STR/SAR Guidelines

(Updated July 2025)

FINANCIAL INTELLIGENCE UNIT, NEPAL

(FIU-Nepal)

Nepal Rastra Bank, Baluwatar, Kathmandu

VERSION CONTROL

Version	Description	Release Date
1	**First Issue**	January 2014
2	**Second Issue** Major changes: • Addition of red flags/indicators	January 2020
3	**Third Issue** Major changes: • Addition of new categories of red flags/indicators	July 2021
4	**Fourth Issue** Major changes: • Addition of new categories and sector-wise red flags/indicators • Addition of predicate offence-wise red flags/indicators	July 2025

ACRONYMS/ABBREVIATIONS

AI	Artificial Intelligence
ALPA	Asset (Money) Laundering Prevention Act, 2008
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
CFP	Combating the Financing of Proliferation of weapons of mass destruction (WMD)
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
FDI	Foreign Direct Investment
FIs	Financial Institutions
FIU-Nepal	Financial Intelligence Unit, Nepal
FSRB	FATF Style Regional Body
KYC	Know Your Customer
LEAs	Law Enforcement Agencies
ML	Money Laundering
MVTS	Money Value Transfer Service
NPOs	Non-Profit Organizations
NRA	National Risk Assessment
PF	Proliferation Financing
PSOs	Payment System Operators
PSPs	Payment System Providers
REs	Reporting Entities
SAR	Suspicious Activity Reporting
STR	Suspicious Transaction Reporting
TF	Terrorist Financing
TTRs	Threshold Transaction Reports

TABLE OF CONTENTS

DISCLAIMER

This 'STR/SAR Guidelines' provides general guidance for REs in identifying suspicious transactions and meeting their reporting obligations under Section 7(S) of ALPA, 2008. However, the Guidelines is not intended to constitute legal advice from the FIU. Nothing in the Guidelines should be construed as evidence of complying with the requirements of or relieving REs from any obligations under ALPA, 2008, ALPR 2024 or regulatory provisions issued by the concerned regulator.

The Guidelines 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. Further, the list of indicators provided is not an exhaustive list and should not solely be relied on while carrying out STR/SAR related responsibilities.

FOREWORD

It is my privilege to present the updated *'Suspicious Transaction and Suspicious Activity Reporting (STR/SAR) Guidelines*', issued by the Financial Intelligence Unit of Nepal (FIU-Nepal). This updated edition builds upon earlier versions, incorporating international best practices, national legal requirements, and lessons learned through implementation to further strengthen Nepal's Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) regime.

Since the first issuance of the guidelines in 2014, FIU-Nepal has continuously refined its framework in response to emerging risks, the evolving global financial landscape, and recommendations of the Financial Action Task Force (FATF) and Asia/Pacific Group on Money Laundering (APG).

This version has added sector-specific red flag indicators across banks, insurance, cooperatives, securities, real estate, non-profit organizations, casinos, remittance services, PSPs/PSOs, DPMS etc. We have also incorporated predicate offence–wise indicators to help reporting entities better identify, classify, and report suspicious transactions/activities linked with money laundering, terrorist financing, proliferation financing, fraud, corruption, cybercrime, tax evasion, and other offences. Updated guidance focuses on reporting quality and narrative requirements, ensuring STRs/SARs are comprehensive, accurate, and analytically useful for FIU-Nepal and law enforcement agencies. This version is aligned with Nepal's National Risk Assessment (NRA) 2020 and amendments to the Asset (Money) Laundering Prevention Act (ALPA, 2008 – amendment 2024), ensuring alignment with national priorities and international commitments.

The guidelines are intended to serve as a practical tool for Reporting Entities (REs)— Financial Institutions (FIs), and Designated Non-Financial Businesses and Professions (DNFBPs)—to fulfill their statutory obligations under ALPA, 2008. By outlining indicators, this document seeks to improve the quality and effectiveness of STR/SAR submissions.

