Guidelines

for

Suspicious Transactions Reporting (STR)

NEPAL RASTRA BANK

FINANCIAL INFORMATION UNIT, NEPAL

(FIU-Nepal)

Effective from January, 2020

Acronyms/Abbreviations

ALPA	Asset (Money) Laundering Prevention Act, 2008 (4^{th} amendment in 3 March, 2019)
AML/CFT	Anti Money Laundering and Combating the Financing of Terrorism
APG	Asia/Pacific Group on Money Laundering
BFIs	Bank and Financial Institutions
DNFBPs	Designated Non-Financial Businesses and Professions
FATF	Financial Action Task Force
FIU-Nepal	Financial Information Unit, Nepal
KYC	Know Your Customer
LEAs	Law Enforcement Agencies
ML/TF	Money Laundering and Terrorist Financing
REs	Reporting Entities
STRs	Suspicious Transaction Reports
TTRs	Threshold Transaction Reports

Disclaimer

This guideline cannot be relied on as evidence of complying with the requirements of the AML/CFT Act. The guideline is intended solely as an aid, and must not be applied as a routine instrument in place of common sense.

It should be noted that this guideline is not intended to be exhaustive. It requires constant updating and adaptation to changing circumstances and new methods of laundering money from time to time.

1. Introduction

This guideline has been issued for reporting entities to clarify the obligation to report suspicious transactions under the ALPA, 2008 and Asset (Money) Laundering Prevention Rules, 2016.

It aims to generate knowledge on indicators of suspicious activities and inform Reporting Entities (REs) about the technical requirements to report suspicious transactions. There are different indicators to detect suspicious transactions. In order to make the detection and filing of Suspicious Transactions Reports (STRs) expedient for the purpose of preventing money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, this guideline has been made and issued exercising the power conferred by ALPA, 2008.

2. Objectives

This guideline simply aims at assisting reporting entities in:

i. Identifying suspicious transactions and activities by providing indicators of suspicion
ii. Improving the quality of Suspicious Transaction Report (STR)
iii. Complying with the STR obligations by specifying when reports must be made, in what circumstances, what details to include and how to report them.

In many cases, reporting entities are unaware of the underlying criminal activity. However, by screening transactions and activities for known indicators, a reasonable suspicion that the transaction or activity is relevant to criminal offending may arise.

3. Reporting Entities and Regulators

As per ALPA, 2008 "Reporting Entity" (RE) means Financial Institutions and Designated Non-Financial Businesses and Professions (DNFBPs'). The reporting entities and their regulators are presented as follow:

Table: Reporting Entities and Regulators for AML-CFT

S.N.	Reporting Entities	Name of Regulators
a) Financial Institutions:		
1.	Bank and Financial Institutions	Nepal Rastra Bank
2.	Money Remitters	
3.	Money Changers	
4.	Security Companies	Securities Board of Nepal
5.	Insurance Companies	Insurance Board
6.	Co-operatives	Department of Co-operatives
7.	Approved Retirement Fund	Inland Revenue Department
8.	Non-Bank Financial Institutions (Employee Provident Fund, Citizen Investment Trust, Postal Bank)	Nepal Rastra Bank

S.N.	Reporting Entities	Name of Regulators
b) Designated Non-Financial Businesses and Professions (DNFBPs'):		
1.	Real Estate Businesses/Agents	Department of Land Management and Archive
2.	Trust and Company Service Providers	Company Registrar's Office
3.	Casinos or Internet Casino Business	Ministry of Culture, Tourism and Civil Aviation
4.	Dealers in precious stones and metals	Inland Revenue Department
5.	Auditors and Accountants	Institute of Chartered Accountants of Nepal
6.	Notary Public	Notary Public Council
7.	Law Practitioners	Nepal Bar Council

Separate AML/CFT directives have been issued by the above mentioned regulators for reporting entities under their jurisdictions.

4. Legal Obligations

As per section 7S (1) of ALPA, 2008, Reporting Entity shall make a suspicious transaction report to the FIU within three days as soon as possible if they find following circumstances in relation to any customer, transaction or property:

i. If it suspects or has reasonable grounds to suspect that if the asset is related to ML/TF or other offence, or

ii. If it suspects or has reasonable grounds to suspect that the asset is related or linked to, or is to be used for, terrorism, terrorist, terrorist acts or by terrorist organization or those who finance terrorism.

5. Transactions

A transaction or attempted transaction for which the customer refuses to provide satisfactory evidence of identity should also be reported as a suspicious transaction/activity to the FIU-Nepal. Throughout this guideline, any mention of a "transaction" includes one that is either completed or attempted as explained below.

i. **Completed transactions:** A completed transaction is one that has occurred. For example, if you process a deposit from a client towards the purchase of an asset such as a life insurance policy or a house, a financial transaction has occurred. This is true even if the final sale associated to the deposit does not go through. In this example, the refund of the deposit shall also be a financial transaction.

ii. **Attempted transactions:** An attempted transaction is one that a client intended to conduct and took some form of action to do so. An attempted transaction is different from a simple request for information, such as an enquiry as to the fee applicable to a

certain transaction. An attempted transaction includes entering into negotiations or discussions to conduct the transaction and involves concrete measures to be taken by either you or the client.

