Suspicious Transaction Reporting
&
Suspicious Activity Reporting
(STR/SAR)
Guidelines

NEPAL RASTRA BANK

FINANCIAL INFORMATION UNIT, NEPAL

(FIU-Nepal)

Updated July, 2021

Acronyms/Abbreviations

ALPA	Asset (Money) Laundering Prevention Act, 2008 *(with amendments)*
AML/CFT	Anti Money Laundering and Combating the Financing of Terrorism
APG	Asia/Pacific Group on Money Laundering
BFIs	Bank and Financial Institutions
CDD	Customer Due Diligence
CIT	Citizen Investment Trust
DNFBPs	Designated Non-Financial Businesses and Professions
EDD	Enhanced Due Diligence
EPF	Employees Provident Fund
FMCG	Fast Moving Consumer Goods
FATF	Financial Action Task Force
FIU-Nepal	Financial Information Unit, Nepal
FSRB	FATF Style Regional Body
KYC	Know Your Customer
LEAs	Law Enforcement Agencies
ML/TF	Money Laundering and Terrorist Financing
MVTSPs	Money Value Transfer Service Providers
NRA	National Risk Assessment
PSOs	Payment System Operators
PSPs	Payment System Providers
REs	Reporting Entities
STR	Suspicious Transaction Reporting
SA / SAR	Suspicious Activity / Suspicious Activity Reporting
TTRs	Threshold Transaction Reports

Table of Contents

Disclaimer

This guidance note is a summary of best practices to be adopted by the REs when dealing with the execution and/or review of client's transactions/activities and the assessment of suspicion. It is intended solely as an aid and requires constant updating. It requires frequent adaptation to changing circumstances and new methods of laundering money from time to time. It is not an exhaustive list of steps.

This guideline cannot be evidence of complying with the requirements of the AML/CFT Act.

1. INTRODUCTION

This guideline has been issued as per power conferred under Section 10 (1) (h) of ALPA, 2008 (with amendment) for all the reporting entities to clarify the obligation to report suspicious transactions and suspicious activities.

It aims to generate knowledge on indicators of suspicious transactions/activities and inform REs about the technical requirements to report suspicious transactions to FIU-Nepal. There are different indicators to detect suspicious transactions in order to make the detection and filing of STRs/SARs expedient for the purpose of preventing money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

1.1 International Standards

A number of international AML/CFT standards are relevant. Key AML/CFT standards include but are not limited to:

- UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances – Vienna Convention – 1988;
- UN Convention Against Transnational Organized Crime - Palermo Convention – 2000;
- UN Convention Against Corruption - UNCAC – 2005;
- **Financial Action Task Force (FATF) Recommendations -2012** - (Updated October 2020):

  - The FATF assesses countries against a set of recommendations (the 40 Recommendations) that represent best practices for AML/CFT systems. The Asia Pacific Group (APG) deals with Anti Money Laundering and Combating the Financing of Terrorism and is a FATF Style Regional Body (FSRB). FSRB's perform a similar function as the FATF on a regional basis. Nepal is a member of the APG and is subject to the assessment of its AML/CFT framework by the APG.

  - As per The FATF Recommendations R20 on Reporting of suspicious transactions, 'If a financial institution suspects or has **reasonable grounds** to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU)'.

  - As per FATF Methodology - 2013, Financial institutions should be required to report all suspicious transactions, including attempted transactions, regardless of the amount of the transaction.

1.2 Domestic Legislation

Key AML/CFT Laws and Regulations in Nepal that need to be complied with:

- Asset (Money) Laundering Prevention Act (ALPA), 2008
- The Prevention of Corruption Act, 2002
- Criminal Assets and Resources (Prevention, Control and Seizure) Act, 2070
- Mutual Legal Assistance Act, 2070
- Organized Crime Prevention Act, 2070
- Assets (Money) Laundering Prevention Rules, 2016
- Mutual Legal Aid Rules, 2070
- Prevention of Money Laundering (confiscation of assets or funds of listed Persons, group or organization) Rules, 2070
- Criminal Assets and Resources (Prevention, Control and Seizure) Rules, 2077
- AML/CFT related directives and circulars issued by respective regulators
- Other relevant laws and regulations

1.3 National Risk Assessment 2020

The REs should obtain a comprehensive approach in recognizing and reporting STRs/SARs to FIU-Nepal as per national threats identified and rated by Nepal National Risk Assessment Report 2020, as below:

- **Major:** The offences found as the major threats include Corruption, Tax Evasion, Financial crimes such as Banking Offence and *Hundi*.
- **Issues of Concern:** The offences found as the threats of concern includes Drug trafficking, Organized Crime, Extortion, Arms-related Offence, Domestic Terrorism, Fraud, Environmental Crime, Robbery (Theft), Smuggling (including black marketing) and Forgery.
- **Low:** The low threat posing offences includes Counterfeiting and Piracy of Products, Kidnapping, Illegal Restraint and Hostage Taking, International Terrorism, Trafficking in Stolen Goods, Insider Trading and Market Manipulation.

