high quality to the FIU. The FIU can also through the analysis of STRs identify patterns and trends and ultimately detect emerging threats to the financial system.

As such, to assist the FIU to develop better-quality financial intelligence reports, it is important that the information being provided in the STR is accurate and complete.

#### 7. When to Submit the STR

A RE shall submit an STR to the FIU within two business days of ascertaining the reasonable grounds, forming the suspicion or receiving the information.

7.1. Non-business days are excluded from the counting of the prescribed reporting

period. The following are considered non-business days:

- i. Sunday
- ii. Official regular public holiday; and
- iii. Officially declared public holiday.

#### 8. Who Submits the STR

The obligation to report suspicious transactions in line with section 48 of the AML/CFT Act applies to all REs (as specified under the first schedule of the AML/CFT Act, as amended listed hereunder.

#### **PART A**

A licensee under the Financial Institutions Act.

Any entity to which the Financial Institutions (Application of Act) Regulations, 2010 apply.

A licensee under the Credit Union Act.

A licensee under the Financial Leasing Act.

A payment services provider and operator of a payment, clearing or settlement system under the National Payment System Act, excluding the Central Bank of Seychelles.

#### PART B

A Fund Administrator licensed under the Mutual Fund and Hedge Fund Act.

A licensee under the Securities Act, except an investment advisor's representative or a securities dealer's representative;

A licensee under the Insurance Act:

A licensee under the Seychelles Gambling Act, 2014

A licensee under the International Corporate Service Providers Act.

#### PART C

Accountants

Lawyers and notaries

Real Estate Agents

High-value dealers (this includes persons who receives at least SCR 200,000 for payment of goods and services by way of business, e.g., Motor Vehicle Dealers etc...)

Dealers in precious metals

Dealers in precious stones

#### Casinos

Trust and Company Service Providers which provide any of the following services to third parties;

- acting as a formation agent of legal persons;
- acting as a director or secretary of a company; a partner of a partnership or a similar position in relation to other legal persons;
- providing a registered office, business address or accommodation or correspondence or administrative address for a company, a partnership

or any other legal person or legal arrangement;

acting as a trustee of an express trust or performing the equivalent

function for another form of legal arrangement; and

acting as a nominee share holder for another person.

A person who, by way of business invests, administers or manages funds or money on behalf of third parties.

8.1. In accordance with section 34 (2) (g) of the AML/CFT Act, the CO has the function to receive and review reports of suspicious transactions made by the staff of the RE and if sufficient basis exists, report same to the FIU. Accordingly, the CO of a RE shall be the reporter for Suspicious Transaction Reporting for the purpose of section 48 of the AML/CFT Act. The ACO appointed in line with section 34 (3) of the AML/CFT Act, shall assume the role of reporter for suspicious transactions/activities in the absence of the CO.

#### 9. How to Identify a Suspicious Transaction or Activity

REs must develop their own understanding of reasonable suspicion which may be related to risk indicators and incorporate established views of doubt about circumstances relating to the behaviour, to a transaction, to a series of transactions, an attempted transaction or to any combination thereof. A number of indicators, as listed in the next section, can assist in identifying or recognising a suspicious transaction or activity. However, indicators alone do not confirm a ML/TF offence or criminal conduct. An assessment of the suspicion should be based on a reasonable evaluation of other relevant factors, including the knowledge of the customer's business, financial history, background and behaviour. A RE should know its customers and understand their line of business. Transactions or activities that are not within the normal practices of their customer's line of business could then be identified and used to determine whether there are reasonable grounds to suspect that the transactions or activities are related to ML, TF or PF.

All circumstances surrounding a transaction(s) should be reviewed. A transaction can be suspicious regardless of its amount.

#### 9.1. Indicators of Suspicious Transactions or Activity

Below are some of the general indicators, otherwise known as 'red flags', that may point to a suspicious transaction or activity. It is important to note that these indicators are not intended to cover every possible situation and are not to be viewed in isolation. As such, a single indicator on its own may not be enough to form a suspicion or be indicative of reasonable grounds to suspect the transaction/activity. The indicators have to be assessed in the context in which the transaction occurs and considered along with other factors in order to determine the merit to report. These indicators have been derived from trends and patterns experienced in other jurisdictions but they may assist REs in identifying a suspicious transaction/activity.