The following are examples of attempted transactions:

- A financial institution refuses to accept a deposit because the client refuses to provide identification as requested.
- A client of a real estate agent starts to make an offer on the purchase of a house with a large deposit, but will not finalize the offer once asked to provide identification.
- An individual asks an accountant to facilitate a financial transaction involving large amounts of cash. The accountant declines to conduct the transaction.
- A money services business will not process a request to transfer a large amount of funds because the client requesting the transfer refuses to provide identification requested.

6. Suspicious Transaction Report

Suspicious Transactions are financial transactions in which there are reasonable grounds to suspect that, the funds involved are related to the proceeds of criminal activity. What is reasonable depends on the particular circumstances, industry, normal business practices within the industry.

Suspicious Transactions Reports (STRs) include detailed information about transactions that are or appear to be suspicious. The purpose of a STR is to report known or suspected violations of law or suspicious activity observed by reporting entities subject to the provision related ALPA, 2008. The goal of STR filing is to help FIU-Nepal to identify individuals, groups and organizations involved in predicate offences as defined in ALPA, 2008. In many instances, STRs have been instrumental in enabling law enforcement to initiate or supplement major money laundering or terrorist financing investigations and other criminal cases.

The quality of a STR is important in increasing the effectiveness of the quality of analysis and investigations undertaken by FIU-Nepal and LEAs which would assist in preventing abuse of the Nepalese financial system by criminals and terrorists. Furthermore, the reporting entity has to submit STRs as per the prescribed STR format by their regulators.

7. Who must Report?

REs must report STR of any transactions conducted (or attempted) that are considered suspicious to FIU-Nepal. STR can start with any employee of a reporting entity; however a reporting institution has to appoint a compliance officer of management level to report STRs and to deal with FIU on matters relating to STRs as per Section 7P of ALPA, 2008.

8. What to report?

REs must fill up the STR format as prescribed by their regulators. However the STR must contain at minimum following information:

- Summary of suspicious activities
- Analysis or Examination
- Possible Linkage
- Suspected Beneficiary (if any)
- Mandatory details (as required by regulators)
- Correct identifications
- Other details

The STR submitted to FIU-Nepal should contain following supporting documents:

i. In case of Person

- Updated KYC related documents
- Account Statement (if available)
- Summary suspicious transaction identified
- Media news/reports and other relevant documents if any

ii. In case of Entity

- Registration Certificate
- PAN/VAT Certificate
- Updated KYC related documents of Entity and its Director(s) and Signatory(ies)
- Account Statement (if available)
- Summary of suspicious transaction identified
- Media news/reports and other relevant documents if any

9. How to Report?

i. STR can be reported to the FIU-Nepal electronically through goAML system by BFIs and through signed paper reports by other REs. FIU-Nepal will gradually makes compulsory reporting of STR through goAML to all REs.

ii. REs should provide their reports of suspicious transactions to the FIU-Nepal through their Compliance Officer. There should be clear internal reporting procedures in REs and all employees must follow the reporting procedures.

10. When to Report?

i. A suspicious transaction must be reported to the FIU-Nepal as soon as possible but no later than three working days after detection the initial suspicion or the receipt of the information being reported on.

ii. If the reporting entity discovers additional facts and circumstances to either support or refuse the reporting entity's initial suspicion after sending the report, then the reporting entity shall inform the FIU-Nepal appropriately through hard copy or electronically.

11. Are cash transactions only to be reported as suspicious transactions?

i. The requirement to report any suspicious transaction applies to all types of transactions or activities regardless of whether cash is involved or not. Thus non-cash transactions, such as telegraphic/wire transfers, suspicious activities, that may appear suspicious shall also be reported.

ii. **There is no monetary threshold amount for reporting suspicious transactions.** Thus, a transaction considered suspicious should be reported to the FIU-Nepal regardless of the amount of the transaction.

12. Content of Reporting

i. **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 behaviors are connected with a suspicion, a single report should be filed capturing all of these.

ii. **Narrative:** The narrative portion of the report is most important. REs should perform proper analysis at their end regarding the STR and provide preliminary analysis report with relevant information and details as to why the reported transactions are suspicious. The narrative should attempt to answer to the RE should provide clear quantitative and qualitative data and should refrain from providing vague details.

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

- What is the nature of the suspicion and how was the suspicion formed?
- Why do these facts and circumstances support the suspicion?
- What red flag, triggers or indicators are present?
- What offences may have been committed?
- What transactions, attempted transactions, behaviors, facts, beliefs and circumstances are involved and relevant to the suspicion?
- Who are the natural and legal persons involved?
- Who are the beneficial owners, their employers?
- What are their identifiers such as names, citizenship numbers, registration numbers, etc.?
- What are their addresses, occupations or types of business?

- Any political exposure?
- How are they connected with each other and with the transactions?
- What were their roles in the transactions?
- What asset is involved?
- What are the nature, disposition and estimated value of involved property?
- When and where did the transactions or attempted transactions or behaviors occur? How, if at all, does the timing or location of the transactions contribute to the reporting entity's suspicion?
- What actions have been taken by the reporting entity?
- What related STRs have the reporting entity already submitted?
- What deviations from expected activities have taken place?

The narrative shall be structured in a logical manner so that information can be conveyed to the FIU-Nepal analyst as efficiently, completely and accurately as possible. Narrative shall not be so brief as to compromise the goals of the narrative.

iii. **Accuracy:** It is imperative that factual information provided in the report is accurate. This is particularly true for identifiers such as names, citizenship numbers, registration numbers, etc. All spellings and transcriptions of identifiers should be double checked. A single inaccurate digit in a passport number or work permit, 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) shall be exactly identical in every respect to those found on the official registration documents.

