ශ්‍රී ලංකා මහ බැංකුව
இலங்கை மத்திய வங்கி
CENTRAL BANK OF SRI LANKA

මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதற் பிரிவு
FINANCIAL INTELLIGENCE UNIT

අංක 30, ජනාධිපති මාවත, කොළඹ 01, ශ්‍රී ලංකාව
இல. 30, சனாதிபதி மாவத்தை, கொழும்பு - 01, இலங்கை
No. 30, Janadhipathi Mawatha, Colombo 01, Sri Lanka

**Guidelines-01/2019**

**Ref: 037/08/001/0032/019**

August 22, 2019

To: Chief Executive Officer/ General Manager/ Proprietor

Dear Sir/Madam,

**Guidelines for Designated Non-Finance Businesses on Suspicious Transactions Reporting, No. 01 of 2019**

The above mentioned guidelines will come into force with immediate effect and shall be read together with the Financial Transactions Reporting Act, No. 6 of 2006, Designated Non-Finance Business (Customer Due Diligence) Rules No. 1 of 2018 and the Suspicious Transactions (Format) Regulations of 2017.

Yours faithfully,

**E H Mohotty**
**Actg. Director/ Financial Intelligence**

**Cc:** Compliance Officers

☎ 011-2477125
011-2477509
011-2477692
011-2477708
flu@cbsl.lk
dflu@cbsl.lk
www.flusrilanka.gov.lk

# Guidelines for Designated Non-Finance Businesses on Suspicious Transactions Reporting, No. 01 of 2019

## Introduction

1. These Guidelines are issued pursuant to Section 15 (1) (j) of the Financial Transactions Reporting Act, No. 6 of 2006 (FTRA), and be applicable to Designated Non-Finance Businesses (herein after referred to as DNFBs) engaged in or carrying out "designated non-finance business" as defined in Section 33 of the FTRA.

2. These Guidelines provide an aid to interpret and apply Suspicious Transactions (Format) Regulations of 2017 issued under Gazette Extraordinary No. 2015/56 on April 21, 2017 to Institutions that engaged in or carrying out "designated non-finance business" as defined in Section 33 of the FTRA.

3. These Guidelines are not intended to be exhaustive and cannot be interpreted as legal advice from the Financial Intelligence Unit (FIU).

## Legal Obligation

4. As per Section 7 of the FTRA all "Institutions", should report suspicious transactions to the FIU. "Institution" is defined as any person or body of persons engaged in or carrying out any finance business or designated non-finance business. The following businesses and professions are included in the definition of "designated non-finance business" under Section 33 of the FTRA among others.
    a) casinos, gambling houses or conducting of a lottery, including a person who carries on such a business through the internet when their customers engage in financial transactions equal to or above the prescribed threshold.
    b) real estate agents, when they are involved in transactions for their clients in relation to the buying and selling of real estate.
    c) dealers in precious metals and dealers in precious and semi-precious stones, including but not limited to, metals and stones covered by the National Gem and Jewellery Authority Act, No. 50 of 1993 when they engage in cash transactions with a customer, equal to or above the prescribed threshold.

d) lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for their clients in relation to any of the following activities :-

(i) buying and selling of real estate;

(ii) managing of client money, securities or other assets;

(iii) management of bank, savings or securities accounts;

(iv) organization of contributions for the creation, operation or management of companies; and

(v) creation, operation or management of legal person or arrangements and the buying and selling of business entities.

e) a trust or company service provider not otherwise covered by this definition, which as a business provides and one or more of the following services to third parties :-

(i) formation or management of legal persons;

(ii) acting as or arranging for another person to act as, a director or secretary of a company, a partner or a partnership or a similar position in relation to other legal persons;

(iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or for any other legal person or arrangement;

(iv) acting as or arranging for another person to act as, a trustee of an express trust;

(v) acting as or arranging for another person to act as, a nominee shareholder for another person.

5. Section 7 (1) of the FTRA requires:

"Where an Institution -

a) has reasonable grounds to suspect that any transaction or attempted transaction may be related to the commission of any unlawful activity or any other criminal offence;

or

b) has information that it suspects may be relevant-

i. to an act preparatory to an offence under the provisions of the Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005;

ii. to an investigation or prosecution of a person or persons for an act constituting an unlawful activity, or may otherwise be of assistance in the enforcement of the Money Laundering Act, No. 5 of 2006 and the Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005,

the Institution shall, as soon as practicable, after forming that suspicion or receiving the information, but no later than two working days therefrom, report the transaction or attempted transaction or the information to the FIU".

