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

මූල්‍ය බුද්ධි ඒකකය நிதியியல் உளவறிதல் பிரிவு **Financial Intelligence Unit**

Ref : 037/03/011/0001/018

Guidelines – 06/2018

August 06, 2018

To: CEOO of All Financial Institutions

Dear Sir / Madam,

Guidelines for Financial Institutions on Suspicious Transactions Reporting, No. 06 of 2018

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 and the Suspicious Transactions (Format) Regulations of 2017.

Yours faithfully

D M Rupasinghe
Director
Financial Intelligence Unit

Cc : Compliance Officers

14 වන මහල, අංක **30**, ජනාධිපති මාවත,
තැ. පෙ. **590**, කොළඹ **01**, ශ්‍රී ලංකාව
94 11 2477125/509 **94 11 2477692**

14 ஆம் மாடி, இல. 30 சனாதிபதி மாவத்தை கொழும்பு 1
த. பெ. இல. 590, கொழும்பு 01, இலங்கை
fiu@cbsl.lk

Level **14** , No. 30, Janadhipathi Mawatha,
P. O. Box. 590, Colombo 01, Sri Lanka.
www.cbsl.gov.lk

Guidelines for Financial Institutions on Suspicious Transactions Reporting, No. 06 of 2018

Introduction

1. These Guidelines are issued pursuant to section 15(1)(j) of the Financial Transactions Reporting Act, No. 6 of 2006 (FTRA) applicable to Financial Institutions that engaged in or carrying out "finance business" as defined in Section 33 of the FTRA.

2. Suspicious Transactions (Format) Regulations of 2017 was issued on dated April 21, 2017 by Gazette Extraordinary No. 2015/56 applicable to Institutions which include institutions that engaged in or carrying out "finance business" as defined in Section 33 of the FTRA. These Guidelines are provided as an aid to interpret and apply Suspicious Transactions (Format) Regulations of 2017. These Guidelines are not intended to be exhaustive and do not constitute legal advice from the Financial Intelligence Unit (FIU). Nothing in these Guidelines should be construed as relieving Financial Institutions from any of their obligations under the Suspicious Transactions (Format) Regulations of 2017 or the FTRA.

3. The quality of a Suspicious Transaction Report (STR) is important in increasing the effectiveness of the quality of analysis and investigations undertaken by FIU and law enforcement agencies relating to such STR which would assist in preventing abuse of the Sri Lankan financial system by criminals and terrorists. Quality, in this sense, means reports should be based on results from an AML/CFT programme that is effectively implemented and that the content in reports are complete, accurate and latest. This guideline aims at assisting Financial Institutions in improving the quality of STRs submitted.

Legal Obligation

4. Section 7 of the Financial Transactions Reporting Act, No. 6 of 2006 (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 Financing of Terrorism 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 Financial Intelligence Unit.

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

5. As stated above as per the section 7 of the FTRA all "Institutions", should report suspicious transactions to the FIU. Institution means, any person or body of persons engaged in or carrying out any finance business or designated non-finance business as defined in the Section 33 of the FTRA.

6. As per Section 14 (1) (b) (iv) of the FTRA every institution is required to establish and maintain procedures and systems to implement the reporting requirement under Section 7 of the FTRA. Further, Section 14 (1) (d) requires every Institution to train its officers, employees and agents to recognize suspicious transactions.

7. As per Rule 15 of the Financial Institutions Customer Due Diligence Rule, No 1 of 2016, the internal AML/CFT Policy approved by the Board of Directors should include policies, procedures on the detection and internal reporting procedure of unusual and suspicious transactions and the obligation to report suspicious transactions to the Financial Intelligence Unit.

Prerequisites for Development of Suspicion

8. Reporting of suspicious transactions is a major functionality in the operation of an effective institutional AML/CFT programme. For the AML/CFT function to be meaningful, they must result from a Financial Institution's effective implementation of the FTRA, including all rules and instructions issued in relation to the FTRA. Financial Institutions without such effective implementation either tend to submit STRs that are inaccurate, incomplete or inappropriate or they may fail to report suspicious transactions entirely. Such failures expose the financial institution to regulatory, reputational, operational, and legal risks. In some cases, such failures may also expose both natural and legal persons to criminal liability.