13. Reporting STRs through goAML software

For those REs who report STR through goAML software has to submit the reports as per the goAML Schema and Operational Guideline, 2020 issued by FIU-Nepal. The REs should properly understand the business logic behind any transaction and provide all the necessary and available information while reporting in goAML as per the goAML operational guideline which also exemplifies various transactions that REs have to report. Since there are numerous groups of REs, FIU-Nepal has adopted phase-wise implementation plan for the effective and successful implementation of goAML system.

14.Indicators of Suspicious Transactions

A transaction may have certain 'red flags' that give rise to a suspicion that it is linked to criminal activity or criminals. These 'red flag' features are described as indicators. It is important that reporting entity staff can recognize indicators, especially indicators relevant to its specific business as this will help determine if a transaction is suspicious. The presence of

one or more indicators may not be evidence of criminal activity; it may however raise a suspicion. The presence of multiple indicators should act as a warning sign that additional inquiries may need to be undertaken. Additional inquiries made by compliance officer may help to dismiss or support the suspicion.

There are various indicators to detect suspicious transactions. In order to make the detection of STRs expedient for the purpose of preventing money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, the indicators of suspicious transactions have been categorized into; 1)General and 2)Sector-specific indicators. These indicators are offered as a guide and it is not an exhaustive list of every possible indicator. The staffs of REs should be aware that criminals and organized crime groups regularly adapt their behavior to exploit weaknesses within different industries to launder funds.

A) General Indicators

I. Cash

- Transactions conducted in a relatively small amount but with high frequency (structuring).
- Transactions conducted by using several different individual names for the interest of a particular person (smurfing).
- If customer conducts series of transactions or bookkeeping tricks for concealing the source of fund (layering).
- If 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.
- The purchase of several insurance products in cash in a short period of time or at the same time with premium payment entirely in a large amount and followed by policy surrender prior to due date.
- If person sending money cannot provide even general information about the recipient of money.
- If anyone attempts to transfer or receive amount in a suspicious manner.

II. Economically Irrational Transactions

- Transactions having no conformity with the initial purpose of account opening.
- Transactions having no relationship with the business of the relevant customer.
- Transaction amount and frequency are different from that of normally conducted by the customer.

III. *Behaviors of the Customer*

- Unreasonable behaviors of the relevant customer when conducting a transaction (nervous, rushed, unconfident, etc.)
- Customer with significant Money Laundering, Terrorist Financing and Proliferation Financing related adverse news or other indicators relating to financial crime.
- If customer shows unusual curiosity about internal system, control and reporting.
- If customer admits or makes statements about involvement in criminal activities.
- If customer offers money, gratuities or unusual favors for the provision of services that appear unusual or suspicious.
- If customer/prospective customer gives doubtful or false information with respect to his/her identity, sources of income or businesses.
- If customer/prospective customer uses identification document that is unreliable and refuses to provide information/documents requested by the officials of the relevant reporting entity without any valid reasons.
- If customer or his/her legal representative tries to persuade the officials of the relevant reporting entity not to report his/her transaction as a Suspicious Financial Transaction.
- If customer opens the account for a short period and closes without a valid reason.
- If customer is unwilling to provide right information or immediately terminating business relationship or closing his/her account at the time the officials of the relevant reporting entity request information with respect to his/her transaction.
- Only online transactions are done in the customer's account, in such case there can be separate beneficial owners.

IV. *Employees and Agents of REs*

- Changes in employee characteristics, (e.g. lavish lifestyles or avoiding taking holidays).
- Changes in employee or agent performance.
- Any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

V. *Use of third party*

- Multiple deposits made to an account by non-account holders.
- Unrelated parties sending fund transfers or other forms of electronic transfers to the same beneficiary with no apparent relation to the recipient.
- If a client conducts transaction while accompanied, overseen or directed by another party.
- If a client makes numerous outgoing payments to unrelated parties shortly after they receive incoming funds.

- Wire transfers, deposits or payments to or from unrelated parties (foreign or domestic).
- If a client appears or states to be acting on behalf of another party.
- Account is linked to seemingly unconnected parties.
- If power to attorney to operate account is given to third party

VI. Corporate and Business Transactions

- If accounts are being used to receive or disburse large amounts but shows no normal business related activities, such as the payment of payrolls, invoices, etc.
- If the transaction is not economically justified considering the account holder's business or profession.
- If business transactions is found to be done through personal accounts
- If customer makes a large volume of cash deposits from a business that is not normally cash-intensive.
- If customer does not want to provide complete customer due diligence information of their business.
- If the financial statements of the business differ noticeably from those of similar businesses without valid reasons.
- If size of wire/fund transfers is inconsistent with normal business practice/transactions for the customer.
- If unexplained transactions are repeated between personal and business accounts.
- If deposits to or withdrawals from a corporate account are primarily in cash rather than in the form of debit and credit normally associated with commercial operations (e.g. Cheques, Letters of Credit, Bills of Exchange, etc.)

VII. Wire/Funds Transfer Activities

- If customer fails to provide adequate information about the originator, beneficiary, and purpose of the wire transfer.
- If customer orders wire transfers in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- If the pattern of wire transfers shows unusual patterns or has no apparent purpose.
- If customer receives frequent fund transfers from individuals or entities who have no account relationship with the person/institution.
- Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
- If several customers request transfers either on the same day or over a period of two to three days to the same recipient.
- If beneficiaries of wire transfers involve a large group of nationals of countries associated with terrorist activities.