The industry specific indicators that may give rise to reasonable grounds for suspicion are listed in annexure 2.0

#### **General indicators**

- Transaction or activity differs from the customer's known or expected activity;
- The purpose or source of funds is ambiguous;
- Customer is nervous or hesitating to provide information being requested;
- Customer is known to be a subject of an investigation;
- Customer provides false information;
- Customer holds a public position and is conducting an unusual transaction;
- Transaction or activity involving a politically Exposed Person (PEP);
- Non-face-to-face customers; or
- Customer is making payment in cash for substantial amounts.

#### 10. How to complete the STR form

An STR should create the picture of the suspicious transaction and/or activity as well as the circumstances that gave rise to and support that suspicion. Refer to annexure 3.0 for the detailed steps in completing the STR form. All relevant fields on the form should be completed accurately. The information provided should be clear and comprehensive and this will result in a high-quality STR. Annexure 4.0 provides an example of a high versus a low-quality STR.

When submitting an STR, REs must ensure that all relevant supporting documents are enclosed with the STR. The supporting documents may include copies of the below but note that this is not an exhaustive list and supporting documents may vary depending on the case:

- bank account statements;
- deposit slips;
- published articles;
- photos;
- account opening forms;
- identification documents;

- source of funds;
- swift messages;
- company formation request;
- business plan;

In order to ensure that the STR is complete, the RE should provide a response for each of the questions below.

Who is conducting the suspicious transaction/activity?

Provide all information that you have on the subject.
Should you hold any further

Should you hold any further information on any known associates or related entities then this should also be provided.

When did the suspicious transaction/ activity take place?

The correct date of occurrence should be clearly stated. If there have been repeated occasions this should be highlighted.

What is it that you consider suspicious about the transaction/activity?

The mode that the transaction was conducted e.g., wire transfer, cash deposit or western Union. The use of other financial instruments such as shell companies or insurance covers.

Where was the suspicious transaction/activity detected?

The location of where the suspicious transaction was detected should be provided, e.g., at which branch or branches. The jurisdictions involved if any should be stated.

Why is the transaction/activity considered as suspicious?

The narrative should show the context of the suspicious activity for FIU's analytical purposes. If there has been a deviation from the customer's normal behaviour mode of operation, this should be clearly highlighted.

#### 11. How to Submit a STR

STRs must be filed with the FIU in line with section 48 (2) (a) of the AML/CFT Act, in writing and may be hand delivered in a sealed envelope and stamped "CONFIDENTIAL" addressed to: The Director Financial Intelligence Unit or sent electronically by emailing the completed form to <a href="mailto:suspicious.reporting@fiu.sc">suspicious.reporting@fiu.sc</a>. The STR forms are available on the FIU website, <a href="mailto:swww.seychellesfiu.sc">www.seychellesfiu.sc</a>

For security purposes, all completed STRs sent electronically must be compressed and encrypted, followed by submission via email, as per the detailed process hereunder:

- a. The completed STR form should be compressed into a zipped file (follow the instruction and the video link on the FIU website (www.seychellesfiu.sc) on "How to Compress & Encrypt Using Peazip" for more information on how to compress and encrypt your STR form).
- b. Password protect the zipped file before emailing to the FIU;
- c. Email <u>only</u> the password-protected zipped file to the same email address, <u>enquiries@fiu.sc</u>;
- d. An acknowledgement from FIU, via return email, will be sent which confirms the receipt of the email with the zipped file;
- e. After you receive the acknowledgement email from the FIU, then in a separate email you are requested to email the password and attach the key file (encryption file) to <a href="mailto:enquiries@fiu.sc">enquiries@fiu.sc</a> This is a one-time exercise. You are advised to save the password securely and apply the same password every time when reporting to the FIU.

The steps from a) to e) are only for the first-time reporting. From subsequent reporting, only steps a), b) and c) will need to be performed.

#### 12. Receipt of STR by the FIU

In line with section 48(1) (b) of the AML/CFT Act, the FIU shall acknowledge receipt of the STR by sending a signed letter to the disclosing party within 24 hours of its receipt.

#### 13. Feedback on STRs

Whilst the FIU has an important role as the national centre for the receipt, analysis and dissemination of information, the private sector is a critical stakeholder in the fight against ML/TF and in the protection of our financial system. Therefore, the usefulness of the FIU's analysis will depend greatly on the quality of STRs submitted. It must be appreciated that certain STRs may lead to investigation and must be kept confidential. As such, it is not always possible for the FIU to provide detailed feedback on all STRs to the REs. However, the FIU provides feedback to the REs in relation to STRs through its awareness sessions, targeted meetings and typologies identified and published.