9. For all but the very smallest institutions with the most intimate customer relationships, information about customers and transactions should be captured in a systematic manner and incorporated into their compliance and risk management processes. For larger Financial Institutions, this almost always means an electronic information

system. Such systems typically operate based on rules, scenarios and profiles that seek to measure and assess deviance of observed patterns from expected patterns, or seek to measure and assess conformity of observed patterns to known patterns of abuse of the financial system. Such systems need to be carefully configured to reflect the specific assessed risks of the Financial Institution. Such systems need to be continually evaluated and adjusted to maximize effectiveness, need to be continually updated with new operational and third-party information and need to be fully integrated into the Financial Institution's risk management process. When such systems generate alerts, it is important that the alerts are reviewed by the Financial Institution's Compliance Officer. While such system-generated alerts may be the cause for an STR, such alerts are not by themselves likely to form a complete STR in accordance with these guidelines and are not an acceptable substitute for such an STR.

Systems that operate in isolation are not effective. A system can only operate based on the information that is available to it. Systems are not generally capable of intuition or inference or human levels of perception. As such systems operate based on rules, scenarios and profiles that are designed by humans. For these reasons, Financial Institutions should not rely exclusively on systems to the exclusion of human involvement.

10. Whatever the source of customer and transaction knowledge, and whatever the technical sophistication of the AML/CFT system there must be an institutional will to make the system work. That is, there must be a will to detect suspicious transactions, to recognize in good faith such suspicious transactions for what they are when detected, and fully and accurately report such transactions, when recognized. Such institutional will is most effectively created by a commitment from those at the Senior Management including the Board of Directors of the Financial Institution and propagated through concrete actions and demonstrations (e.g. development of effective internal policies, processes and training programmes, compliance audits, investment in systems, consistent, fearless and disciplined exercise of judgment) to the rest of the staff of the Financial Institution.

Suspicion

11. Financial Institution must develop its own operating definition for suspicion. A Financial Institution's operating definition of suspicion should incorporate elements of unresolved and unsubstantiated but persistent feelings of doubt about an objective set of facts and circumstances relating to a behaviour, to a single transaction, to a series of transactions, 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 exits. The feeling of doubt cannot be relieved by proof, one way or another, since no proof is available. The definition should allow formation of a belief that is not firmly grounded or perfectly

clear. At the same time, the definition should not allow these beliefs to be fanciful or fleeting. Certainly, the definition should count as suspicious behaviours and activities that are unusual for the circumstances and not adequately or believably explained.

The operating definition for suspicion must pass a test of reasonableness. If the definition is too narrow or rigid, it may exclude generation of reports that concern unknown or unanticipated unlawful circumstances (i.e. "false negatives") and may also result in avoidance behaviour by criminals. On the other hand, a definition that is too broad or flexible might result in large number reports that are insufficiently analyzed and that do not reflect unlawful circumstances (i.e. "false positives" or "over compliance"). For Financial Institutions where electronic information systems are integrated into their processes, operating definitions are partially implemented by the triggers, profiles, scenarios and rules defined by the Financial Institution. Suspicious indicators and typologies may also be elements of such definition. The concept of "unusual" patterns of behaviour and transactions should also reflect in these definitions.

A non-exhaustive and unofficial list of suspicious indicators for transactions and behaviours is provided in Appendix I. The Financial Institution should complement this list with the Financial Institution's own indicators. When using indicators, it should be remembered that these indicators are not formulae and they do not necessarily indicate the presence of criminality. Conversely, the lack of known indicators does not necessarily mean the absence of criminality, in part because criminals may adjust behaviour to avoid such indicators. Instead, indicators, and especially combinations of indicators, should cause increased scrutiny that may lead to the formation of suspicion.

12. Financial Institutions being over compliance or malicious compliance will not generate expected quality of the STR. Overcompliance and malicious compliance are strongly discouraged.

    Over compliance results when Financial Institutions submit a large volume of reports that are inadequately analyzed or that fail to meet a reasonable standard of suspicion. Over compliance can be viewed as an attempt to transfer risk management from the Financial Institution to the FIU.

    Malicious compliance is when an Financial Institution submits reports that, although they may contain some superficial elements of suspicion, are known by the Financial Institution to not actually of suspicious nature.

13. If after consideration of facts and circumstances available to the Financial Institution in good faith and within the context of the Financial Institution's own understanding of suspicion and risks for the Financial Institution, and after gaining a thorough understanding of the FTRA and its implementing rules, regulations, circulars and guidelines, the Financial Institution has doubts about whether a behaviour or activity should be reported as suspicious, the best course of action is to report.