1.4 Objectives

The objective of this guideline is to assist reporting entities in:

a) Identifying suspicious transactions and activities by providing indicators of suspicion
b) Improving the quality of Suspicious Transaction Reports (STRs)
c) Adopting Risk Based Approach in assessing the quality of AML risk in order to identify, measure and consider four main risk measures i.e. delivery channel risks, geographical risks, products and services risks and customers' risks.
d) 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 may not be aware 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 offence may arise.

1.5 Predicate Offence

Reporting of STR/SAR should provide a reference to the 'Predicate offence' listed in the ALPA 2008, Section 2(Y). As per the Annexure under Section 2(Y) "Predicate offence" means

(1) Any below mentioned offence under the prevailing laws:

a) Participation in an organized criminal group and racketeering,
b) Disruptive (terrorist) act and terrorism,
c) Trafficking in human being and migrant smuggling in any form,
d) Any kinds of sexual exploitation including the children,
e) Illicit trafficking in narcotic drugs and psychotropic substances,
f) Illicit trafficking in arms and ammunition,
g) Illicit trafficking in stolen and other goods,
h) Corruption and bribery,

i) Fraud,
j) Forgery,
k) Counterfeiting of coin and currency,
l) Counterfeiting and piracy of products, or imitation, illegal copy or theft of products,
m) Environmental crime,
n) Murder, grievous bodily injury,
o) Kidnapping, illegal restraint or hostage-taking,
p) Theft or rubbery,
q) Smuggling (including custom, excise and revenue),
r) Tax (including direct and indirect),
s) Extortion,
t) Piracy,
u) Insider Dealing and Market Manipulation in securities and commodities,
v) Ancient monument conservation,
w) Forest, National park and wild animals,
x) Money, banking, finance, foreign exchange, negotiable instruments, insurance, cooperatives,
y) Black marketing, consumer protection, competition, supply,
z) Election,
aa) Communication, broadcasting, advertising,
bb) Transportation, education, health, medicine, foreign employment,
cc) Firm, partnership, company, association,
dd) Real estate and property,
ee) Lottery, gambling, donation,
ff) Citizenship, immigration and passport.

(2) Offence of terrorist financing pursuant to section 4,

(3) Any other offence as designated by the Government of Nepal by publishing a notice in the Nepal Gazette, or

(4) An offence under a law of a foreign State, in relation to act or omission under paragraph (1), (2) or (3), which had they occurred in Nepal, would have constituted an

offence.

Note: *While reporting STR/SAR, if any particular offence(s) cannot be linked or if source is not clear, then report should mention 'Money Laundering' as an offence.*

1.6 Suspicious Transaction Reporting (STR)

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

a) If it suspects or has **reasonable grounds** to suspect that if the property is related to ML/TF or other offence, or

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

Suspicious Transactions Reports (STRs) include detailed information about transactions that are suspected violations of law or appear to be suspicious/ doubtful or arouse suspicion. The goal of STR filing is to help FIU-Nepal to identify individuals, groups and organizations involved in predicate offences declared 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.

1.7 Suspicious Activity Reporting (SAR)

As per Section 7(S)(2) of ALPA 2008, Reporting entity shall also submit the report of attempted transactions or activity to FIU as mentioned under sub-section (1).

Suspicious Activity (SA) arises from suspicion relating to general behavior of the person in question which creates the knowledge or belief that he or she may be involved in illegal activities out of which proceeds might be generated. Any suspicious attempted transaction also falls in this category. For example:

- 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.

- Activities related to Identity Theft.

- Information on Fake Bank Statement issued by any organization.

2. WHO MUST REPORT?

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

3. REPORTING ENTITIES

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 below:

S.N.	Institutions	Name of Regulators
a) <u>Financial Institutions:</u>		
1.	Bank and Financial Institutions	Nepal Rastra Bank
2.	Money Remitters	Nepal Rastra Bank
3.	Money Changers	Nepal Rastra Bank
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
b) <u>Designated Non-Financial Businesses and Professions (DNFBPs'):</u>		
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 regulators for reporting entities under their jurisdictions.

4. WHAT TO REPORT?

STR/SAR submitted to FIU-Nepal must contain following details. Similarly, SAR should contain as much details as possible.

- Summary of suspicious activities along with updated CDD information
- Analysis or Examination
- Possible Linkage

- Suspected Beneficiary
- Related account statement
- Mandatory details (as required by regulators)
- Correct identifications
- Other details or supporting documents.

Sometimes LEAs seek for information from REs. In such instances, REs are not required to send such information to the FIU. Further, REs are encouraged to add value to the information by searching and adding web materials along with its sources.

STR should be reported to FIU-Nepal along with the below mentioned supporting documents:

4.1 In case of Person

- Account Opening Form
- Updated KYC related documents (with relationship details)
- Account Statement (for STRs)
- Summary suspicious transaction identified
- Media news/reports and other relevant documents if any.

4.2 In case of Entity

- Account Opening Form
- Registration Certificate
- PAN/VAT Certificate
- Updated KYC related documents of Entity and its Director(s) and Signatory(ies)
- Account Statement (if available)
- Information related to Holding Company, Subsidiary and Associates or Other Business entities within the Group
- Summary of suspicious transaction identified
- Media news/reports and other relevant documents if any.