- If customer conducts series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds.
- Fund transfers to and from high-risk offshore financial centers without any clear business purpose.
- Fund transferred to and from high risk jurisdictions and sanctioned countries.
- Receipts of fund transfer in several phases and once accumulated the funds are subsequently transferred entirely to other account.
- Receipts/payments of funds made by using more than one account, either in the same name or different names.
- Fund transfers using the account of reporting entities' employee in an unusual amount.
- Remittance and donations are received on personal account whereby the use of the fund is not clear e.g. fund received for day to day transactions of school, monastery, church, Madarsa etc.
- If multiple inward or outward remittance transaction is conducted with the person from the country or region where terrorist organizations operate.

VIII. Lending

- If customer makes a large, unexpected loan payment with unknown source of funds, or a source of fund that does not match what the credit institution knows about the customer.
- If customer suddenly repays a problematic loan unexpectedly without a valid reason.
- If customer repays a long term loan, such as a mortgage, within a relatively short time period.
- If the source of down payment is inconsistent with borrower's financial ability, profession and business as per the declaration.
- If customer shows income from foreign sources on loan application without providing further details.
- If customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction.
- If the loan transaction does not make economic sense (e.g. the customer has significant assets, and there does not appear to be a valid business reason for the transaction).

IX. Trade Based Money Laundering

- Submitting the fake documents and false reporting by the customer such as commodity misclassification, commodity over- or under-valuation etc.
- If the transaction involves the use of repeatedly amended or frequently extended letters of credit without reasonable justification.

- Phantom shipping – If no goods are shipped and all documentation is completely falsified to move funds in the guise of trade.
- Payments to the vendor by unrelated third party.
- If the customer trades commodities that do not match the nature of business of the customer.
- If the commodity is shipped to (or from) a jurisdiction designated as "high risk" for money laundering activities.
- In case of Double-invoicing.
- If there are significant discrepancies between the descriptions of the goods on the transport documents, the invoice, or other related documents.
- If customer is involved in potentially high-risk activities, including those subject to export/import restricted goods such as weapons, ammunition, chemical mixtures, classified defense articles, sensitive technical data, nuclear materials etc.

X. Money Service Businesses (Including Currency Exchange and Money Remittance)

- The use of numerous agent locations for no apparent reason to conduct transactions.
- Multiple low-value international funds transfers, possibly indicating a large amount of funds broken down into smaller amounts.
- Several Customers request transfers either on the same day or over a period of two to three days to the same recipient.
- Customer does not appear to know the recipient to whom he or she is sending the transfer.
- Customer conducts large transactions to/from countries known as narcotic source countries or as trans-shipment points for narcotics or that is known for highly secretive banking and corporate law practices.
- Customer exchanges currency and requests the largest possible denomination bills in a foreign currency.
- Customer knows little about address and contact details for payee, is reluctant to disclose this information, or requests a bearer instrument.
- Customer instructs that funds are to be picked up by a third party on behalf of the payee.
- Customer makes large purchases of traveler's cheques which are inconsistent with known travel plans.
- Customer requests that a large amount of foreign currency be exchanged to another foreign currency.
- Large amounts of currency exchanged for traveler's checks.
- Customer exchange small denomination of bills for larger denominations.

XI. Company and Trust service providers

- Creation of complicated structures where there is no legitimate economic reason.
- Use of an intermediary without a legitimate reason.
- Trust assets are withdrawn immediately after being settled into the trust account, unless there is a plausible reason for such immediate withdrawal.
- Funds received from high risk jurisdictions.
- Previously inactive trust account is now used intensively, unless there is a plausible reason for such use.
- Transactions relating to the trust account are conducted with countries or entities that are reported to be associated with terrorist activities or with persons that have been designated as terrorists.
- Frequent changes to the address or authorised signatories.
- Unconvincing or unclear purpose or motivation for having trusts established in Nepal.

XII. Accountants and Lawyers

- Use of an agent or intermediary without obvious reason.
- Customer's business account particularly shows large cash deposits without a valid reason.
- Funds are received from a foreign jurisdiction, particularly, where there is no connection between the jurisdiction and the customer.
- Overseas instruction from a customer for no economic reason.
- Customer is not concerned about the level of fees/charges.
- Customer appears to have access to cash substantially above their means.
- Use of many different firms of auditors and advisers for connected companies and businesses
- Client has a history of changing bookkeepers or accountants yearly.
- Company shareholder loans are not consistent with business activity.
- Company makes large payments to subsidiaries or other entities within the group that do not appear within normal course of business.
- Client is willing to pay fees without the requirement for legal work to be undertaken.
- Purchase of properties for family members where there is a lack of personal contact without good reason gives raises doubts as to the real nature of the transaction
- Significant amount of private funding/cash from an individual who was running a cash intensive business.
- Involvement of third parties funding without apparent connection or legitimate explanation.
- Client provides false or counterfeited documentation
- There are attempts to disguise the real owner or parties to the transaction
- Large financial transactions requested by recently set up companies, not justified by

the activity of the client

- Unexplained use of Power of Attorney to purchase\sale assets.
- Customer uses a virtual office.