## 14. Further Requests for Information

During the analysis or investigative process, additional information may be required. As such, pursuant to section 48 (3) of the AML/CFT Act, REs which have filed STRs with the FIU are expected to provide the FIU with any additional information that it holds in relation to the transaction or about the parties to the transaction, if requested to do so by the FIU, or a Law Enforcement Agency, as the case may be.

# 15. Rejection of STRs

The FIU reserves the right to reject STRs which are incomplete or which do not have sufficient relevant information to enable the FIU to make an informed determination. The FIU will provide the reason for rejection in a letter. The rejected STR shall be treated as a non-reported STR. The STR may be resubmitted, once the reason for rejection, informed by the FIU, is addressed. However, re-submission must be done within 24 hours of receiving the rejection

letter.

#### 16. Failure to Submit STR

A CO commits an offence if, they have 'reasonable suspicion' of money laundering activity or criminal property and fail to submit an STR. They will be liable on conviction to imprisonment for a term not exceeding 3 years or a fine not exceeding SCR 400,000, or to both.

#### 17. Tipping Off

Tipping off is the process of letting the customer know that he/she is or might be the subject of a suspicion. Tipping off could occur at the stage of initial contact with the customer, during the processing of transactions or obtaining information when investigations are being conducted on a suspicion or even after reporting to an appropriate agency. REs should refrain at all times, under all circumstances, from advising their clients, or the subject(s) of the STR, about the intention to file or existence of the STR.

In line with section 50 (1) of the AML/CFT Act it is an offence if a person (which may include a reporting entity, its officers, employees or agents) discloses to the subject of the suspicion or any third party that:

- a) An STR or direction from the FIU has been made;
- b) A reporting entity has formed a suspicion in relation to a transaction;
- c) An investigation is being or is to be carried out

All members of staff of a RE needs to be fully aware of their personal obligations under the tipping-off clause. They need to know what to say to a customer and what to do to avoid alerting the customer to the concerns that the RE might actually be harboring. Note that tipping off may jeopardize an ongoing or even a prospective investigation but may also pose a threat to the safety of the CO.

# 18. Protection for Persons Reporting STRs

Reporting entities and the supervisory authorities are provided protection under section 54 (3) of the AML/CFT Act whereby:

"No criminal or disciplinary proceedings shall be taken against-

- (a) A reporting entity or supervisory authority of a reporting entity;
- (b) An employee or agent of a reporting entity or an officer of a supervisory authority of a reporting entity acting in the course of that person's employment or agency,

In relation to any action by the reporting entity or the supervisory authority or their officer, employee or agent, taken in good faith under the provisions of this Act, or in compliance with the directions given by the FIU under the provisions of this Act."

## 19. Record Keeping

A reporting entity is required to maintain records of all STRs made, either in a physical or digital form, for a minimum period of 7 years from the date of the transaction. Moreover, the following entities:

- a) Banks;
- b) Bureau de Change;
- c) Insurance Companies; and
- d) Securities Exchange infrastructures.

are required to maintain in digital form, records of all STRs made, for a period of 30 years from the date on which the business relationship ceases.

#### Annexure 1.0: Indicators of suspicious transaction/activity

#### Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction

Account activity of a non-profit organisation which is inconsistent with its established purpose.

Transactions involving individuals who are listed on sanction lists or known in the media for having terrorist affiliations.

Transactions involving jurisdictions which are known to be locations where terrorist groups operate.

Customer seems to be using their account from high-risk jurisdictions.

Fund raising or donations which are not official and which do not have a clear purpose.

Individual or entity's online presence supports violent extremism or radicalisation.

Customer trades in commodities that may also be dually used in missiles, and chemical, biological and nuclear weapons.

The sudden conversion of financial assets to a virtual currency exchange.

Particulars of the customer or beneficiary of a transaction are similar to those listed under sanctions lists, for example the address, register of directors and shareholder.

#### Annexure 2.0 Industry specific indicators

#### BDC

Transaction to and from high-risk jurisdictions.

Customer sending large transaction to countries known as narcotic source countries.

Transactions involving amounts which are just below the reporting threshold.