5. REPORTING GUIDANCE

a) STR/SAR should be reported to the FIU-Nepal **electronically through goAML web reporting system by BFIs, Insurance sector, Securities dealers (Brokers) and assigned REs where as other REs through signed paper reports**. FIU-Nepal has adopted phase-wise implementation plan for the effective and successful implementation of goAML system for numerous groups of REs.

b) Reporting through goAML software should be as per:

i.) Reporting TTR and STR in goAML Operational Guideline for REs

ii.) Standard XML Reporting Instructions and Specifications

iii.) goAML Web Reporting Guideline, issued by FIU-Nepal.

c) The REs should properly understand the business logic behind any transaction and provide all the necessary and available information while reporting in goAML.

d) REs should provide their reports of suspicious transactions/activities to the FIU-Nepal through their Compliance Officer. Clear internal reporting procedures should be in place and all employees must follow the reporting procedures.

e) STR/SAR should be reported to the FIU-Nepal as soon as practicable but no later than three working days after REs have taken **reasonable measures** that enable them to establish that there are **grounds to suspect** that the transaction or attempted transaction is related to the commission of a money laundering offence or a terrorist activity financing offence.

f) If the reporting entity discovers additional facts and circumstances to either support or refute the reporting entity's initial suspicion after sending the report, REs should then inform the FIU-Nepal appropriately.

6. 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.

7. CONTENTS OF REPORTING

7.1 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.

7.2 Updated

ALPA, 2008 requires customer information should be updated when there is any suspicion. CDD and EDD (in case of high risk transactions) should be completed and updated by REs before reporting to FIU-Nepal.

7.3 Quality

The quality of a STR/SAR 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. Therefore, the relevant information should include:

- Full details of the customer and complete statement as far as possible of the information giving rise to knowledge, suspicion or **reasonable grounds for suspicion** of money laundering and terrorist financing or both;
- If a particular type of criminal conduct is suspected, a statement of this conduct;
- Where a financial business has additional relevant evidence that could be made available, the nature of this evidence;
- Any statistical information as the FIU-Nepal may require.

It is pertinent that person preparing the report have all relevant information at hand so that a clearer picture can be drawn. This is more so for the descriptive aspect of the report or the narrative.

7.4 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 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?
- Which **Predicate Offence**?
- What transactions, attempted transactions, behaviors, facts, beliefs and circumstances are involved and relevant to the suspicion?
- Who are the natural and legal persons involved? What are the relationships details?

- 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 assets are 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.

7.5 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.

8. INDICATORS OF SUSPICIOUS ACTIVITIES / TRANSACTIONS (RED FLAGS)

A transaction may have certain 'red flags' or indicators of STR/SAR. It is important that reporting entity staff can recognize indicators, especially indicators relevant to your 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.

In order to make the detection of STRs/SARs 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 indicators,
2) Sector-specific indicators and
3) Indicators related to laws.

These indicators are offered as a guide and are 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.

8.1 General Indicators

8.1.1 Economically Irrational transactions

a) Transactions having no conformity with the initial purpose of account opening.
b) Transactions having no relationship with the business of the customer.
c) If customer conducts complex, unusual large transactions and unusual pattern of transactions or which have no apparent economic or visible lawful purpose.
d) Transaction amount and frequency are different from that of normally conducted by the customer.
e) There are attempts to disguise the real owner or parties to the transaction.

f) 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.

g) If customer fails to provide reasonable justification for the transaction.

h) If any suspicious pattern emerges from customer's transactions.

i) The intensity of transactions for an inactive trading account suddenly increases without plausible reason.

j) Frequent selling of securities at significant losses.

8.1.2 Use of third party

a) Multiple deposits made to an account by non-account holders.

b) Unrelated parties sending fund transfers or other forms of electronic transfers to the same beneficiary with no apparent relation to the recipient.

c) If a client conducts transaction while accompanied, overseen or directed by another party.

d) If a client makes numerous outgoing payments to unrelated parties shortly after they receive incoming funds.

e) Wire transfers, deposits or payments to or from unrelated parties (foreign or domestic).

f) If a client appears or states to be acting on behalf of another party.

g) Account is linked to seemingly unconnected parties.

h) Unrelated third person is repeatedly depositing/withdrawing as a conductor in particular account.

i) Account holder's profession is non-income generating such as housewife, student, unemployed etc. but transaction amount is relatively high.

j) Involvement of third parties funding without apparent connection or legitimate explanation.

k) If unknown third party frequently transfer funds into customer's account.

l) If unrelated third party is unnaturally, unnecessarily involved or is more active in transaction.

m) Nominee third party.

n) Simultaneous transfer of funds to a group of customers' accounts from a third party.

8.1.3 Behaviors of the Customer

a) Frequent changes to the address, telephone/mobile no. or authorized signatories.
b) Customer/Client's address is a virtual office.
c) Unreasonable behaviors of the relevant customer when conducting a transaction (nervous, rushed, unconfident, etc.).
d) Customer with significant Money Laundering, Terrorist Financing and Proliferation Financing related adverse news or other indicators relating to financial crime.
e) If customer shows unusual curiosity about internal system, control and reporting.
f) If customer admits or makes statements about involvement in criminal activities.
g) If customer offers money, gratuities or unusual favors for the provision of services that appear unusual or suspicious.
h) If customer/prospective customer gives doubtful or false information with respect to his/her identity, sources of income or businesses.
i) 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.
j) 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.
k) If customer opens the account for a short period and closes without a valid reason.
l) If customer is unwilling to provide right information or immediately terminating business relationship or closing his/her account at the time of enquiry by reporting entity with respect to his/her transaction.
m) Simple signature.