Such reports are herein referred to as Suspicious Transaction Reports (STRs).

6. As specified above, all DNFBs are required to report STRs to the FIU.

7. DNFBs are required to establish and maintain procedures and systems to implement the reporting requirement under Section 7 of the FTRA. Further, the FTRA requires DNFBs to train its officers, employees and agents to recognize suspicious transactions.

8. As per the Rule 6 (f) and 6 (g) (iii) of the Designated Non-Finance Business (Customer Due Diligence) Rules, No. 1 of 2018 (CDD Rules), DNFBs are required to formulate an internal AML/CFT Policy approved by its Senior Management or Board of Directors and that policy must include procedures and controls on reporting suspicious transactions to the FIU.

9. Under the FTRA every DNFB is required to maintain the records of transactions and of correspondence relating to transactions and records of all reports furnished to the FIU for a period of six years from the date of the transaction, correspondence or the furnishing of the report, as the case may be. 'All reports furnished to the FIU' shall also include the records of STRs.

## Importance of Reporting Suspicious Transactions

10. Reporting of suspicious transactions is an important mode of detection of money laundering, terrorist financing and related transactions of proceeds of crime.

11. Reporting of suspicious transactions is a major function of an effective AML/CFT programme of an Institution.

12. For the AML/CFT function to be meaningful, it must result an effective implementation of the FTRA, and other Rules and Regulations issued thereunder. Ineffective implementation can result in DNFBs either submitting STRs that are inaccurate, incomplete or inappropriate or DNFBs failing to report suspicious transactions entirely. Such failures expose the DNFBs to regulatory, reputational, operational, and legal risks. In some cases, such failures may also expose both natural and legal persons to criminal liability.

13. Whatever the source of customer information and knowledge of transactions, there must be an institutional will to make the system work. That is, there must be the will of the DNFB to detect suspicious transactions, to recognize in good faith such suspicious transactions, and fully and accurately report such transactions when recognized. Such institutional will and implementation is most effective when there is a clear commitment from those at the Senior Management level including the Board of Directors/Owners of the DNFBs and propagated through concrete actions and demonstrations to the rest of the staff of the DNFBs (e.g. development of effective internal policies, processes and training programmes, audits of AML/CFT functions).

14. The key to being able to identify unusual and possibly suspicious transactions is the DNFB's knowledge of their customer and the customer's business and related transactions.

## Suspicion

15. DNFBs must develop their own operating definition for suspicion. It may incorporate persistent feelings of doubt about circumstances relating to a behavior, to a single transaction, to a series of transactions, an attempted transaction or to any combination thereof. It can be a feeling that something is not as it was expected to be, or as it was

explained to be, given the totality of knowledge of the circumstances in which that something exists. The feeling of doubt cannot be relieved by proof, since proof will rarely be available. The definition should allow formation of a belief that is not necessarily firmly grounded or perfectly clear. At the same time, the definition should not allow these beliefs to be fanciful or brief. Certainly, the definition should count as suspicious behaviors and activities that are unusual for the circumstances and not adequately or credibly explained.

The operating definition for suspicion must pass a test of reasonableness. If the definition is too narrow or rigid, it may exclude transactions which are unanticipated unlawful circumstances and may also result in avoidance behavior by criminals. On the other hand, a definition that is too broad or flexible might result in large number of STRs that do not reflect possible unlawful circumstances. Suspicious indicators and typologies may be the main element of identifying such suspicious transactions and "unusual" patterns of behavior and transactions should also be considered in identifying such suspicions.

A non-exhaustive and unofficial list of suspicious indicators for transactions and behaviours is provided in Appendix I. The DNFBs should identify and prepare their own indicators based on nature and size of its business. When using indicators, the DNFBs need to consider that these indicators are not formulae and do not necessarily indicate criminal activity. The DNFB's identification of suspicious transactions should not be limited to the circumstances set out in the indicators but should ultimately be based on the knowledge of the customer and the customer's business and related transactions.