FIU-Nepal acknowledges that combating money laundering, terrorist financing, and proliferation financing is a shared responsibility. Strong compliance frameworks, vigilant monitoring, and effective reporting by REs are indispensable in safeguarding the integrity and stability of Nepal's financial system. We trust that this updated Guidelines will further support reporting entities, regulators, and other stakeholders in discharging their legal obligations, enhancing operational effectiveness, and reinforcing Nepal's standing in the global AML/CFT community.

I extend my sincere appreciation to Deputy Director Mr. Sworup Shrestha and the Policy and Planning team for their leadership in updating this Guidelines. I also acknowledge with gratitude the valuable contributions of Deputy Directors Mr. Keshav Prasad Rimal and Mr. Bishnu Prasad Guragain and all employees of FIU-Nepal whose constant support has been instrumental throughout this process. I would also like to acknowledge the valuable feedback and contribution received from Regulatory/Supervisory authorities and REs. We remain committed to continuous improvement and warmly welcome your feedback to further strengthen our endeavors.

Bashu Dev Bhattarai
Head/Director, FIU-Nepal
July 2025

CHAPTER 1: INTRODUCTION

1.1 Background

This Guidelines has been issued in pursuant to Section 7 (S)(2)and Section 10 (1)(b) of ALPA, 2008*(with amendment)*for all the reporting entities to clarify their obligation regarding reporting of suspicious transactions and suspicious activities.

Criminals and criminal groups are continuously attempting to exploit the products and services offered by financial institutions and DNFBPs to launder their illicit proceeds. Therefore, along with other safeguards, a strong mechanism for reporting suspicious transactions is critical for an effective AML/CFT regime in any jurisdiction. Through the submission of STRs/SARs, the REs helps in the detection and disruption of criminal proceeds entering the formal system. 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.

1.2 Objectives

The objectives of this Guidelines are:

i. To provide practical guidance for REs to identify and recognize suspicious transactions.
ii. To provide a wide-ranging list of general and sector-specific and predicate offense-specific indicators to assist REs in fulfilling their STR/SAR responsibilities.
iii. To improve the quality of STRs and SARs reported to FIUs such that they are based on reasonable ground for suspicion of ML/TF/PF offense.
iv. To inform REs on technical requirements regarding what to report, when to report and how to report STR/SARs.

1.3 Scope and Limitations

This Guidelines provides guidance for REs of all sizes and across all sectors in identifying suspicious transactions and meeting their reporting obligations. The list of REs, along with their respective regulators, is presented in the next section.

This Guidelines is not intended to act as a substitute to RE's own assessment and judgment. Further, using this Guideline doesn't relieve REs from the responsibility to exercise their own knowledge of customer's line of business, financial history and behavior, as well as, apply due care in relation to the specific circumstances of the transaction or activity.

1.4 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

- 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.

1.5 Domestic Legislation

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

- Asset (Money) Laundering Prevention Act (ALPA), 2008 (amendment, 2024)
- The Prevention of Corruption Act, 2002
- The Proceeds and Instrumentalities of Crime (Freezing, Seizing and Confiscation) Act 2014
- Mutual Legal Assistance Act, 2070
- Extradition Act, 2013
- Organized Crime Prevention Act, 2070
- Assets (Money) Laundering Prevention Rules, 2024
- AML/CFT related directives and circulars issued by respective regulators
- Other relevant laws and regulations

1.6 National Risk Assessment (NRA), 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 include Counterfeiting and Piracy of Products, Kidnapping, Illegal Restraint and Hostage Taking, International Terrorism, Trafficking in Stolen Goods, Insider Trading and Market Manipulation.

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.

CHAPTER 2: STR / SAR: WHO, WHAT AND HOW TO REPORT

2.1 Legal Provision:

As per Section 7(S)(1) of ALPA 2008*(amendment,2024),* Reporting Entities shall make a suspicious transaction report to the FIU **immediately after assessing** the 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/CF or other offence, or

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

As per Section 7(S) (2) of ALPA 2008, RE shall also submit the report of attempted transactions or activity to FIU-Nepal.