XIII. Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction

- In case of an account opened in the name of an entity, an organization or association, which found to be linked or involved with a suspected terrorist organization.
- Transactions involving certain high-risk jurisdictions such as locations in the midst of or in proximity to, armed conflict where terrorist groups operate or locations which are subject to weaker ML/TF controls.
- The use of funds by a non-profit organization is not consistent with the purpose for which it was established.
- Raising donations in an unofficial or unregistered manner (and its ultimate use is also not clear)
- Client identified by media or law enforcement as having travelled, attempted or intended to travel to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Transactions involve individuals or entities identified by media and/or sanctions lists as being linked to a terrorist organization or terrorist activities.
- Law enforcement information provided which indicates individuals or entities may be linked to a terrorist organization or terrorist activities.
- Client conducted travel-related purchases (e.g. purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Individual or entity's online presence supports violent extremism or radicalization.
- Client donates to a cause that is subject to derogatory information that is publicly available (e.g. crowdfunding initiative, charity, non-profit organization, non-government organization, etc.)
- If any person or entity is involved to provide, receive, collect or make arrangements of funds whether from legitimate or illegitimate source, by any means, directly or indirectly, to carry out terrorist activities and proliferation of weapons of mass destruction.
- If the customer is found to have involvement in illicit trafficking of arms and ammunition, nuclear chemical, biological weapons and related materials and their means of delivery.
- If it is evident that the asset is earned from the offence relating to arms and ammunition under the prevailing law.

B) Sector- Specific Indicators

I) Bank and Financial Institutions

- If transaction seems to be inconsistent with the customer's apparent financial ability or profession or usual pattern of financial transaction as per the declaration.
- If customer attempt to open or operate accounts under a false name.
- If transaction involves a country known for highly secretive banking and corporate law.
- If customer shows reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the institution to verify.
- Opening accounts when the customer's address or employment addresses are outside the local service area without a reasonable explanation.
- There is a sudden change in customer's financial profile, pattern of activity or transactions.
- Customer uses notes, monetary instruments, or products and/or services that are unusual for such a customer.
- If unknown third party frequently transfer funds into customer's account.
- If there is suspicion on the transaction of the customer who is blacklisted by Credit Information Bureau or the reporting institution itself has placed the concerned customer in a high-risk customer category.
- If customer is suspected for using of personal account for business or other purposes, or vice-versa.
- If customer fails to provide reasonable justification for the transaction.
- If customer conducts series of complicated transfers of funds that seems to be an attempt to hide the source and intended use of the funds.
- If unnaturally huge amount is transferred to the name or account of any foreign citizen, tourist, student, visitor, worker or a person recently migrated to Nepal from the country or region where terrorist organizations operate.
- If unrelated third party is unnaturally, unnecessarily involved or is more active in transaction.
- If multiple personal and business accounts are being used to collect and then channel funds to foreign beneficiaries of the countries known or suspected to facilitate money laundering activities or terrorism financing.
- If there is repeated transfer of money to and from the name of foreign individual or the individual living outside Nepal without any valid reason.
- If customer has frequent deposits identified as proceeds of asset sales but assets

cannot be substantiated.

- In case of large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.
- If account has close connections with other business accounts without any apparent reason for the connection.
- If deposits to or withdrawals from a corporate account are primarily in cash.
- If customer requests movement of funds that are uneconomical without any valid justification.
- If customer visits the locker (safety deposit box) area immediately before making cash deposits.
- If customer repeatedly conducts large foreign exchange transactions.
- If any suspicious pattern emerges from customer's transactions.
- If customer is found to have used/made or involved with counterfeit coin and currency.

II) Securities Market

- If customer conducts complex, unusual large transactions and unusual pattern of transactions or which have no apparent economic or visible lawful purpose.
- If accounts that have been inactive for a long period suddenly experience large investments that are inconsistent with the normal investment practice of the client or their financial ability.
- If there is reasonable ground to suspect that the purchase or sale of security is related or linked to, or is to be used for, terrorism, terrorist, terrorist acts or by terrorist organization or those who finance terrorism.
- Trading between numerous accounts controlled by the same people or use of the same passwords for different client accounts.
- Request by client for investment management or administration services where the source of the fund is unclear or not consistent with the client's apparent standing.
- If client deposits fund into the broker's account and requested repayment of funds within a short period of time with no apparent reason; little or no trading was recorded during the period; and the amount of funds deposited was not in line with the client's profile.
- Suspicious behavior of client (high profits within one day, purchase and sale of the security one day later).
- Purchase of securities by cash, transfer, or cheques under other person's name.
- If client wishes to purchase a number of investments especially below the reporting threshold limit, where the transaction is inconsistent with the normal investment practice of the client or their financial ability.
- If client purchases a large number/value of securities with cheques issued by a third

party.

- Transaction with the client sanctioned by APG/FATF/United Nations or other Inter-government international organizations.
- If transaction patterns resemble a form of market manipulation, for example, insider trading and pump and dump.
- **Insider Trading:**

REs must watch out for suspected insider trading made by someone who possesses material and nonpublic information. Such person can be:

- Corporate insiders who traded the company's securities after learning of significant, confidential developments;
- Insiders' friends and family, as well as other recipients of tips who traded securities after receiving such information;
- Employees of service firms such as law, banking, brokerage, and printing companies who came across material nonpublic information on companies and traded on it; and
- Government employees who obtained inside information because of their jobs.