8.1.4 Cash

a) Transactions conducted in a relatively small amount but with high frequency (structuring).
b) Transactions conducted by using several different individual names for the interest of a particular person (Smurfing).
c) If customer conducts series of transactions or book-keeping tricks for concealing the source of fund (layering).

d) 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.
e) 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.
f) If person sending money cannot provide even general information about the recipient of money.
g) If any person brings huge cash for deposits which appears to be soiled and dusty or have unusual odor.
h) If cash is handled with unnatural binding or packaging during transaction.

8.1.5 Wire/Fund transfer activities

a) If customer fails to provide adequate information about the originator, beneficiary, and purpose of the wire transfer.
b) If customer orders wire transfers in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
c) If the pattern of wire transfers shows unusual patterns or has no apparent purpose.
d) If customer receives frequent fund transfers from individuals or entities who have no account relationship with the person/institution.
e) Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
f) If several customers request transfers either on the same day or over a period of two to three days to the same recipient.
g) If beneficiaries of wire transfers involve a large group of nationals of countries associated with terrorist activities.
h) 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.
i) Fund transfers to and from high-risk offshore financial centers without any clear business purpose.
j) Receipts of fund transfer in several phases and once accumulated the funds are

subsequently transferred entirely to other account.

k) Receipts/payments of funds made by using more than one account, either in the same name or different names.

l) Fund transfers using the account of reporting entities' employee in an unusual amount.

m) If multiple inward or outward remittance transaction is conducted with the person from the country or region where terrorist organizations operate.

n) Customer shows unusual interests in wire transfer ceiling and availability of alternative or informal channels.

o) Wire transfer from foreign country is followed by multiple transfers to other domestic accounts.

p) High frequency and high volume of wire transfers, which does not match with declaration made by customer.

8.1.6 Money Laundering involving employees and agents of REs

a) Changes in employee characteristics, (e.g. lavish lifestyles or avoiding taking holidays).

b) Changes in employee or agent performance.

c) 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.

8.1.7 Corporate and business transactions

a) 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.

b) If the transaction is not economically justified considering the account holder's business or profession.

c) If customer makes a large volume of cash deposits from a business that is not normally cash-intensive.

d) If customer does not want to provide complete customer due diligence information of their business.

e) If the financial statements of the business differ noticeably from those of similar

businesses without valid reasons.

f) If size of wire/fund transfers is inconsistent with normal business practice/transactions for the customer.
g) If unexplained transactions are repeated between personal and business accounts.
h) 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.)
i) Structuring transactions to evade substantial shareholding.
j) Existing company struggling with cash-flow problem suddenly find silent investor/partner steering into high level of transactions.
k) Same person as a shareholder/owner of two or more companies/entities and there exists high frequency of huge transfer to and from accounts of these companies/entities without any valid reason.
l) Sales turnover reflected in bank statement is reasonably different from that of audited report.
m) Repeated cash transactions just below TTR limit, just to avoid reporting.
n) Business is not fully operational due to various reasons but there is equal or more bank transactions without valid reasons.

8.1.8 Lending

a) 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.
b) If customer suddenly repays a problematic loan unexpectedly without a valid reason.
c) If customer repays a long term loan, such as a mortgage, within a relatively short time period.
d) If the source of down payment is inconsistent with borrower's financial ability, profession and business as per the declaration.
e) If customer shows income from foreign sources on loan application without providing further details.
f) If customer seems unconcerned with terms of credit or costs associated with

completion of a loan transaction.

g) 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).

8.1.9 Trade Based Money Laundering

a) Submitting the fake documents and false reporting by the customer such as commodity misclassification, commodity over- or under-valuation etc.

b) If the transaction involves the use of repeatedly amended or frequently extended letters of credit without reasonable justification.

c) Phantom shipping – If no goods are shipped and all documentation is completely falsified to move funds in the guise of trade.

d) Payments to the vendor by unrelated third party.

e) If the customer trades commodities that do not match the nature of business of the customer.

f) If the commodity is shipped to (or from) a jurisdiction designated as "high risk" for money laundering activities.

g) In case of Double-invoicing.

h) If there are significant discrepancies between the descriptions of the goods on the transport documents, the invoice, or other related documents.

i) 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.

j) Re-cycling of previous documentation with few or no edits during financing through documentary collections.

k) Misuse of food supply chains involving highly perishable items such as fresh fruits, vegetables, flowers, FMCG & Dairy products (low value, high volume products)

l) Exploiting legitimate supply chains involving third party for invoice settlement, continued occurrence of third-party intermediaries in financial settlement process.

m) Development of new supply chain and financial intermediaries as there was no pre-existing commodity supply chain to exploit.