2.2 Who should report?

ALL REs must report STR/SAR to FIU-Nepal. Failure to submit STR is punishable by law. As per section 10(7) of ALPA, 2008 *(amendment, 2024),* Financial Intelligence Unit, on the basis of gravity, may fine up to ten 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.

STR/SAR process may start with any employee of a RE; however, a RE has to appoint a compliance officer at management level to report STR/SARs as per Section 7(P)(3) of ALPA, 2008.

As per ALPA, 2008 "Reporting Entity" (RE) means Financial Institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs). The reporting entities and their regulators are presented in Table 1 as below:

Table 1: Regulators and Reporting Entities

Regulators & Supervisors	Reporting Entities
Nepal Rastra Bank (NRB)	A, B, C, D Class Banks and Financial Institutions
	Infrastructure Development Bank
	Cooperatives Bank
	Money Remitters
	Money Changers
	Payment System Operators (PSOs)

Regulators & Supervisors	Reporting Entities
	Payment Service Providers (PSPs)
	Employee Provident Fund
	Citizen Investment Trust
	Social Security Fund
	Public Debt and Securities licensed by NRB
	Hire Purchase Loan Providers
	Other entities licensed by NRB
Securities Board of Nepal (SEBON)	Securities Brokers
	Merchant Bankers
	OTC Market
	Commodity Trading Brokers
	Investment Management Professionals
	Investment Companies
	Other entities licensed by SEBON
Nepal Insurance Authority (NIA)	Life Insurance Company
	Micro Life Insurance Company
	Non-Life Insurance Company
	Micro Non-Life Insurance Company
	Re-Insurance Company
	Insurance Brokers
	Other entities licensed by NIA
Department of Cooperatives	Cooperatives regulated by Federal Level
	Cooperatives regulated by Province Level
	Cooperatives regulated by Local Level
	Central Cooperative Associations carrying out financial transactions with cooperative organizations
Inland Revenue Department (IRD)	Approved Retirement Funds
	Dealers in Precious Metal & Stones

Regulators & Supervisors	Reporting Entities
Ministry of Culture, Tourism & Civil Aviation (MOCTCA)	Casinos or Online Casinos
Department of Land Management and Archive (DOLMA)	Real Estate Business/Agents
Nepal Notary Public Council	Notary Public
Institute of Chartered Accountants of Nepal (ICAN)	Registered Auditors and Accountant/Chartered Accountants' Firm
Office of the Company Registrar (OCR)	Company & Trust Service Providers
Nepal Bar Council	Law Practitioners

Regulators & Supervisors	Reporting Entities
Department of Transport	Automobile Selling Companies (Vehicle Dealers)

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

2.3 How to Report?

- STR/SAR should be reported to the FIU-Nepal electronically through goAML system.
- Reporting through goAML software should be as per goAML Operational Guidelines issued by FIU-Nepal.
- REs should properly understand the business logic behind any transaction and provide all the necessary and available information while reporting in goAML.
- 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.
- STR/SAR should be reported to the FIU-Nepal as soon as possible and within three days after establishing the reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of money laundering offence or a terrorist financing offence.
- 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.
- REs should provide reference to the 'Predicate offence' listed in the ALPA 2008*(amendment, 2024),* Section 2(Y).
- Besides, REs should follow any other guidelines issued by concerned regulators and other concerned authorities.