16. After gaining a thorough understanding of the FTRA and other Rules, Regulations, Circulars and Guidelines issued thereunder and after consideration of facts and circumstances available to the DNFBs and if such facts are identified in good faith and within the context of the DNFB's understanding of suspicion and risks for the DNFB, transactions that are deemed "suspicious" must be reported to the FIU regardless of the amount of the transaction.

17. DNFBs are not expected to establish the unlawful activity before submitting the STR to the FIU rather they may report the unusual circumstances surrounding a transaction or transactions or set of behaviours that lead to a suspicion.

## Reporting of STRs

18. The STR duly completed and signed by the Compliance Officer must be submitted to the FIU using Schedule V of the Suspicious Transactions (Format) Regulations of 2017 (Appendix II).

19. The DNFB must submit STRs in writing through the prescribed format and these may be delivered by way of mail, fax or electronic mail or such other manner as may be determined by the FIU.

20. The suspicion may be informed through telephone; however it must be followed up in writing within twenty-four hours through the prescribed format.

## Timing of Reporting

21. The Section 7 (1) of the FTRA requires STRs to be submitted to the FIU as soon as practicably possible but no later than two working days after formation of a suspicion. This means that, regardless of the respective DNFBs' processes, procedures and steps after the initial formation of suspicion, the suspicion itself must be reported even if the DNFB's process has not been completed. The process of the DNFB for dealing with suspicion may proceed concurrently with the filing of an STR. It is to be noted that the suspicion can be formed at any time for the business relationship with customer and at any stage of the business relationship - for example – as suspicion can be formed when establishing the business relationship, when verifying the identity, when the DNFB is monitoring the accounts and transactions of the customers.

    For example, a customer approaches a real estate agent to purchase an apartment. He continually emphasized that he does not want his name to be appeared in any document relating to the property and instead requested to include a non-related third party's name in all the documents. This formed an immediate suspicion about the customer and as soon as practicable but within two working days from the transaction this

suspicion should be reported to the FIU while the DNFB may continue with its internal processes to verify the authenticity and details of the payment.

22. If, after sending the STR, the DNFB discovers additional facts and circumstances to either support or refute the initial suspicion after sending the STR, then the DNFB should provide such additional information to the FIU appropriately.

## Content of Reporting

23. **Completeness:** A single STR must stand alone and contain complete information about the suspicion. An STR should provide a full picture of the suspicion itself as well as the circumstances that gave rise to and support that suspicion. Where multiple transactions and/or behaviours are connected with a suspicion, a single STR should be filed capturing all of these.

24. **Form Narrative:** The narrative portion of the STR is most important. When submitting the STR, the DNFB may provide full detailed narrative in the Schedule V of the Suspicious Transactions (Format) Regulations of 2017. The narrative should attempt to answer to the extent possible the basic descriptive questions of **what, who, when, where, why and how.**

    The DNFB should provide clear quantitative and qualitative data as much as possible such as;

    - Amount of money involved
    - Place where the respective transaction was made
    - The date of the transaction(s)

    Some of the questions that the narrative should attempt to answer, if possible, include: Common attributes to be questioned;

    - What is the nature of the suspicion?
    - Any likely offenses that may have been committed?
    - What transactions, attempted transactions, behaviours, facts, beliefs and circumstances are involved and relevant to the suspicion?
    - Who are the natural and legal persons involved?
    - Who are the beneficial owners (if relevant)?

- What identifying information such as names, ID numbers, registration numbers, etc. is available?
- What are the addresses/locations involved?
- What are their occupations or types of business?
- Who are their employers?
- What political exposure do they have, if any?
- How are they connected with each other and with the transactions?
- What were their roles in the transactions?
- When and where did the transactions or attempted transactions or behaviours occur?
- How does the timing or location of the transactions contribute to the suspicion?
- Why do these facts and circumstances support the suspicion?
- How was the suspicion formed?
- Actions taken by the DNFB, if any?
- Are there any related STRs already submitted by the DNFB?

The narrative should be structured in a logical manner so that information can be conveyed to the FIU as efficiently, completely and accurately as possible. Essay formats could be used for an STR narratives i.e. having an introduction, a body, and a conclusion. Paragraph breaks can be used to divide the narrative into logical units and enhance readability.