n) Supply Chains moving low value goods frequently (Cosmetics, medicines, spurious/fake goods).
o) Unnecessary complicated and complex supply chains involving multiple shipments.
p) The extreme price variability, wrongly described prices in supply of goods.
q) Portable or handheld electronics business, construction materials, plant machinery, scrap metal dealers, fuel and energy products, alcoholic and soft drink business (mischaracterizing goods to circumvent controls and other custom and tax violations).
r) Importer routinely depositing cash in advance using open account for business transactions.
s) Shipping of products of no value as a saleable good.
t) Previously established business unexpectedly pivots into entirely unrelated sector.
u) Fraudulent trade circuits- Exporters claim duty drawback on inflated export bills or non-existent imports.
v) Misuse and exploitation of relaxations in laws and import restrictions for import of necessary medical equipment and medicines.
w) New cash-intensive and highly-liquid lines of business.
x) Trade in goods with extended trade cycles - Unusual shipping routes or transshipment points.
y) Trade in services and other intangibles to disguise and justify the movement of illicit proceeds.
z) Goods which are difficult for authorities to examine as well as having dual usages e.g. hazardous, chemicals, poisonous, inflammable, etc.

8.1.10 Money Service Businesses (including currency exchange, money transfers, remittances, PSPs and PSOs)

a) The use of numerous agent locations for no apparent reason to conduct transactions.
b) Multiple low-value international funds transfers, possibly indicating a large amount of funds broken down into smaller amounts.
c) Several Customers request transfers either on the same day or over a period of two to three days to the same recipient.

d) Customer does not appear to know the recipient to whom he or she is sending the transfer.
e) 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.
f) Customer exchanges currency and requests the largest possible denomination bills in a foreign currency.
g) Customer knows little about address and contact details for payee, is reluctant to disclose this information, or requests a bearer instrument.
h) Customer instructs that funds are to be picked up by a third party on behalf of the payee.
i) Customer requests that a large amount of foreign currency be exchanged to another foreign currency.
j) Large amounts of currency exchanged for traveler's checks.
k) Customer exchange small denomination of bills for larger denominations.
l) 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
m) Frequent international wire transfers from bank accounts which appear inconsistent with stated business activities.
n) Frequent deposits by multiple individuals into a single bank account, followed by international wire transfers and /or international withdrawals through ATMs.
o) Sudden change in pattern of financial transactions from low value international fund transfers to large value transfers by a money remitter.
p) Amount frequently getting credited in account through wire transfer of a person returned from foreign employment.
q) Money transfer business persons running other businesses as well.
r) MVTSPs communicating only limited information on customer & Beneficiary in Individual transactions. Information just sufficient to ensure that delivery is made to right person in an effective manner.

s) Unusual transactions to a Digital Wallet account from various wallet accounts.
t) Online platform used for payment of trading transactions like PayPal balance, Bitcoin, etc.

8.1.11 Trust or Company Service providers (TCSP)

a) Creation of complicated structures where there is no legitimate economic reason.
b) Use of an intermediary without a legitimate reason.
c) Funds received from high risk jurisdictions.
d) Customers use directors /shareholders as nominee.

8.1.12 Accountants and Lawyers

a) Use of an agent or intermediary without obvious reason.
b) Customer's business account particularly shows large cash deposits without a valid reason.
c) Funds are received from a foreign jurisdiction, particularly, where there is no connection between the jurisdiction and the customer.
d) Overseas instruction from a customer for no economic reason.
e) Customer is not concerned about the level of fees/charges.
f) Customer appears to have access to cash substantially above their means.
g) Use of many different firms of auditors and advisers for connected companies and businesses
h) Client has a history of changing bookkeepers or accountants yearly.
i) Company shareholder loans are not consistent with business activity.
j) Company makes large payments to subsidiaries or other entities within the group that do not appear within normal course of business.
k) Client is willing to pay fees without the requirement for legal work to be undertaken.
l) Significant amount of private funding/cash from an individual who was running a cash intensive business.
m) Client provides false or counterfeited documentation

n) Large financial transactions requested by recently set up companies, not justified by the activity of the client.

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

a) 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.
b) Raising donations in an unofficial or unregistered manner (and its ultimate use is also not clear).
c) If client is linked to the terrorist activities or proliferation financing, etc.
d) 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.
e) Transactions involve individuals or entities identified by media and/or sanctions lists as being linked to a terrorist organization or terrorist activities.
f) Law enforcement information provided which indicates individuals or entities may be linked to a terrorist organization or terrorist activities.
g) 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.
h) Individual or entity's online presence supports violent extremism or radicalization.
i) Client donates to a cause that is subject to derogatory information that is publicly available (e.g. crowd funding initiative, charity, non-profit organization, non-government organization, etc.)
j) 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.

k) If the customer is linked to illicit trafficking of arms and ammunition, nuclear chemical, biological weapons and related materials and their means of delivery.

l) If it is evident that the asset is earned from the offence relating to arms and ammunition under the prevailing law.