PREDICATE OFFENCE

Reporting of STR/SAR should provide a reference to the as per the Annexure under Section 2(Y) "Predicate offence" means: -

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

1. Participation in Organized Criminal Groups and Illegal or Fraudulent Racketeering Related,
2. Destructive Acts, Including Terrorism Related,
3. Every Form of Human Trafficking and Smuggling Related,
4. Every Form of Child Sexual Exploitation and Sexual Exploitation Related,
5. Illegal Trafficking of Narcotic Drugs and Psychotropic Substances Related,
6. Illegal Trafficking in Arms and Ammunition Related,
7. Illegal Trafficking of Stolen or Other Goods Related,
8. Corruption and Bribery Related,
9. Fraud Related,
10. Forgery Related,
11. Counterfeiting of Coin and Currency Related,
12. Production of Counterfeit Goods and Illegal Reproduction or Theft (Piracy Of Products) Related,
13. Environment Related,
14. Murder and Grievous Bodily Injury Related,
15. Kidnapping, Illegal Detention / Restraint, or Hostage-Taking Related,
16. Theft or Robbery Related,
17. Smuggling (Including Customs, Excise, and Tax) Related,
18. Tax (Including Direct or Indirect) Related,
19. Criminal Extortion Related,
20. Maritime Piracy Related,
21. Adversely Affecting the Securities or Commodities Market (Market Manipulation) or Insider Trading Related,
22. Conservation of Ancient Monuments Related,
23. Forests, National Parks and Wildlife Conservation Related,

24. Money (Currency), Banking, Finance, Foreign Exchange, Negotiable Instruments, Insurance, Or Cooperatives Related,
25. Black Marketing, Consumer Protection, Competition, or Supply Related,
26. Elections Related,
27. Communication, Broadcasting, and Advertising Related,
28. Fraud in Transportation Business, Education, Health, Medicine, or Foreign Employment Related,
29. Firms, Partnerships, Company or Association/Organizations Related,
30. Real estate and Property Related,
31. Lottery, Gambling, or Donations Related,
32. Citizenship, Immigration, or Passport related,

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

(3) The Government of Nepal added following offences as predicate offences of ML as per the decision by Council of Ministers on 24 December 2024:

1. Human Trafficking Related,
2. Hundi Related,
3. Use of Virtual Currency Related,
4. Undue Transaction Related,
5. Match Fixing and Irregularities in Sports Related,
6. Unauthorized Casino Operation Related.

(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.*

2.4 What to Report?

In general, STR must contain following details. Similarly, SAR shall contain as much details as possible.

- Summary of suspicious transaction(s)/activities
- Analysis or Examination
- Possible Linkage
- Suspected Beneficiary

- Updated CDD information
- Related account statement
- Mandatory details (as required by regulators)
- Correct identifications
- Media/news and other relevant documents (if any)
- Other details or supporting documents.
- REs are encouraged to add value to the information by searching and adding web materials along with its sources.

In addition to above list, in general, STR/SAR shall be reported to FIU-Nepal along with the below mentioned details and supporting documents: -

a) In case of Person

- Full Name (First Name, Middle Name, Last Name)
- Date of Birth (in AD)
- Gender
- Either Father's or Mother's Name (Both if provided)
- Grandfather name (if provided)
- Spouse name (if provided)
- Nationality
- Residence
- Other Nationalities (if provided)
- Permanent Address
- Current Address
- Telephone/Mobile number
- Email Address (if provided)
- ID details
- Employer Details (if provided)
- Occupation
- Source of Income
- PAN number (if provided)

b) In case of Entity

- Name
- Commercial Name
- Registration Legal Form (Type of Entity)
- Nature of Business
- Registration Number
- Registration Date
- Registering Authority
- Registration Country Code
- Registration Certificate (attach)
- PAN/VAT Number
- PAN/VAT Registration Date
- Email
- URL
- Account Opening Form(attach)
- PAN/VAT Certificate(attach)
- Updated KYC related documents of Entity and its Director(s) and Signatory(ies)(attach)s
- Account Statement (if available attach in excel)
- Information related to Holding Company, Subsidiary and Associates or Other Business entities within the Group

For specific requirements for reporting STR/SAR, kindly refer to sector specific goAML operational guidelines issued by FIU-Nepal.