Reporting of STRs

14. **When Financial Institutions are provided with access to the LankaFIN system:** All reports must be submitted via LankaFIN online system or a successor system designated by the FIU followed by the signed hard copy of the STR submitted to the FIU by delivery or post.

15. **When Financial Institutions are not provided with access to the LankaFIN system:** Signed hard copy of the STR should be submitted to the FIU by delivery or post.

16. The Financial Institutions may submit STRs through other forms such as by way of email, fax or telephone in urgent situations to be followed by submission though LankaFIN and/or signed hard copy as appropriate within twenty-four hours.

Timing of Reporting

17. The FTRA requires suspicious reports to be submitted to the FIU as soon as practicably possible but no later than two working days of formation of suspicion. This means that, regardless of the Financial Institution's processes, procedures and steps after the initial formation of suspicion, the suspicion itself must be reported even if the Financial Institution's process has not completed. The Financial Institution's process for dealing with suspicion may proceed concurrently with the reporting of suspicion.

    For example, if the Financial Institution has a customer that receives a wire transfer in circumstances that the Financial Institution immediately considers to be suspicious, the Financial Institution must report the suspicious circumstances of that transaction as soon as practicable but within two working days even while the Financial Institution may continue with the internal processes that to verify the authenticity and details of the wire transfer.

18. If, after sending the report, the Financial Institution discovers additional facts and circumstances to either support or refute the Financial Institution's initial suspicion, then the Financial Institution should inform the FIU appropriately.

Content of Reporting

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

20. **Form Narrative:** The narrative portion of the report is most important. This is particularly true with respect to LankaFIN since other form fields capture only a limited amount of information. This is the Financial Institution's chance to fully describe the suspicion and the objective facts and circumstances that gave rise to and support the Financial Institution's suspicion. In any case the Financial Institution is unable to provide the full detailed narrative through LankaFIN, the Financial Institution may provide the narrative in a separate document and submit to the FIU along with the signed hard copy of the STR. In such cases, the Financial Institution should mention a brief summary of the narrative in the LankaFIN system and explicitly mention that a full narrative will be sent with the hard copy. The narrative should attempt to answer to the extent possible the basic descriptive questions of **what, who, when, where, why and how**.

    Financial Institutions should refrain from providing vague details of suspicions such as 'several high value third party deposits from several branches around the country'. Instead, Financial Institutions should provide clear quantitative and qualitative data such as '10 number of third party deposits having values between LKR 75,000 – 90,000 from Jaffna, Trincomalee, Kandy, Matara, Galle, Kataragama and Badulla branches during September, 2017' and provide relevant supporting documents (e.g. account statement for September 2017 including the details of third party depositors / deposits).

    Some of the questions that the narrative should attempt to answer, if possible, include:

    - What is the nature of the suspicion?
    - What offenses may have been committed?
    - What transactions, attempted transactions, behaviours, facts, belief and circumstances are involved and relevant to the suspicion?
    - Who are the natural and legal persons involved?
    - Who are the beneficial owners?
    - What are their identifiers such as names, ID numbers, registration numbers, etc.?
    - What are their addresses?
    - What are their occupations or lines/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?
    - What property is involved?
    - What is the nature and disposition and estimated value of involved property?
    - When and where did the transactions or attempted transactions or behaviours occur?

- How, if at all, do the timing or location of the transactions contribute to the Financial Institution's suspicion?
- Why do these facts and circumstances support the suspicion?
- How was the suspicion formed?
- What triggers or indicators are present?
- What actions have been taken by the reporting Financial Institution?
- What related STRs have the Financial Institution already submitted?
- What red flags are present?
- What deviations from expected activities have taken place?

Financial Institutions are required to provide reasonable grounds for the suspicion and are requested to refrain from citing unjustifiable reasons such as 'relationship between customers cannot be derived with the surnames', 'funds from African countries', etc.

The narrative should be structured in a logical manner so that information can be conveyed to the FIU analyst as efficiently, completely and accurately as possible. Essay formats could be used for 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. Within the body, information could be presented in a chronological manner when attempting to demonstrate possible causal links along a timeline. It is advised to minimize the use of Financial Institution's internal jargon and acronyms brandings, product names by using generic descriptors instead. For example, use "six-month term deposit account" rather than "Mega-Six Platinum Elite Plus Super Saver Account." Use punctuation and sentence case. Narrative should not be so brief as to compromise the goals of the narrative. It is advised to avoid words that do not contribute to the meaning of a sentence and to refrain from using too generic narratives such as 'the transaction pattern does not match with the customer profile'.