8.1.14 Miscellaneous grounds for suspicion

a) Customer/Client is linked to adverse media news (national or international).

b) 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.

c) 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.

d) If anyone lives unusual lifestyle compared to his/her economic strength, profession/business.

e) 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.

f) 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, Department of Co-operatives, Bar Council, Institute of Chartered Accountant of Nepal, etc., have initiated proceedings.

g) 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.

h) If it is evident that the asset is earned from any offence against or abuse of children, women or destitute or any other individual.

i) 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.

j) If the transaction conducted by customer comes under suspicion on the basis of the ground provided by regulator or concerned authority

k) If any customer shows unnecessary interest in suspicious transaction or makes unnecessary and unnatural queries about the internal management of such transaction.

l) 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.

m) If there is suspicion that any transaction is aiding criminal activities or receiving amount from such activities.

n) If multiple transactions are conducted with the people living in the country where AML/CFT regime is poor with no apparent reason.

o) If anyone tries to complete transaction by paying more without any reason.

p) If there are multiple claims for the amount received from one person.

q) If anyone denies providing identity information or clear justification of the transfer though there are sufficient grounds to know such information.

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

s) Customer conducts several transactions just below reporting thresholds.

t) Non-refundable tourism packages.

u) Triangular and prolonged settlement of transactions.

8.2 Sector- Specific Indicators:

Sector-specific indicators are not exhaustive lists of indicators and it should be read in conjunction with general indicators.

8.2.1 Bank and Financial Institutions

a) If customer attempt to open or operate accounts under an identity that does not appear genuine.

b) 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.

c) 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.

d) If transaction involves a country known for highly secretive banking and corporate law.

e) Opening accounts when the customer's address or employment addresses are outside the local service area without a reasonable explanation.

f) There is a sudden change in customer's financial profile, pattern of activity or transactions.

g) Customer uses notes, monetary instruments, or products and/or services that are unusual for such a customer.

h) If there is suspicion on the transaction of the customer who is blacklisted by Credit Information Bureau or the REs itself has placed the concerned customer in a high-risk customer category.

i) If customer is suspected for using of personal account for business or other purposes, or vice-versa.

j) 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.

k) 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.

l) 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.

m) 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.

n) If customer has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.

o) 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.

p) If account has close connections with other business accounts without any apparent reason for the connection.

q) If deposits to or withdrawals from a corporate account are primarily in cash.

r) If customer requests movement of funds that are uneconomical without any valid justification.

s) If customer visits the locker (safety deposit box) area immediately before making cash deposits.

t) If customer repeatedly conducts large foreign exchange transactions without valid justification.

u) Regular return of cheques for insufficient funds.

v) If customer is found to have used/made or involved with counterfeit coin and currency.

w) Frequent deposits of third-party cheques or IPS transfer into business or personal accounts.

x) Large amount/frequency of transactions in salary saving accounts, student saving accounts, housewife saving accounts etc. and significantly different from initial declaration by the customer without valid sources or justification.

y) Repeated behavior of withdrawal from own individual account and deposit in multiple accounts without valid reasons.

z) 'U-turn' transaction: Fund receives from person/company in a foreign country are immediately remitted to another person/country in the same country.

8.2.2 Securities Market

a) 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.

b) 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.

c) Trading between numerous accounts controlled by/from the same people or IP

address.

d) 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.

e) 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.

f) Purchase of securities by cash, transfer, or cheques under other person's name/third party.

g) If customer 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.

h) Transaction with the client sanctioned by APG/FATF/United Nations or other Inter-government international organizations.

i) If transaction patterns resemble a form of market manipulation, for example, insider trading and pump and dump.

j) Two or more accounts are involved for selling and purchase pattern in order to increase or decrease the price in unusual manner.

k) Large amount of wire transfer is used for securities purchase as foreign indirect investment, especially from high-risk countries.

l) Customer is reluctant to provide further information for CDD.

m) Customer's address is associated with multiple other unrelated accounts.

A) Insider Trading:

Insider trading involves situations where the person who buys and sells securities, whether a company insider or not, does so in violation of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about the security. As a predicate offence for money laundering, and an offence in its own right, this type of misconduct is reportable on STRs. The

illicit assets generated by insider trading can be laundered through the security sector. The suspicious indicators for Insider Trading are: -

i) If client (a director, employee or a person, who can obtain any information or a notice in the capacity of a shareholder of that body corporate or person who can obtain any information or a notice in the capacity of a professional service provider to that body corporate) conducts suspicious activities and makes a large purchase or sale of a security, shortly before news is issued that affects the price of the security.
ii) The client is known to have friends or family who work at or for the securities issuer.
iii) The client sells his or her position in a security in conjunction with a significant announcement about the security.

B) 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: -

i) The client engages in large or repeated trading in securities that are illiquid, low priced or difficult to price.
ii) The officers or insiders of the issuing company have a history of regulatory violations.
iii) The issuing company has failed to make required regulatory disclosures.
iv) If security price is artificially raised ("pumped"); the security is then sold ("dumped") for profit.

8.2.3 Insurance Sector

a) If client purchases products which are inconsistent with the buyer's age, income, profession or financial history.

b) 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.
c) If client shows more interest in the cancellation or surrender than in the long-term results of investment.
d) If client is known to purchase several insurance products and uses the proceeds from an early policy surrender to purchase other financial assets.
e) Insurance surrender having high value insurance premium.
f) If client purchases an annuity with a lump sum rather than paying regular premiums over a period of time.
g) If client funds the policy using payments from a third party.
h) If client purchases several policies just under the threshold limit, instead of purchasing one large policy.
i) If client terminates product, especially at a loss, or where cash was tendered and/or the refund cheque is to a third party.
j) If client purchases various policies and cancels regularly.
k) If client makes overpayment of premiums with a request for a refund of the amount overpaid.
l) 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.
m) If client is found to have involvement in establishment of bogus reinsurers/ insurers to launder the proceeds of crime.
n) Repeated behavior of surrender of existing policy and subscription of new policies of same or different life insurance companies.
o) High frequency of insurance subscription and immediate avail of loan from it.
p) An unusual (a typical) incidence of pre-payment of insurance premium.
q) An insurance agent is reluctant to provide information for updating CDD.