25. **Accuracy:** It is imperative that factual information provided in the STR is accurate. This is particularly true for identifiers such as names, ID numbers, registration numbers, etc. All spellings and transcriptions of identifiers should be double checked. A single inaccurate digit in a passport number or a NIC, or a misplaced or transposed character in a name, can make the difference between a successful or an unsuccessful analysis by the FIU. Identifiers for legal entities (e.g. company / business registration number, registered name of company) should be exactly identical in every respect to those found on any official registration documents.

## Submission of Supporting Documents

26. DNFBs are required to submit relevant supporting documents along with the STR.

27. Supporting documents should support rather than replace the STR contents, including the narrative. It is not acceptable to only refer to a supporting document in the narrative when information from the supporting document can be directly included in the narrative. For example, if the suspicion involves a purchase of a real estate, all the details relating to purchase that are related to the suspicion should be included in the narrative.

28. An indicative but non-exhaustive list of supporting documents along with corresponding scenarios are given below for reference.

| **Scenario** | **Indicative List of Supporting Documents** |
|---|---|
| Suspicion regarding forged / altered identity (NIC/ Passport / Driving License) | • Copy of the documents |
| Discrepancy between the source of funds of the owner and the property in a property deal | • Sales and purchase agreement<br>• Receipts relating to the property transaction |
| Occupation details does not match with the transaction value of a gem | • Receipts involved with the gem sale |
| Customers regular purchases of casino value instruments and frequent wagers in cash just below the identification threshold | • Receipts involved with the casino transaction |
| Customer of a lawyer transfers a deed to a third party without physically meeting the customer and without a power of attorney | • Transfer deed<br>• Payment receipts |
| Customer of accountants have overpaid their invoices | • Statement of accounts<br>• Overpaid invoices |

## Miscellaneous

### Confidentiality

29. As per the Section 9 of the FTRA, DNFBs are prohibited from informing any person, including the customer, about the contents of an STR and even that the DNFB has filed or is contemplating filing such a STR to the FIU.

30. As per CDD Rules, where a DNFB forms a suspicion of money laundering or terrorist financing risk relating to a customer and reasonably believes that conducting the process of CDD measures would tip off the customer, then the DNFB can proceed without conducting the CDD measures. However, the DNFB is required to immediately file a STR in compliance with Section 7 of the FTRA.

### Breach of Confidentiality

31. If any customer is tipped off about the reporting of STRs by any officer of the DNFB it would be considered as a violation under the Section 9 and 10 of the FTRA. This is described as the offence of 'tipping off' and is an offense punishable with a fine not exceeding five hundred thousand rupees or imprisonment for a term not exceeding two years, or both.

### Protection for Persons Reporting STRs

32. As per Section 12 of the FTRA:

"No civil, criminal or disciplinary proceedings shall lie against —

(a) an Institution, an auditor or supervisory authority of an Institution; or

(b) a director, partner, an officer, employee or agent acting in the course of that person's employment or agency of an Institution, firm of auditors or of a supervisory authority,

in relation to any action by the Institution, the firm of auditors or the supervisory authority or a director, partner, officer, employee or agent of such Institution, firm or authority, carried out in terms of the FTRA in good faith or in compliance with regulations made under this Act or rules or directions given by the Financial Intelligence Unit in terms of the FTRA".

33. Pursuant to Section 7 and 10 of the FTRA, all information in an STR, or additional information provided in support of the STR, including the identity of any officer or employee of a DNFB, will be treated in the strictest confidence by the FIU.

## Failure to Report STRs

34. If a DNFB fails to submit STRs when reasonable grounds exist to suspect that a transaction is related to money laundering or terrorist financing, it is considered as non-compliance with the FTRA. As per Section 19 of the FTRA, who fails to conform with Section 7 of the FTRA, shall be liable to a penalty as may be prescribed taking into consideration the nature and gravity of relevant non-compliance: provided however such penalty shall not exceed a sum of rupees one million in any given case. Where a person who has been subjected to a penalty on a previous occasion, subsequently fails to conform to a requirement on any further occasion such person shall be liable to the payment of an additional penalty in a sum consisting of double the amount imposed as a penalty on the first occasion and for each non- compliance after such first occasion.