The suspicious transaction indicators for Insider Trading are:-

- The customer makes a large purchase or sale of a security, or option on a security, shortly before news is issued that affects the price of the security;
- The client is known to have friends or family who work at or for the securities issuer.
- A customer's trading patterns suggest that he or she may have inside information.
- The customer's purchase does not correspond to his or her investment profile. For example, the customer may never have invested in equity securities, but does so at an opportune time.
- A customer trades in selective stock just after opening the account and makes sizeable profit in each trade.
- A customer trading in small amount of shares suddenly takes a sizable position in a specific stock and makes a considerable profit on it.
- A customer earns a sizable profit by generating a considerable portion of market volume in illiquid stock.
- The customer's account is opened or significantly funded shortly before a purchase
- The client sells his or her position in a security in conjunction with a significant announcement about the security.

- **Market Manipulation:**
  Market manipulation generally refers to conduct that is intended to deceive investors by controlling or artificially affecting the market for a security. In particular, the manipulator's purpose is to drive the price of a security up or down in order to profit from price differentials. The suspicious indicators for Market Manipulation are:-
    - The client engages in large or repeated trading in securities that are illiquid, low priced or difficult to price.
    - The officers or insiders of the issuing company have a history of regulatory violations.
    - The issuing company has failed to make required regulatory disclosures.
    - If security price is artificially raised ("pumped"); the security is then sold ("dumped") for profit.

III) Insurance Sector

- If client purchases products which are inconsistent with the buyer's age, income, profession or financial history.
- If client purchases insurance products using a single, large premium payment, particularly when payment is made through unusual methods such as currency or payment made through third party.
- If client shows more interest in the cancellation or surrender than in the long-term results of investment.
- If client is known to purchase several insurance products and uses the proceeds from an early policy surrender to purchase other financial assets.
- If client makes lump sum contributions to personal pension contracts.
- If client purchases an annuity with a lump sum rather than paying regular premiums over a period of time, particularly if the beneficiary is of an age which entitles him to receive the funds soon after.
- If client funds the policy using payments from a third party.
- If client purchases several policies just under the threshold limit, instead of purchasing one large policy.
- If client terminates product, especially at a loss, or where cash was tendered and/or the refund cheque is to a third party.
- If client purchases various policies and cancels regularly.
- If client makes overpayment of premiums with a request for a refund of the amount overpaid.
- If client intentionally caused, inflated or fraudulent claims and intentionally destroy the asset in order to access funds through insurance claim, which then appear legitimate.
- If client is found to have involvement in establishment of bogus reinsurers/ insurers

to launder the proceeds of crime.

- If client is found to have involvement in the terrorist activities or proliferation financing, etc.

IV) Real Estate

- If there exists discrepancy between the income or occupation and wealth of the buyer and the property as per the declared source of income.
- Transactions carried out on behalf of minors, incapacitated persons or other persons who appear to lack the economic capacity to make such purchases.
- Purchaser buys multiple properties in a short time period, and seems to have few concerns about the location, condition or with no interest in the characteristics of the property.
- Manipulation of the appraisal or valuation of a property (undervaluation, overvaluation and successive sales at higher values).
- If the amount listed on the contract of sale is found to be less than or greater than the real transaction price and Rajinama (Sales Deed).
- If customer purchase or sale real estate using a third party or family member (often someone with no criminal record) as the legal owner for concealment of the ownership.
- If the purchaser is a company with complicated beneficial ownership.
- Transactions involving persons who are being tried or have been sentenced for crimes related to Money Laundering/Terrorist Financing or who are publicly known to be linked to criminal activities involving illegal enrichment, or there are suspicions of involvement in such activities.
- Transactions in which the party asks for the payment to be divided into smaller parts with a short interval between them.
- Immediate resale of the property, especially when the resale price is dramatically higher without explanation compared to purchase price.

V) Non Profit Organizations

- Inconsistencies between the pattern or size of financial transactions and the stated purpose for which the organization was established and activities of the organization as per the declaration.
- Sudden increase in the frequency and amounts of financial transactions for the organization, or if the organization seems to hold funds in its account for a very long period.
- If the account of NGO/INGOs receives foreign funds without the knowledge of its regulator (Social Welfare Council).
- If the funds for the organizational use comes in the name of individuals instead of the

organization's account.

- If there is absence of contributions from donors as per the declaration.
- If the organization has operations or funds from, or transactions to, high-risk jurisdictions.
- If the account shows signs of unexplained increase in deposits and transaction activities.
- If the organization performs activities for encouraging or glorifying terrorism, money laundering, illicit fundraising, inciting racial or religious hatred, or inciting other criminal acts or public order offences.
- If the organization raises donations in an unofficial or unregistered manner.
- If the organization plans or commits act of terrorism, which may include the use of weapons of mass destruction and fosters extremism.
- If the organization has the donors from the countries identified as lacking appropriate anti-money laundering or counter terrorist financing regulation.
- If the act of donor, beneficiaries or partner is found to be suspicious with the suspect of Money laundering or Terrorist financing.
- If the organization or its representatives are linked to third parties that support or are engaged in terrorist activity or procure dual-use equipments.
- If the bank accounts of the organization are used by entity/person whose own accounts are under restrictions.
- If the organization merges with another organization believed to support terrorist activities.