8.2.4 Cooperatives

a) If customer attempt to open or operate accounts under a false name.

b) 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.

c) Opening accounts when the customer's address or employment addresses are outside the local service area without a reasonable explanation.

d) There is a sudden change in customer's financial profile, pattern of activity or transactions.

e) Customer uses notes, monetary instruments, or products and/or services that are unusual for such a customer.

f) 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.

g) If customer is suspected for using of personal account for business or other purposes, or vice-versa.

h) 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.

i) 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.

j) If customer has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.

k) In case of large cash withdrawals from a previously dormant/inactive account.

l) If account has close connections with other business accounts without any apparent reason for the connection.

m) If deposits to or withdrawals from a corporate account are primarily in cash.

n) If customer requests movement of funds that are uneconomical without any valid justification.

o) Regular return of cheques for insufficient funds.

p) If customer is found to have used/made or involved with counterfeit coin and currency.

q) Large amount/frequency of transactions in individual saving accounts and significantly different from initial declaration by the customer.

r) Repeated behavior of withdrawal from own individual account and deposit in multiple other accounts without valid reasons.

8.2.5 Real Estate

a) If there exists discrepancy between the income or occupation and wealth of the buyer and the property as per the declared source of income.

b) Transactions carried out on behalf of minors, incapacitated persons or other persons who appear to lack the economic capacity to make such purchases.

c) 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.

d) Manipulation of the appraisal or valuation of a property (undervaluation, overvaluation and successive sales at higher values).

e) 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).

f) 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.

g) If the purchaser is a company with complicated beneficial ownership.

h) 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.

i) Transactions in which the party asks for the payment to be divided into smaller parts with a short interval between them.

j) Immediate resale of the property, especially when the resale price is dramatically higher without explanation compared to purchase price.

k) Purchaser worries about threshold reporting or request not to report.

8.2.6 Non Profit Organizations (NGOs/INGOs) and Trust

a) Obscure beneficial ownership.
b) 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.
c) 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.
d) If the account of NGO/INGOs receives foreign funds without the knowledge of its regulator (Social Welfare Council).
e) The use of funds by a non-profit organization is not consistent with the purpose for which it was established.
f) If the funds for the organizational use comes in the name of individuals instead of the organization's account.
g) If the organization has operations or funds from, or transactions to, high-risk jurisdictions.
h) If the account shows signs of unexplained increase in deposits and transaction activities.
i) 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.
j) If the organization raises donations in an unofficial or unregistered manner.
k) If the organization plans or commits act of terrorism, which may include the use of weapons of mass destruction and fosters extremism.
l) If the organization has the donors from the countries identified as lacking appropriate anti-money laundering or counter terrorist financing regulation.
m) If the act of donor, beneficiaries or partner is found to be suspicious with the suspect of Money laundering or Terrorist financing.
n) If the organization or its representatives are linked to third parties that support or are engaged in terrorist activity or procure dual-use equipments.

o) If the bank accounts of the organization are used by entity/person whose own accounts are under restrictions.

p) If the organization merges with another organization believed to support terrorist activities.

q) Withdrawal from NPO account and then deposit in personal account, then channels to persons'/organizations' accounts.

r) Lack of proper information regarding donors of foreign countries, especially of high-risk ones.

s) Seemingly misuse and misappropriation of domestic and international financial aid and emergency funding.

t) Previously inactive trust account is now used intensively, unless there is a plausible reason for such use.

u) Unconvincing or unclear purpose or motivation for having trusts established in Nepal.

8.2.7 Approved Retirement Funds (including EPF, CIT)

a) Large cash sums deposited in retirement fund by members, particularly when followed by substantial withdrawals of funds without a valid reason.

b) 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.

c) If unrelated third party pays contributions on behalf of a member of the retirement fund.

d) Funds or other assets deposited into a retirement fund which are inconsistent with the profile of the client.

e) Media reports of illegal activity.

f) High contribution in self employed or unemployed person's account by oneself or any third party.

g) Small or newly established organization with huge contributions to employees' provident funds or retirement policy.

h) There are significant inconsistencies in the deposit amount and timing without valid reasons.

8.2.8 Casinos

a) 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.
b) Activities inconsistent with the customer's profile.
c) Dramatic or rapid increase in size and frequency of transactions.
d) Client requests a winning cheque in a third party's name.
e) Noticeable changes in spending/betting pattern.
f) Inconsistent identity information presented or refusal to provide required identification.
g) Client request cheques that are not for gaming winnings. Purchase of chips in huge cash and then exchange it at last in cheque.
h) Customer's intention to win is absent or secondary.
i) Purchasing and cashing out casino chips with little or no gaming activity.
j) 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.
k) Client exchanges small denomination bank notes for large denomination bank notes.
l) If client is known to have used multiple names.
m) Any deviation in transactions or suspicious activities identified by casino business.
n) Funds withdrawn from account shortly after being deposited.
o) Lack of proper sources of deposited account.
p) Use of false identity to open and operate casino accounts.
q) Transactions in which PEPs and high net worth customers are linked.