21. **Accuracy:** It is imperative that factual information provided in the report 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 an NIC, or a misplaced or transposed character in a name, can make the difference between a successful and an unsuccessful analysis. 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 the official registration documents.

Submission of Supporting Documents

22. Financial Institutions are required to submit relevant supporting documents along with the STR. If the Financial Institution is unable to submit the supporting documents via LankaFIN, the Financial Institution should submit the relevant supporting documents

through email and/or along with the signed hard copy of the STR. In such cases, Financial Institutions should mention in LankaFIN that additional supporting documents are submitted via email or through post.

23. 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 letter of credit, all the details from the letter of credit that are related to the suspicion should be included in the narrative. A copy of letter itself can then be provided as a supporting document.

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

Scenario	**Indicative list of Supporting documents**
Third party deposits	Bank Statements List of third party deposits Details of third party depositors
Foreign inward remittance	Bank statement Copy of SWIFT message
Suspicion regarding forged / altered identity (NIC/ Passport / Driving license)	Copy of the document
Suspicion related to a company	Registration documents Director details

Miscellaneous

Confidentiality

25. As per the Section 9 of the FTRA Financial Institutions are not allowed to inform any person, including the customer, about the contents of an STR and even that the Financial Institution has filed such a report to the FIU.

26. As per Rule 46 of the Financial Institutions Customer Due Diligence Rule, No. 1 of 2016, where a Financial Institution forms a suspicion of money laundering or terrorist financing risk relating to a customer and where the Financial Institution reasonably believes that conducting the process of CDD measures would tip off the customer, then the Financial Institution should terminate conducting the CDD measures and proceed with the transaction and immediately file an STR.

Breach of Confidentiality

27. If any customer is being tipped off about the reporting of STRs by any officer of the Financial Institution it would consider as a violation under the FTRA Section 9 and 10. This is described as the offence of 'tipping off' and is an offence punishable with a fine not exceeding five hundred thousand rupees or imprisonment of either description for a term not exceeding two years, or to both such fine and imprisonment.

Protection for Persons Reporting STRs

28. As per Section 12 of the FTRA:
    No civil, criminal or disciplinary proceedings shall lie against —
    (a) a such 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.

Failure to Report STRs

29. If a Financial Institution fails to submit STRs when reasonable grounds exist to suspect that a transaction is related to money laundering or terrorist financing, such is considered as non-compliance with the FTRA. As per Section 19 of the FTRA such non-compliances are liable to penalties up to one million rupees (Rs. 1,000,000.00) or double this for subsequent failures to report.

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

30. The FTRA does not prohibit Financial Institutions from continuing business relationships with customers about whom STRs has been reported or suspicion has been formed. Especially Financial Institution's behaviour toward the customer should not amount to any tipping off subject to the provisions of the Section 3 of the FTRA.

Obligations of Financial Institutions which has submitted an STR in relation to a customer and is continuing the business relationship

31. After the submission of an initial STR, the Financial Institution 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

32. Where the FIU has requested further information regarding any STR, the Financial Institution should take all necessary measures to provide such information promptly to the FIU.

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 Financial Institution. 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 Financial Institution 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 Institution to believe that unlawful activity may be involved.
- Any unresolved and persistent feelings of doubt related to customers and their transactions and 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 correspondence sent to home address.
- Customer appears to have accounts with several financial institutions for no apparent reason.
- 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 Financial Institution.
- Customer shows unusual curiosity about internal systems, controls and policies.
- Customer has only vague knowledge of the amount of a deposit.
- Customer presents confusing or inconsistent details about the transaction.
- Customer over justifies or explains the transaction.
- Customer tries to convince Financial Institution staff to alter or omit reporting data.
- Customer is secretive and reluctant to meet in person.
- Customer is nervous, not in keeping with the transaction.
- Customer insists that a transaction be done quickly.
- Customer attempts to develop a close rapport with staff.
- Customer offers money, oversized commissions, gratuities or unusual favours for the 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.
- Customer has no apparent ties to the community.
- Customer has irregular work/travel patterns.

Account Opening/Identity Indicators

- Customer provides doubtful or vague information.
- Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Customer refuses to produce personal identification documents.
- Customer only possesses copies of personal identification documents.
- Customer wants to establish identity using something other than his or her personal identification documents.
- Customer's supporting documentation lacks important details.
- Customer unnecessarily delays presenting corporate documents.
- All identification presented is foreign or otherwise unreasonably difficult to verify.
- All identification documents presented appear new or have recent issue dates.
- Customer is unemployed, or is an independent consultant, or switches jobs frequently.
- Customer conspicuously displays large amount of cash.