CONTENTS OF REPORTING

a) Completeness

A single STR/SAR must stand-alone and contain complete information about the suspicion. A STR/SAR shall provide 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.

b) Updated

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

However; as per sub-section (2A) of section 7S of ALPA, if the reporting entity feels that the customer may know regarding identification of suspicious transaction, then CDD shall be updated after reporting STR/SAR to FIU-Nepal.

c) Quality

The quality of a STR/SAR is important in increasing the effectiveness of the quality of analysis by FIU-Nepal and investigation by LEAs which would assist in preventing abuse of the Nepalese financial system by criminals and terrorists. Furthermore, the REs have to submit STR/SARs as per the prescribed format and medium. Therefore, the relevant information shall 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 or terrorist financing or proliferation financing;
- 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.

d) Narrative

The narrative portion of the report is most important. REs should perform proper analysis at their end regarding the STR/SAR and provide preliminary analysis report with relevant information and details as to why the reported transactions/activities 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 offences relinked?
- 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/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 is 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 STR/SARs 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.

e) 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.

CHAPTER 3: INDICATORS

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/activity 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;

- General indicators,
- Sector-specific indicators, and
- Indicators related to Predicate-Offences and other 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.

3.1 GENERAL INDICATORS

General indicators are the common signs that may show a transaction or activity is unusual or suspicious. They help reporting entities recognize when to review and possibly report such transactions.

3.1.1 Economically irrational transactions

1. If the transactions have no conformity with the initial purpose of account opening.
2. If the transactions have no relationship with the business or nature of the business (e.g. regular transaction between a cement company and a shoe factory).
3. If customer conducts complex, unusual large transactions and unusual pattern of transactions or which have no apparent economic or visible lawful purpose.
4. If the transaction amount and frequency are different from that of normally conducted by the customer.
5. If there are attempts to disguise the real owner or parties to the transaction.
6. 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.
7. If customer fails to provide reasonable justification of the transaction.

8. If any suspicious pattern emerges from customer's transactions.
9. If the intensity of transactions for an inactive trading account suddenly increases without plausible reason.
10. If there is frequent selling of securities at significant losses.
11. If there are large number of transaction in accounts of home maker, farmer, student etc.
12. If a high volume of low-value online transactions conducted by a business—such as an unusually large number of digital payments by a small auto workshop, grocery stores, etc. on certain days compared to its typical activity. Further, similar type of transaction in individual accounts too.
13. If irregular international wire transfers to/from high-risk or unrelated jurisdictions.

3.1.2 Use of third party

1. If multiple deposits are made to an account by non-account holders.
2. If unrelated parties are sending fund transfers or other forms of electronic transfers to the same beneficiary with no apparent relation to the recipient.
3. If a client conducts transaction while being accompanied, overseen or directed by another party.
4. If a client makes numerous outgoing payments to unrelated parties shortly after they receive incoming funds.
5. If there is wire transfers, deposits or payments to or from unrelated parties (foreign or domestic).
6. If a client appears or states to be acting on behalf of another party.
7. If an account is linked to seemingly unconnected parties.
8. If unrelated third person is repeatedly depositing/withdrawing as a conductor in a particular account.
9. If an account holder's profession is non-income generating such as housewife, student, unemployed etc. but transaction amount is relatively high.
10. If there is involvement of third parties funding without apparent connection or legitimate explanation.
11. If unknown third party frequently transfers funds into customer's account.
12. If unrelated third party is unnaturally, unnecessarily involved or is more active in transaction.
13. If the nominee is third party.
14. If there is simultaneous transfer of funds to a group of customers' accounts from a third party.