35. Further, in terms of Section 28 of the FTRA, a person who is making an STR under Section 7 makes any statement that the person knows is false or misleading in a material particular or omits from any statement any matter or thing without which the person knows that the statement is false or misleading in a material particular is guilty of an offence punishable on conviction to a fine not exceeding one hundred thousand rupees or imprisonment of either description for a term not exceeding one year, or to both such fine and imprisonment.

## Should a reporting entity continue a business relationship with a customer about whom an STR has been reported?

36. The FTRA does not prohibit DNFBs from continuing business relationships with customers about whom STRs has been submitted or suspicion has been formed. Especially the behaviour of the DNFB towards the customer should not amount to any tipping off subject to the provisions of the Section 3 of the FTRA.

## Obligations of DNFBs which have submitted an STR in relation to a customer and is continuing the business relationship

37. After the submission of an initial STR, the DNFB should continue to comply with all relevant provisions of the FTRA in all future dealings with that customer, which may include a requirement to submit additional STRs /information on further suspicions identified / further developments.

## Further Information Requests

38. Pursuant to Section 7 (3) of the FTRA, where the FIU has requested further information regarding any STR, the DNFBs should take all necessary measures to provide such information promptly to the FIU.

39. In addition, as specified in Section 15 (1) (b) of the FTRA, the DNFBs must submit any information that the FIU requests relevant to an act constituting an unlawful activity, or an offence of money laundering or financing of terrorism, or a terrorist activity whether or not publicly available, including commercially available databases, or information that is collected or maintained, including information that is stored, in databases maintained by the Government.

## Appendix I—Suspicious Indicators

This appendix contains a list of indicators related to customer behaviours and activities. This list is necessarily non-exhaustive and incomplete and should be modified and supplemented as necessary by each DNFB. Indicators are not formulae and they do not always indicate the presence of criminality. Conversely, the lack of indicators does not mean the absence of criminality. **However, the presence of an indicator, and especially the presence of multiple indicators, should cause increased scrutiny by the DNFB and such scrutiny may lead to the formation of suspicion.**

## General Indicators

- Any behaviour unusual for the circumstances.
- Any activity unusual for the customer.
- Any activity unusual in itself.
- Any knowledge that leads the DNFB to believe that unlawful activity may be involved.
- Any unresolved and persistent feelings of doubt related to customers and their transactions or attempted transactions.

## General Behavioural /Customer Indicators

- Customer talks about or hints about involvement in criminal activities, even if in a humorous way.
- Customer does not want any correspondence sent to home address.
- Customer repeatedly uses an address but frequently changes the names involved.
- Customer uses addresses in close proximity of each other.
- Customer is accompanied and watched when visiting the premises.
- Customer shows unusual curiosity about internal systems, controls and policies.
- Customer presents confusing or inconsistent details about the transaction.
- Customer over justifies or explains the transaction.
- Customer tries to convince the staff to alter or omit reporting data.
- Customer is secretive and reluctant to meet in person.
- Customer seems nervous when doing the transaction.
- Customer insists to do the transaction quickly.

- Customer attempts to develop a close rapport with the staff.
- Customer offers money, huge commissions, or unusual favours for the transactions or provision of services.
- Customer has unusual knowledge of the law in relation to suspicious transaction reporting.
- Customer jokes about needing or not needing to launder funds.

## Identity Indicators

- Customer provides doubtful or vague information.
- Customer produces false identification or identification that appears to be counterfeited, altered or inaccurate.
- Customer refuses to produce personal identification documents.
- Customer doesn't have the original identification documents and only possesses copies of such documents.
- Customer's supporting documentation lacks important details.
- Customer unnecessarily delays presenting identity documents or any other document relating to CDD.
- A foreign customer produces identification documents which do not reflect his/her nationality and are difficult to be verified.
- Customer presents identification documents appearing as new or have recent 'issued dates'.
- Customer is unemployed, or switches jobs frequently.
- Customer displays large amount of cash to do the transaction.

## Indicators for a Business

- Business is having irregular business hours.
- Business is an unusually profitable business.
- Business is a profitable business in a failing industry.
- Business receipts and income seems far above the industry norms.
- Use of high cost or inconvenient methods when lower cost or more convenient methods are available.
- Apparent lack of in-depth knowledge of his own business or industry.