Customer frequently sending money to countries known for scams.

Use of third parties at money service businesses to send and receive funds.

The use of different branch locations to conduct transactions for no apparent reason.

Multiple customers sending funds to the same beneficiary.

Customer exchanges small denomination of bills for larger denominations.

Customer has very little information or is reluctant to provide details of the beneficiary.

Customer frequently sending money to a foreign country with no plausible reason.

#### Banks

Transactions being conducted shows a significant mismatch with the customer's declared earnings

Fake documents & false information submitted by the customer.

Customer's or depositor's reluctant to provide requested information.

Account activity inconsistent with the customer profile.

Multiple deposits made to the customer's account by third party depositors.

Multiple transactions to the same account or beneficiary.

Cash deposited domestically, with the funds subsequently withdrawn from ATMs offshore.

Customer or beneficiary has link with terrorist activities or terrorist financing or sanctioned organisation.

Customer prefers to use the night safe to make deposits to avoid any declarations.

Taking a loan and repaying same in cash within a short period of time.

Adverse media report against the customer or beneficiary.

Transaction or activities related to Trade-Based Money Laundering/ Terrorist Financing.

Funds are moved to another account immediately after being credited.

Account shows large deposits or withdrawals but no other normal business-related activities such as payrolls, rentals or invoices.

There is a sudden change in transaction pattern.

The movement of money between accounts owned by the customers for no apparent reason.

Sudden increase in transactions on a dormant account.

Frequent cash deposits to loan accounts which are not in line with the agreed repayment schedule.

#### Insurance

Customer cancels insurance contracts with no concerns over losses in fees and charges.

Customer requests for insurance products with no intended purpose and is reluctant to provide the purpose of the investment.

Customer requesting for payout of an insurance product before maturity.

Customer cancels his insurance contract and send funds to a third party.

Customer changing beneficiary shortly after purchasing an insurance product.

Customer paying in cash for large transactions.

Customer making an overpayment in cash for a policy premium and requesting for refund.

#### Casinos

Customer purchases casino chips with cash and requests a cheque payment for unused chips.

Customer stores value on the casino cards and later claims back the money as winnings

Customer always requests for winnings payment to be made in a third party's name.

Customer spending is not in line with their financial status.

Using third parties to either purchase chips or gamble

Exchanging low denominations notes for large denomination notes.

#### Real Estate

Multiple purchases of real estate but does not reflect the income of the customer.

Purchase of multiple properties but with no real interest in the location or condition.

Purchase of real estate in the name of another person who has no clear or justifiable connection to the purchaser.

#### Lawyers

Appointing a lawyer in financial or commercial transactions and requesting the concealment of the customer's name (beneficial owner) in any of these transactions.

#### Accountants

Customer has income which is inconsistent with sales

Customer expenditure is inconsistent with income

Multiple loans being disbursed to shareholders which is inconsistent with the business activity

Company accounts showing a loss but the business keeps operating without plausible reason for the loss

Company is acquiring high value assets which is inconsistent with the business activity

#### High Value Dealers

Customer purchasing high value items without any concerns of the price.

Customer attempting to return high value purchase immediately after purchase with no satisfactory explanation and requesting to be refunded by cheque.

Customer selling high value items shortly after purchase for a lower price than that of the purchased price.

Customer is known to have a criminal background.

Purchase of a high value item with cash

# Company Service Providers

Customer is requesting to remain anonymous and shows interest in using nominees with no justification.

Customer request for the setup of complex legal arrangements with no reasonable explanation.

Customer provides false documents.

The customer is adversely known.

The customer is a PEP.

The business will be operating in a high-risk jurisdiction.

Customer has requested for incorporation of multiple companies in a short period of time.