Indicators for a Businesses

- Lack of regular business hours.
- Unusually profitable business.
- Profitable business in a failing industry.
- Business receipts and incomes above industry norms.
- Cash intensive business.
- 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 uses account(s) that have been dormant.
- 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.

Cash Transaction Indicators

- Customer suddenly starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the customer in the past.
- Customer frequently exchanges small bills for large ones.
- Customer uses notes in denominations that are unusual for the customer, when the norm in that business is much smaller or much larger denominations.
- Customer presents notes that are packed or wrapped in a way that is uncommon for the customer.
- Customer deposits musty or extremely dirty bills.
- Customer makes cash transactions of consistently rounded-off large amounts.
- Customer consistently makes cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold.
- Customer consistently makes cash transactions that are significantly below the reporting threshold amount in an apparent attempt to avoid triggering the identification and reporting requirements.
- Customer presents uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which could trigger reporting requirements.
- Customer conducts a transaction for an amount that is unusual compared to amounts of past transactions.
- Customer frequently purchases traveler's checks, foreign currency drafts or other negotiable instruments with cash when this appears to be outside of normal activity for the customer.
- Customer asks the Financial Institution to hold or transmit large sums of money or other assets when this type of activity is unusual for the customer.
- Shared address for individuals involved in cash transactions, particularly when the address is also for a business location, or does not seem to correspond to the stated occupation (for example, student, unemployed, self-employed, etc.).
- Stated occupation of the customer is not in keeping with the level or type of activity (for example a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area) .
- Customer consistently claims that source of funds is gambling winnings with no evidence of corresponding losses.

Indicators Involving Loans

- Loans secured by pledged assets held by third parties unrelated to the borrower.
- Loan secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties.
- Borrower defaults on a cash-secured loan or any loan that is secured by assets which are readily convertible into currency.
- Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.
- To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via currency or multiple monetary instruments.

- Loans that lack a legitimate business purpose; provide the bank with significant fees for assuming little or no risk; or tend to obscure the movement of funds (*e.g.,* loans made to a borrower and immediately sold to an entity related to the borrower).
- Customer claims true ownership of assets used for collateral, even though assets held in a different name.

Trade Financing Indicators

- Items shipped are inconsistent with the nature of the customer's business (*e.g.,* a steel company that starts dealing in paper products, or an information technology company that starts dealing in pharmaceuticals).
- Customers ship items through high-risk jurisdictions, including transit through countries recognized as non-compliant with AML/CFT requirements.
- Customers involved in potentially high-risk activities, including activities that may be subject to export/import restrictions.
- Obvious over- or under-pricing of goods and services.
- Obvious misrepresentation of quantity or type of goods imported or exported.
- Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
- Customer requests payment of proceeds to an unrelated third party.
- Shipment locations or description of goods not consistent with letter of credit.
- Documentation showing a higher or lower value or cost of merchandise than that which was declared to customs or paid by the importer.
- Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment.

Transactions with Overseas or Offshore Jurisdictions

- Accumulation of large balances, inconsistent with the known turnover of the customer's business, and subsequent transfers to overseas or offshore account(s).
- Frequent requests for travelers checks, foreign currency drafts or other negotiable instruments.
- Loans secured by obligations from offshore banks.
- Loans to or from offshore companies.
- Offers of multimillion-value deposits from a confidential source to be sent from an offshore bank or somehow guaranteed by an offshore bank.
- Transactions involving an offshore bank whose name may be very similar to the name of a major legitimate institution.
- Unexplained electronic funds transferred by customer to/from offshore jurisdictions on an in-and-out (pass through) basis.
- Use of letter-of-credit and other method of trade financing to move money between countries when such trade is inconsistent with the customer's business or with national trade patterns.
- Use of a credit card issued by an offshore bank.

Suspicious Patterns involving Multiple Transactions

- Round trip transactions where funds are transferred to one destination, and then return in roughly the same amount from a different origin.
- Structured transactions that break transactions into smaller amounts to avoid reporting.
- Distributer/collector transactions where multiple accounts funnel into one, or one funnels into multiple without adequate explanation. This is an especially strong indicator when accounts may be controlled by single beneficial owner.