8.2.9 Dealers in precious gems, stones and metal

a) Established customer dramatically increases purchase for no apparent reason.
b) If the origins of the precious stone, precious metal or precious product appear to be fictitious/suspicious.
c) The customer is unable or unwilling to provide information for due diligence and record keeping purposes.
d) 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.

e) The customer appears to be in a hurry to complete the transaction.
f) If customer requests for or conducts over/under-invoicing, structured, complex, or multiple invoice requests.
g) Large or frequent transactions that are in a foreign currency.
h) 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.
i) The customer is suspected to be using forged, fraudulent or false identity documents for due diligence and record keeping purposes.
j) The customer is unusually concerned with the Regulated Dealer's AML/CFT policies.

8.3 Indicators related to 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

9. COVID-19 IMPACT AND POTENTIAL ML/TF RISKS

It is uncertain how long the current situation will last, but we may be in this for the long haul and the impacts may be enduring. So REs will require long-term adjustments to working practices and culture and need to be proactive in assessing and addressing the new emerging risks and the changing priorities.

The potential ML/TF risks emerging from the COVID-19 impact and the emerging risks in the post-pandemic environment could be:

a) Criminals finding ways to bypass CDD measures by exploiting temporary challenges in internal controls caused by remote working situations, in order to conceal and launder funds;
b) Increased misuse of online financial services and virtual assets to move and conceal illicit funds;
c) Misuse and misappropriation of domestic and international financial aid and emergency funding by avoiding standard procurement procedures, resulting in increased corruption and consequent ML risks;
d) Exploitation of COVID-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business, both for the laundering of proceeds as

well as to fund their operations, as well as fraudulently claiming to be charities to raise funds online.

e) Frauds related to medical products (non-delivery of products, gouging and hoarding prices of products, sale of counterfeit goods, etc.), imposter scams (charities frauds, etc.), exploitation of money mule schemes while benefiting from the crisis conditions, cyber attacks targeting victims with Covid-19 lures, etc.

10. TIPPING OFF AND PENALTIES

As per section 44(A)(1) of ALPA, 2008, no reporting entity, nor its official or staff shall disclose to its customer or to any other person that a following report, document, record, notice or information concerning suspected money laundering or terrorist financing or predicate offence has been or is being submitted:

a) Report of suspicious or threshold transaction,
b) Report of ongoing monitoring order pursuant to section 19A,
c) Any document, record or information provided to the Financial Information Unit, investigation officer or investigation authority pursuant to prevailing laws or regulator,
d) Other details or information to be provided by reporting entity under this Act, rules and directives there under,
e) Individual introductory detail of an official or staff providing report, document, document, notice or information from clause (a) to (d)

As per section 44(A) (4) of ALPA, 2008, following authority may impose following sanction at each event of violation of the provision of section 44 (A) (1 to 3) as follows:

a) Regulator to fine up to one million rupees to the bank and financial institution or to casino,

b) Regulator to fine up to two hundred thousand rupees to other designated non-financial business and profession,

c) Reporting entity to take departmental action to its official or staff under their own laws,

d) Notwithstanding whatever written in the prevailing laws of service, concerned authority to take departmental action against the Chief, investigation officer or staff of the department or investigation officer pursuant to prevailing laws,

e) Notwithstanding whatever written in the prevailing laws of service, departmental action to the head and staff of Financial Information Unit.

As per section 10(7) of ALPA, 2008, Financial Information Unit, on the basis of gravity, may fine up to one million rupees to a reporting entity which does not submit STR or does not comply or violate prescribed conditions or does not submit the ordered documents or information.

Finally, this guideline does not cover the exhaustive list of the indicators. REs need to identify, understand and assess the risk and context in line with NRA-2020. Moreover, REs are required to provide reasonable basis of suspicion in accordance with the FATF Recommendations, Methodology and domestic legal provisions.

Note

- While referring Sector-specific indicators or red flags REs are prescribed to follow General indicators (such as Economically Irrational transaction, Use of Third party, Behavior of the customer, Cash and so on)
- REs reporting through goAML software should submit the report as per the
    i.) **Reporting TTR and STR in goAML Operational Guideline for REs**
    ii.) **Standard XML Reporting Instructions and Specifications**
    iii.) **goAML Web Reporting Guideline,** 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.
- For further information, please contact the Financial Information Unit-Nepal (FIU-

NEPAL RASTRA BANK

FINANCIAL INFORMATION UNIT, NEPAL

(FIU-Nepal)

Tel: 01-4410201 (Ext. 841)
Fax: 01-4441051
Emails: fiu@nrb.org.np, fiupolicy@nrb.org.np
goAML Emails - goaml@nrb.org.np,
goamlsupport@nrb.org.np
goAML Tel: 01-4410201 (Ext. 415/418)
Website: www.nrb.org.np/departments/fiu