VI) Retirement Fund

- Large cash sums deposited in retirement fund by members, particularly when followed by substantial withdrawals of funds without a valid reason.
- The type or volume of the transaction, which is untypical of the economic activity of the client and transactions conducted by the client arise suspicion.
- If unrelated third party pays contributions on behalf of a member of the retirement fund.
- Funds or other assets deposited into a retirement fund which are inconsistent with the profile of the client.
- Media reports of illegal activity.

VII) Casino and Internet Casino Business

- In case of win or lose of more than Rs. 2,500,000 by an individual in one transaction or in a series of transactions in one day.
- Activities inconsistent with the customer's profile.
- Dramatic or rapid increase in size and frequency of transactions.
- Client requests a winning cheque in a third party's name.

- Noticeable changes in spending/betting pattern.
- Customer conducts several transactions just below reporting thresholds.
- Inconsistent identity information presented or refusal to provide required identification.
- Client request cheques that are not for gaming winnings.
- Customer's intention to win is absent or secondary.
- Purchasing and cashing out casino chips with little or no gaming activity.
- Client purchases large volume of chips with cash, participates in limited gambling activity with the intention of creating a perception of significant gambling, and then cashes the chips for a casino cheque.
- Client exchanges small denomination bank notes for large denomination bank notes.
- If client is known to have used multiple names.
- Any deviation in transactions or suspicious activities identified by casino business.

VIII) Dealers in precious gems, stones and metal

- Unusual patterns of buying and selling which are inconsistent with customer's financial ability and profile.
- Established customer dramatically increases purchase for no apparent reason.
- If the origins of the precious stone, precious metal or precious product appear to be fictitious/suspicious.
- The customer is unable or unwilling to provide information for due diligence and record keeping purposes.
- The customer appears to be related to a country or entity that is associated with money laundering or terrorism activities or a person that has been designated as terrorists.
- The customer appears to be in a hurry to complete the transaction.
- If customer requests for or conducts over/under-invoicing, structured, complex, or multiple invoice requests.
- Large or frequent transactions that are in a foreign currency.
- Numerous transactions by a customer, especially over a short period of time, such that the amount of each transaction is not substantial (e.g. below the regulatory threshold for customer due diligence), but the cumulative total of which is substantial.
- The customer is suspected to be using forged, fraudulent or false identity documents for due diligence and record keeping purposes.
- The customer is unusually concerned with the Regulated Dealer's AML/CFT policies.

C) Indicators related to laws

- If it is evident that the asset is earned from the offence of murder, theft, fraud, forgery of documents, counterfeiting, trafficking of human beings, abduction and hostage taking under the relevant prevailing laws.
- If it is evident that the asset is earned from the offences under the below mentioned prevailing laws of Nepal:
    - Foreign exchange regulation laws.
    - Narcotics control laws.
    - National park and wildlife conservation laws
    - Human trafficking and transportation control laws.
    - Cooperatives laws.
    - Forestry laws.
    - Corruption control laws.
    - Bank and financial institution laws.
    - Banking offense and punishment laws.
    - Ancient monuments conservation laws.
    - Consumer protection, black market control and competition laws.
    - Company, commerce, supply, transport business laws.
    - Education, health, drugs, and environment laws.
    - Foreign employment laws.
    - Lottery, gambling and charity laws.
    - Insider trading, fake transaction, securities and insurance laws.
    - Negotiable instrument laws.
    - Election laws.
    - Intellectual and industrial property laws.
    - Communication, transmission, and advertisement laws.
    - Land, house and property laws.
    - Immigration, citizenship and passport laws.
    - Non- governmental organization laws.
- Other offences under the prevailing laws of Nepal.

D) Miscellaneous grounds for suspicion

- If it is evident that any one is earning wealth (including cash) by evading tax, custom duty, land revenue, electricity bill, and water bill, phone bill and any other revenue or government fees.
- If anyone lives unusual lifestyle compared to his/her economic strength, profession/business.
- If unreasonable economic growth or economic strength is evident.
- If any act or transaction is not found reasonable or is found to have been conducted

with irrelevant party or where the transaction has no justifiable purpose.

- If reporting institution suspects any transaction relating to the customer against whom the regulatory authorities including Nepal Rastra Bank, Insurance Board, Securities Board, Stock Exchange, Company Registrar, Registrar of Cooperative, Bar Council, Institute of Chartered Accountant of Nepal, etc., have initiated proceedings.
- The transaction of the customer, where it is known or is evident that any investigation or proceeding has been or is being taken by competent law enforcement agency or regulatory institution of foreign state.
- If it is evident that the asset is earned from any offence against or abuse of children, women or destitute or any other individual.
- If it is evident that the asset is earned from extortion, coercive donation collection or from any forcible means to compel one to pay amount or asset.
- If it is evident that the asset is earned from offence of smuggling, illegal profession, trade and business, theft, bribery, robbery, piracy, illegal production, misuse or illegal transportation of goods.
- If transaction seems to be reported based on the news or commentary published in national or international news media about any individual or organization.
- If it is evident that the transaction is related to any person who is involved in suspicious transaction, likely to promote money laundering, terrorist or any other criminal activities or the transaction that appears to be unnatural or suspicious in any manner.
- If same address or telephone number/mobile number is provided for different unrelated customers.
- If the transaction conducted by customer comes under suspicion on the basis of the ground provided by regulator or concerned authority
- If any customer shows unnecessary interest in suspicious transaction or makes unnecessary and unnatural queries about the internal management of such transaction.
- If there is cross transaction between customers who are not related with each other or any individual transmits or receives amount from unrelated person or business institution's account.
- If there is suspicion that any transaction is aiding criminal activities or receiving amount from such activities.
- If cash is handled with unnatural binding or packaging during transaction.
- If multiple transactions are conducted with the people living in the country where AML/CFT regime is poor with no apparent reason.
- If anyone tries to complete transaction by paying more without any reason.
- If there are multiple claims for the amount received from one person.
- If anyone denies providing identity information or clear justification of the transfer

though there are sufficient grounds to know such information.