## General Transaction Indicators

- Transaction is unusual for the customer.
- Transaction is unusual for the country.
- Transaction is unusual for the industry.
- Transaction is unusual for any other reason.
- Transaction seems to be inconsistent with the customer's apparent financial standing or usual pattern of activities.
- Sudden unexplained increase in wealth.
- Transaction appears to be out of the ordinary course for industry practice or does not appear to be economically advantageous for the customer.
- Transaction is unnecessarily complex for its stated purpose.
- Activity is inconsistent with what would be expected from declared business.
- Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

## Red Flag Indicators for Specific Sectors

### Casinos and Gambling Houses

- Customers purchasing and redeeming chips or depositing and withdrawing funds with no gambling or minimal gambling.
- Customers requesting multiple payments of winnings and capital to the account of a third party.
- Multiple players requesting for payments to the same beneficiary.
- Gamblers who appear to be cooperating by placing offsetting bets against each other.
- Structuring the purchase or redemption of chips or other instruments to avoid trigging CDD requirements or other reporting requirements (whether real or perceived).
- "Bill stuffing" by feeding currency to gambling devices that accept cash and then cashing out (e.g. by receiving a TITO ticket or other such instrument) with minimal or no actual gambling.
- Customers befriending/attempting to befriend casino employees.
- A casino player seems to be funded by a third party.

- Dramatic or rapid increase in size and frequency of transactions seen from a established customer.
- Gambling activity that is inconsistent with the financial situation and/or known occupation of the person gambling.
- Purchase of winning tickets from gamblers.
- Purchasing of winning jackpots or winning lottery tickets at a premium.
- Exchanging large amount of small denomination bank notes for larger denominations without gambling.
- Frequent claims for winning jackpots.
- Customers watching/hanging around jackpots sites but not participate in gambling.
- Customers passing significant values in chips or TITO tickets to other customers.
- Loaning funds for gambling to customers by a third party with repayment of the funds being a discounted amount.
- Gambling patterns that appear designed to wager large sums at low risk over a period time, thus achieving a predictable low rate of loss prior to cashing out.
- Customers reluctant to provide information to complete CDD requirements or provide doubtful or unverifiable identification information.

## Real Estate Agents

- Customer purchases property in the name of a nominee such as an subordinate or a relative (other than a spouse), or in the name of minors or incapacitated persons or other persons (other than their own children) who do not have the economic capacity to carry out such purchases.
- Customer tries to hide the identity of the beneficial owner or requests that the transaction be structured to hide the identity of the beneficiary.
- Purchaser is a shell company and the representative of the company does not like to disclose the identity of the beneficial owner.
- Address given by the customer is unknown, believed to be false, or simply a correspondence address.
- Customer purchases the property however, it seems that the property has not been used for a long time after the purchase.
- The person who is making the payment for the property is different from the person who occupies the property.

- Customer does not satisfactorily explain the last-minute substitution of the purchasing party's name.
- Customer pays substantial down payment in cash and balance is funded by an unusual source or offshore bank.
- Customer purchases property without inspecting it. It realizes that the customer needs to fund for the property and not much worries about the location or any other characteristic of the property.
- Customer purchases many properties in a short time period, and seems to have few concerns about the location, condition and anticipated repair costs, etc., of each property.
- Customer is known to have paid large remodeling or home improvement invoices with cash, on a property for which property management services are provided.
- Transaction does not match the business activity known to be carried out by the customer.
- Transaction is entered at a value significantly different (much higher or much lower) from the real or market value of the property.
- Property is sold in a series of successive transactions each time at a higher price between the same parties.
- Buyer takes on a debt significantly higher than the value of the property.
- Customer suddenly cancels/aborts transaction and requests refund either back to himself/herself/itself or to a third party.
- Customer pays for the purchase entirely in cash (to include electronic funds transfers), especially when such a purchase is large or does not match the known profile of the customer, and especially when the purchase funds are transferred from an offshore jurisdiction.

## Gem and Jewellery Dealers

Customer and customer behaviour:

- Customer executes transaction/transactions which is/are not consistent with his usual profile.
- A frequent customer, who buy/sell precious stone/metal or jewellery products makes a transaction/transactions inconsistent with his usual financial status/profile.