3.1.3 Behaviors of the Customer

1. If there are frequent changes to the address, telephone/mobile number or authorized signatories.
2. If the customer/client's address is a virtual office.
3. If there is unreasonable behavior of the customer when conducting a transaction (nervous, rushed, unconfident, etc.).
4. If the customer is linked with Money Laundering or Terrorist Financing or Proliferation Financing or any other crime related adverse news or other indicators relating to the financial or predicate crime.
5. If customer shows unusual curiosity about internal system, control and reporting.
6. If customer admits or makes statements about involvement in criminal activities.
7. If customer offers money, gratuities or unusual favors for the provision of services that appear unusual or suspicious.
8. If customer/prospective customer gives doubtful or false information with respect to his/her identity, sources of income or businesses.
9. 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.
10. 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 Transaction.
11. If customer opens the account for a short period and closes without a valid reason.
12. 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.
13. If customer uses simple signature which can be imitated by other persons.
14. If customer appears to have accounts with several bank and financial institutions without a valid reason.
15. If customer opens an account at a branch which is far from his/her place of residence or office.
16. If customer conducts his/her transactions at a different branch than the branch near to his/her residence of office.
17. If customer over justifies or explains the transaction, has ambiguous knowledge about the transaction amount/details or has little knowledge about the purpose of the transaction.
18. If customer is unwilling to be present in person.

19. If contact number of home or business provided by the customer is invalid/out of service shortly after establishing business relation with him/her.
20. If customer tries to convince staff of bank and financial institutions to alter or omit reporting data.
21. If there are multiple failed login attempts in mobile banking/internet banking platforms.
22. If transactions occur outside normal business hours' such as late night, early morning.
23. If there is creation of multiple wallet accounts across different PSPs using the same mobile number but with different names.
24. If customer insists on opening account using mobile number registered under the name of another person.
25. If customer categorized in higher risk category closes the account and reopens the account in an apparent attempt to avoid due diligence.
26. If customer expresses unusual urgency or pressure to complete large transactions quickly, despite delays in documentation.
27. If the customer aggressively resists EDD or internal audit checks, or threatens to file complaints to authorities.

3.1.4 Cash

1. If the transactions are conducted in a relatively small amount but with high frequency (structuring).
2. If the transactions are conducted by using several different individual names for the interest of a particular person (Smurfing).
3. If customer conducts series of transactions or book-keeping tricks for concealing the source of fund (layering).
4. 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.
5. If a person sending money cannot provide even general information about the recipient.
6. If any person brings huge cash for deposits which appears to be soiled and dusty or have unusual odor.
7. If cash is handled with unnatural binding or packaging during transaction.
8. If customer presents notes that are packed or wrapped in an unusual manner.
9. If customer conducts a series of large deposits within a short period of time in cash or by other medium and keeps on withdrawing or transferring until all deposited funds are nullified.

10. If the customer's level or type of transactions does not tally with the profession/job reported. For instance, a student/housewife/jobless customer makes a series of large cash deposits and withdrawals.
11. If an account balance is increased all of a sudden through large cash deposits.
12. If customer intentionally uses different tellers of same bank and financial institutions to perform numerous transactions on the same day at the same branch.
13. If a customer makes large loan repayments using cash without a valid reason.
14. If cash deposit into dormant account is followed by updating account and then immediate withdrawal via POS machines or ATMs.
15. If high-volume cash transactions are conducted in rural branches where digital banking penetration is low.

3.1.5 Wire/Fund transfer activities

1. If customer fails to provide adequate information about the originator, beneficiary, and purpose of the wire transfer, or gives misleading, vague, or false details.
2. If a customer orders wire transfers in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
3. If the pattern of wire transfers shows unusual patterns or has no apparent purpose.
4. If customer receives frequent fund transfers from individuals or entities who have no account relationship with the person/institution.
5. If multiple cash deposits in small amounts in an account are followed by a large wire transfer to another country.
6. If several customers request transfers either on the same day or over a period of two to three days to the same recipient.
7. If beneficiaries of wire transfers involve a large group of nationals of countries associated with terrorist activities.
8. 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.
9. If fund transfers to and from high-risk offshore financial centers occur without any clear business purpose.
10. If receipts of fund transfer occur in several phases and, once accumulated, the funds are subsequently transferred entirely to other account.
11. If receipts/payments of funds are made by using more than one account, either in the same name or different names.
12. If fund transfers are made using the account of a reporting entity's employee in an

unusual amount.