Transactions Involving Proxies

- Transactions where a person who is matched by two attributes (e.g. name and address, or name and birthday, or birthday and address) appears to maintain multiple accounts with variations in one of these parameters.
- Transactions with multiple accounts at the same address.
- Transactions where the address does not exist in public records.
- Transactions where the name does not exist in public records.
- Transactions where the account holder is a PEP.
- Transactions where the account holder is a relative or close associate of a PEP.
- Transactions where the account holder shares an address with a PEP.
- Large transactions by people with low-income jobs, especially when employed by or related to high wealth individuals.
- Transactions in the name of very young people.
- Transactions in the name of dead people.
- Transactions in the name of people living in areas where such wealth would be abnormal.

Red Flag Indicators for Specific Sectors

Securities Sectors

- Accounts that have been inactive suddenly experience large investments that are inconsistent with the normal investment practice of the client or their financial ability.
- Any dealing with a third party when the identity of the beneficiary or counter-party is undisclosed.
- Client attempts to purchase investments with cash.
- Client wishes to purchase a number of investments with money orders, traveller's cheques, cashier's cheques, bank drafts or other bank instruments, especially in amounts that are slightly less than the reporting threshold, where the transaction is inconsistent with the normal investment practice of the client or their financial ability.
- Client uses securities or futures brokerage firm as a place to hold funds that are not being used in trading of securities or futures for an extended period of time and such activity is inconsistent with the normal investment practice of the client or their financial ability.

- Client wishes monies received through the sale of shares to be deposited into a bank account rather than a trading or brokerage account which is inconsistent with the normal practice of the client.
- Client frequently makes large investments in stocks, bonds, investment trusts or other securities in cash or by cheque within a short time period, inconsistent with the normal practice of the client.
- Client makes large or unusual settlements of securities in cash.
- The entry of matching buying and selling of particular securities or futures contracts (called match trading), creating the illusion of trading.
- Transfers of funds or securities between accounts not known to be related to the client.
- Several clients open accounts within a short period of time to trade the same stock.
- Client is an institutional trader that trades large blocks of junior or penny stock on behalf of an unidentified party.
- Unrelated clients redirect funds toward the same account.
- Trades conducted by entities that you know have been named or sanctioned by regulators in the past for irregular or inappropriate trading activity.
- Transaction of very large value.
- Client is willing to deposit or invest at rates that are not advantageous or competitive.
- All principals of client are located outside of Sri Lanka.
- Client attempts to purchase investments with instruments in the name of a third party.
- Payments made by way of third party cheques are payable to, or endorsed over to, the client.
- Transactions made by your employees, or that you know are made by a relative of your employee, to benefit unknown parties.
- Third-party purchases of shares in other names (i.e., nominee accounts).
- Transactions in which clients make settlements with cheques drawn by or remittances from, third parties.
- Unusually large amounts of securities or stock certificates in the names of individuals other than the client.
- Client maintains bank accounts and custodian or brokerage accounts at offshore banking centres with no explanation by client as to the purpose for such relationships.
- Proposed transactions are to be funded by international wire payments, particularly if from countries where there is no effective anti-money-laundering system.

Money/ Currency Changers

- Customer requests a transaction at a foreign exchange rate that exceeds the posted rate.
- Customer exchanges currency and requests the largest possible denomination bills in a foreign currency.
- Customer is reluctant to divulge the source of currency
- Customer is unable to produce relevant documents to support transaction
- Customer requests that a large amount of foreign currency be exchanged to another foreign currency.
- Customer instructs that funds are to be picked up by a third party on behalf of the payee.

Mobile Money Service Providers

- Customer used multiple names/identities, in conjunction with providing multiple addresses, making it difficult to ascertain the true identity of the customer.
- The frequency of the customer's visits was excessive, and also involved the use a wide range of agent locations.
- The purpose of the transactions, and the relationship between the beneficiary and the ordering customer, does not appear to make business sense.
- Multiple senders transferring funds to a single individual
- Currency notes used are in “used notes” and/or small denominations (“used notes” may imply that notes are worn, dirty, stained, give off unusual smell, etc.)
- Customer attempts to send money to a person on a sanctions list
- Customer fails to provide verifiable identity information or refuses to provide verifiable identity information either for the customer and/or for the beneficiary
- Customer attempts to use or uses unusual or suspect identification documents.
- The customer wishes to engage in transactions that are inconsistent with the customer’s stated purposes when the account was initially set-up.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.