- Customer pays the value of the precious stone/metal or jewellery producing an unusual payment method.
- Customer conducts large or frequent transactions using foreign currency without any economic rationale.
- Frequent transactions by a customer especially over a short period of time below the regulatory threshold for customer due diligence, however the total of such transactions is substantial.
- Payments received for a purchase of a precious stone/metal or jewellery product from a third party who is not the owner of the funds, without any legitimate business purpose.
- Customer is suspected to be using forged, fraudulent or false identity documents for due diligence and record keeping documents.
- Customer is unusually concerned and/or makes inquiries about the AML/CFT requirements and internal compliance policies, procedures or controls.
- Customer attempts to maintain a high degree of secrecy with respect to transactions, for example by requesting not to keep normal business records.
- Customer avoids answering questions related to the source of money to buy the precious stone/metal or jewellery product.
- Customer is known to have a criminal/terrorism background.
- Customer appears to be related to a country or entity that is associated with ML/TF activities.

In addition to the above mentioned indicators, the following suspicious indicators on suppliers and supplier behaviours are depicted for the enhanced awareness of the gem and jewellery dealers;

Supplier and supplier behaviour:

- Supplier under/over invoice the value of the precious gem stone/metal.
- Supplier uses third parties in transactions related to precious gem stones/metals. Ex: funds paid to a third party who is not related to the supplier without any legitimate business purpose.
- Precious stones/metals/jewellery products delivered from a third party who is not related to the supplier, without any legitimate business purpose.

- The origin of the precious stones/metals/jewellery products appears to be fictitious.
- Supplier is unusually concerned with the AML/CFT requirements.
- Supplier attempts to maintain a high degree of secrecy with respect to the transactions and requests not to keep the normal business records.
- Supplier is not willing to disclose beneficial owners or controlling interests.
- Supplier demands the payment for the gem/jewelleries via an unusual payment method. Ex: Request for a bank deposit to a third party bank account, Request to handover cash to a third party, etc.
- For Diamonds;
    a. Rough Diamonds are not accompanied by a valid Kimberley Process (KP) certificate, or broadly recognized equivalent scheme for certification.
    b. No KP certificate attached to the shipment of rough diamonds
    c. The KP certificate is/appears to be forged.
- Supplier appears to be related to a country or entity that is associated with high ML/TF risk or a person that has been designated as terrorist.
- Supplier transports precious stones/metals through a country which is associated with high ML/TF risk, for no apparent economic reason.

**Appendix II**

# Schedule V

**CONFIDENTIAL**

Province :
District :

| SUSPICIOUS TRANSACTION REPORT | | |
|---|---|---|
| a. This report is made pursuant to the requirement to report suspicious transactions under the Financial Transaction Reporting Act, No. 6 of 2006<br><br>b. Under Section 12 of the Act, no civil, criminal or disciplinary proceedings shall be brought against a person who makes such report in good faith | | |
| **PART A - DETAILS OF REPORT** | | |
| 1 | Date of Sending Report | |
| 2 | Is this replacement to an earlier report? | Yes ☐ No ☐ |
| **PART B - INFORMATION ON SUSPICION** | | |
| 3 | Name in Full<br>(if organization, provide registered business/organization name) | |
| 4 | Residential/ Registered Address | |
| 5 | NIC No. / Passport No./ Business Registration No. | |
| 6 | Gender | Male ☐ Female ☐ |
| 7 | Country of Residence and Nationality (if an individual) | |
| 8 | Business/ Employment Type | |
| 9 | Occupation<br>(where appropriate, principal activity of the person conducting the transaction) | |
| 10 | Name of Employer (where applicable) | |
| 11 | Contact Details | |
| **PART C - DESCRIPTION OF SUSPICION** | | |
| 12 | Details of Transaction / Activity | |

**Appendix II**

| | | |
|---|---|---|
| 13 | Ground / Reasons for Suspicion | |
| **PART D - DETAILS OF REPORTING PERSON** | | |
| 14 | Date of Reporting | |
| 15 | Signature | |
| 16 | Name of Reporting Person/Agency | |
| 17 | NIC Number | |
| 18 | Designation / Occupation | |
| 19 | Address | |
| 20 | Contact Details | |