# Annexure 3.0 Steps on how to complete the STR form

ar	t 1 Disclosing Pa	arty		
		-		
1.	Name of Institution	Name of RE submitting the STR		
2.	Address	Complete address of RE submitting the STR		
3.	Telephone Number	+ 248 277777		
4.	Report Related to:	Money Laundering		
		Terrorist Financing Tick relevant box		
		Other Criminal Activities		
2- Information on Person/Entity Engaging in Suspicious Activity or				
		erson/Entity Engaging in Suspicious Activity or		
	nformation on Pe tions	erson/Entity Engaging in Suspicious Activity or		
ac	tions	erson/Entity Engaging in Suspicious Activity or Person/Entity Engaging in Suspicious Activity or		
ac	tions			
ac	tions			
ас	tions	Person/Entity Engaging in Suspicious Activity or		
ac	tions	Person/Entity Engaging in Suspicious Activity or		
Par	tions t 2 Information on Transactions	Person/Entity Engaging in Suspicious Activity or  Tick the relevant box  Individual Company Trust  State the account name of the person/entity engaging		
Par	tions t 2 Information on Transactions  Account Type  Account Name(s)	Tick the relevant box  Individual Company Trust  State the account name of the person/entity engaging in the suspicious transaction		
Par	tions t 2 Information on Transactions  Account Type	Person/Entity Engaging in Suspicious Activity or  Tick the relevant box  Individual Company Trust  State the account name of the person/entity engaging		
Par 1. 2. 3.	Account Name(s)  Account Number	Tick the relevant box  Individual Company Trust  State the account name of the person/entity engaging in the suspicious transaction  State account number of the person/entity engaging in the suspicious transaction		
Par	tions t 2 Information on Transactions  Account Type  Account Name(s)	Tick the relevant box  Individual Company Trust  State the account name of the person/entity engaging in the suspicious transaction  State account number of the person/entity engaging		
Par	Account Name(s)  Account Number	Tick the relevant box  Individual Company Trust  State the account name of the person/entity engaging in the suspicious transaction  State account number of the person/entity engaging in the suspicious transaction  DD/MM/YYYY Date that the account was opened with		

Identification on the Accou	Details of Account Holder(s) and Other Persons Authorized
<ol> <li>Name</li> <li>Date of B</li> <li>ID Number</li> <li>Passport</li> <li>Nationalit</li> </ol>	account holder and any other authorized signatories on the account
	conducting the transaction in the case that it
1. Place of Incorpor 2. Date of Incorpor 3. Business Activity	Person

1 (j) A	Name .		
A (ii) A	Date of Birth	DD/MM/YYYY/	
A (iii)	ID Number .		
A (iv)	Passport Number .		
1 (v) A	Nationality .		Provide the
A (vi)	Occupation .		complete  details of the
B (į) 1	Name .		director(s) of
B (ii)	Date of Birth	DD/MM/YYYY	the entity
B (iii)	ID Number .		
B (iv)	Passport Number .		
B (v) B	Nationality .		
B (vi)	Occupation .		
A (ii)	Date of Birth	DD/MM/YYYY –	
Identi	fication Details of	Beneficial Owners	
A (i)	Name Date of Birth	DD/MM/YYYY	
	Dute of Birth		
A (iii)	ID Number		
A (iii) A (iv)	ID Number  Passport Number		
A (iii) A (iv)			
A (iv)	Passport Number		Provide the
A (iv)	Passport Number	ent DD/MM/YYYY/	complete
A (iv)  A (v)  A (vi)  A (vii)	Passport Number  Nationality  Occupation  Date of Appointment		complete details of th beneficial
A (iv)  A (v)  A (vi)	Passport Number  Nationality  Occupation  Date of Appointment		complete details of th beneficial owner(s) of
A (iv)  A (v)  A (vi)  A (vii)	Passport Number  Nationality  Occupation  Date of Appointment		complete details of th beneficial
A (v) A (vi) A (vii) A (viii)	Passport Number  Nationality  Occupation  Date of Appointment  Date of Resignation  (if relevant)	on DD/MM/YYYY//	complete details of th beneficial owner(s) of
A (iv)  A (v)  A (vi)  A (vii)  A (viii)  B (i)	Passport Number  Nationality  Occupation  Date of Appointment  Date of Resignation (if relevant)  Name	on DD/MM/YYYY /	complete details of th beneficial owner(s) of
A (iv)  A (v)  A (vii)  A (viii)  B (i)  B (ii)	Passport Number  Nationality Occupation Date of Appointme  Date of Resignatio (if relevant) Name Date of Birth	DD/MM/YYYY	complete details of th beneficial owner(s) of
A (iv)  A (v)  A (vii)  A (viii)  B (i)  B (iii)	Passport Number  Nationality Occupation Date of Appointme  Date of Resignatio (if relevant) Name Date of Birth ID Number	DD/MM/YYYY	complete details of th beneficial owner(s) of
A (iv)  A (v)  A (vii)  A (viii)  B (i)  B (ii)  B (iii)	Passport Number  Nationality Occupation Date of Appointme Date of Resignatio (if relevant) Name Date of Birth ID Number Passport Number	DD/MM/YYYY	complete details of th beneficial owner(s) of
A (iv)  A (v)  A (vii)  A (viii)  B (i)  B (ii)  B (iii)  B (iv)  B (v)	Passport Number  Nationality Occupation Date of Appointme Date of Resignatio (if relevant) Name Date of Birth ID Number Passport Number Nationality	DD/MM/YYYY	complete details of th beneficial owner(s) of