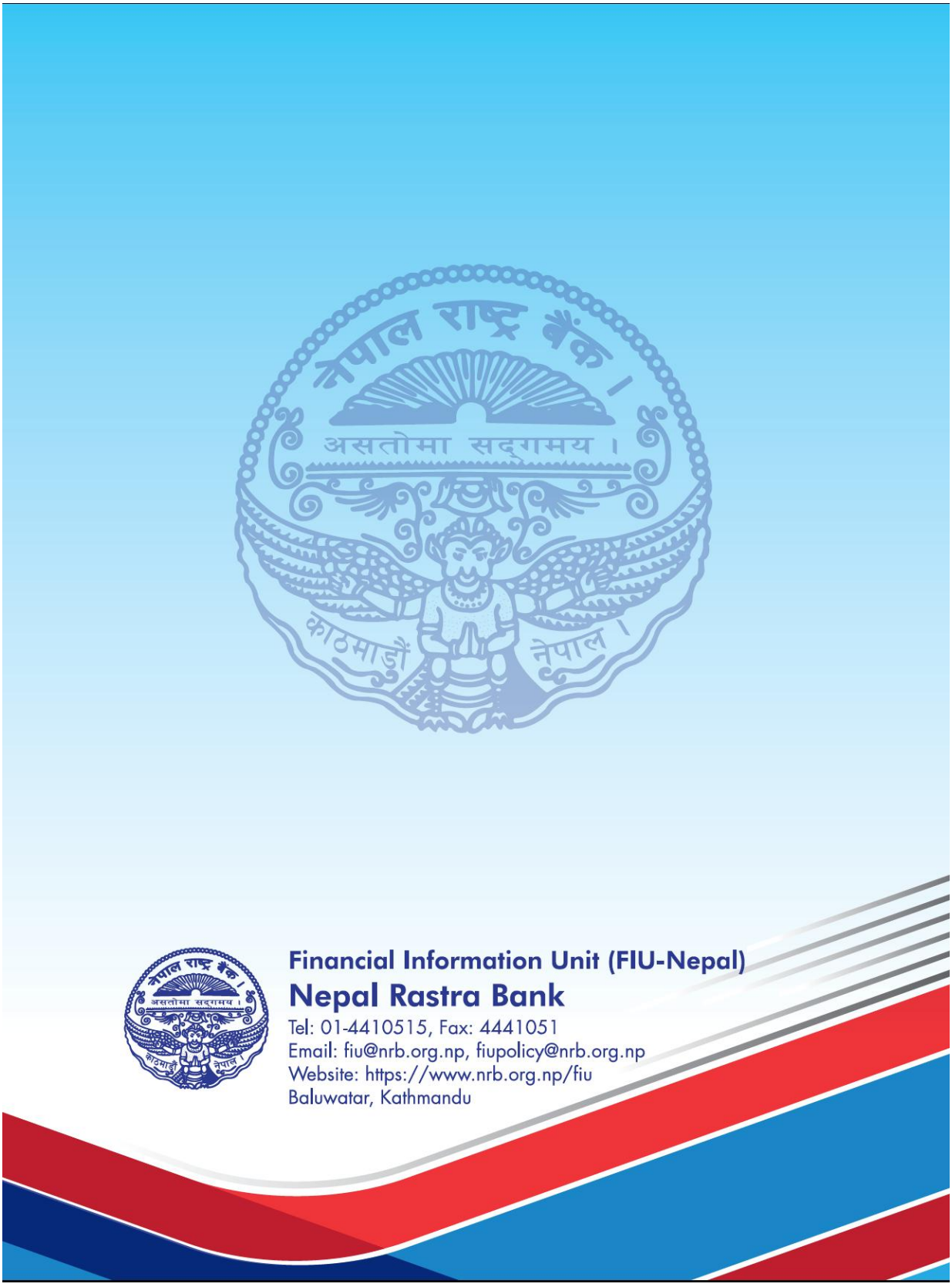
- Any other transaction the reporting institution finds the grounds for suspicious transaction reporting as per the prevailing law.

Note:

- *REs reporting through goAML software should submit the report as per the goAML Schema and Operational Guideline, 2020 issued by FIU-Nepal.*
- *REs should submit the reports as per the AML/CFT directives issued by their respective regulators. Those RE for which the regulator has not issued any AML/CFT directives need to submit the report as per this guideline.*

Disclaimer

This guideline cannot be relied on as evidence of complying with the requirements of the AML/CFT Act. The guideline is intended solely as an aid, and must not be applied as a routine instrument in place of common sense.


Financial Information Unit (FIU-Nepal)
Nepal Rastra Bank
Tel: 01-4410515, Fax: 4441051
Email: fiu@nrb.org.np, fiupolicy@nrb.org.np
Website: https://www.nrb.org.np/fiu
Baluwatar, Kathmandu