1. Date of Transaction DD/MM/YYYY	./	
2. Date of Detection         DD/MM/YYYY	./	
3. Amount Involved		ia.
4. Currency	Tick as appropria	
5. Type of Transaction Cash Swift Transfer Cheque	Tick as appropria	
Swift Transfer	Tick as appropria	
Cheque	Tick as appropria	
		riate
Card		
transaction. The date of occurrence and if the transaction previously, the period of time should be stated.	action had occurred	
previously, the period of time should be stated.  If the Transaction is a Transfer, Details of the Beneficiary  1. Name of		Provid details
If the Transaction is a Transfer, Details of the Beneficiary  1. Name of Beneficiary		details the
If the Transaction is a Transfer, Details of the Beneficiary  1. Name of Beneficiary		details the benefi in the
If the Transaction is a Transfer, Details of the Beneficiary  1. Name of Beneficiary  2. Address		details the benefi in the that th
If the Transaction is a Transfer, Details of the Beneficiary  1. Name of Beneficiary  2. Address		details the benefi in the

#### Annexure 4.0 High Quality versus low quality STR

Below is an example of a low-quality STR.

1.	Date of Transaction	DD/MM/YYYY	10/06/2021
2.	Date of Detection	DD/MM/YYYY	15/06/2021
3.	Amount Involved	130,000	
4.	Currency	Scr	
5.	Type of Transaction	Cash	X
		Swift Transfer	
		Cheque	
		Card	
6. Fu	II Details and Descripti	on of Transactior	

The description does not provide sufficient details as to who made the deposits, whether all deposits were made by the account holder or other individuals; what was suspicious about the deposits; when were the deposits made, all on the same day or in parts on different days; Where were the deposits made, at which branch?

1. Name of Beneficiary
2. Address
3. Account Number
4. Beneficiary Bank
5. IBAN Number

7. Reasons why the transaction was reported as suspicious:

Not in line with customer profile

The narrative as to why the transaction was considered to be suspicious is not comprehensive.

Only an indicator has been mentioned but what has been the findings of the RE that supports the decision that the transaction merits reporting?

F	ar	t 3	Information a	about Suspicio	us Activity or Transaction
1		Date	of Transaction	DD/MM/YYYY	9 <sup>th</sup> ,1/1 <sup>th</sup> ,1/4 <sup>th</sup> ,15 <sup>th</sup> June 2021
2	2.	Date	of Detection	DD/MM/YYYY	15/06/2021
3	3.	Amou	unt Involved	40,000,	20,000, 30,000, 40,000
4	ŀ.	Curre	ency	Scr	
5	5.	Туре	of Transaction	Cash	X
				Swift Transfer	
				Cheque	
				Card	

Mr. X personally deposited to his savings account the following amounts in cash: SCR40,000 on 9<sup>th</sup> June, SCR20,000 on 11<sup>th</sup> June, SCR30,000 on 14<sup>th</sup> June and SCR40,000 on 15<sup>th</sup> June 2021. The transaction took place at the Victoria branch. The deposited amounts were made mostly in small notes denominations of SCR50 and SCR25 Refer to attached deposit slips. The customer was hesitant to provide the source of the deposit when requested by the cashier but then claimed to be instalment payments from the sale of his car. No supporting documents were provided by the customer.

Mr. X is employed as a custom's officer and earns a salary of SCR 12,000. According to the customer profile, which was last updated in December 2020, Mr. X anticipated only his monthly salary as the source of funds to the account. The customer conducts most of his transaction online or through POS. The account balance is maintained at a monthly average of SCR 3000. Mr. X has never taken a loan with the bank and since account opening the account has never attained a balance of more than SCR 50,000. The bank has contacted Mr. X to provide a supporting document for the sale but to date he has not responded.

Complete details of the suspicious transaction