13. If multiple inward or outward remittance transaction is conducted with the person from the country or region where terrorist organizations operate.
14. If customer shows unusual interests in wire transfer ceiling and availability of alternative or informal channels.
15. If wire transfer from foreign country is followed by multiple transfers to other domestic accounts.
16. If there is high frequency and high volume of wire transfers which does not match with declaration made by customer.
17. If frequent cash withdrawal and online transfer occur from a customer's account while the customer is abroad for foreign employment.
18. If customer staying abroad for foreign employment receives regular cash deposits and IPS transfers from different people.
19. If cash deposits or withdraws mention purpose or source of funds as “borrowing” or “borrowing returns”.
20. If same amount is deposited via transfer and withdrawn in cash on the same day.
21. If frequent fund transfers between bank and digital wallet accounts occur with no clear commercial link.
22. If transfers are made to Indian banks or mobile wallets from Nepali customers without supporting documentation.

3.1.6 Money Laundering involving employees and agents of REs

1. If a significant change is found in employee/agent's lifestyle (e.g. lavish lifestyles or avoiding taking holidays).
2. If significant changes is found in employee or agent performance.
3. If employee/agent's any dealing is found with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.
4. If the employee/agent's account has elements of unusual fund transfer and/or structuring.
5. If employee/agent is found involved in misuse of ATM cards, false identification and inadequate source of funds.
6. If the employee is involved in frequent internal fund transfers outside their job scope.
7. If employee/agent is showing excessive curiosity about accounts not part of their regular duties, especially high-value or unusual ones.

8. If employee/agent is developing unusually personal or secretive ties with clients who exhibit red flags or are known to be high-risk.
9. If employee/agent is trying to pressure or persuade AML or compliance personnel to ignore red flags or expedite suspicious processes.
10. If an agent consistently facilitates large cash transactions on behalf of clients, especially when not typical for their business or the client's profile.

3.1.7 Corporate and business transactions

1. If accounts are being used to receive or disburse large amounts but show no normal business related activities, such as the payment of payrolls, invoices, etc.
2. If the transaction is not economically justified considering the account holder's business or profession.
3. If the customer makes a large volume of cash deposit from a business that is not normally cash-intensive.
4. If the customer does not want to provide complete customer due diligence information of their business.
5. If the financial statements of the business differ noticeably from those of similar businesses without valid reasons.
6. If size of wire/fund transfers is inconsistent with normal business practice/transactions for the customer.
7. If unexplained transactions are repeated between personal and business accounts.
8. 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.)
9. If transactions are structured to evade substantial shareholding requirements.
10. If an existing company struggling with cash-flow problems suddenly receives funding from a silent investor or partner, resulting in high levels of transactions.
11. If the same person is a shareholder or owner of two or more companies or entities, and there are frequent large transfers to and from their accounts without any valid commercial reason.
12. If the sales turnover/transactions reflected in bank statement differ significantly from that reported in the tax clearance certificate/ audited financial statements for the same fiscal year.
13. If the business is not fully operational for various reasons, yet there are bank transactions equal to or exceeding normal levels without valid justification.
14. If there is a transfer of funds to multiple unrelated individual or legal entity accounts.

15. If the same person owns or is engaged in multiple businesses that are contrary/ unusual compared to the initial declaration made by the customer.
16. If there are repeated cash withdrawals from the account by Key Management Personnel in an apparent attempt to disguise the ultimate end use of funds.
17. If frequent or large fund transfers recorded in financial statements among sister companies or subsidiaries operating under the same business group - having common shareholders or directors- without a clear business rationale, service contract, or economic justification for such movements.
18. If there is exponential growth in business transactions for a company whose products or services show no corresponding demand in the market.

3.1.8 Lending

1. If the customer makes a large, unexpected loan repayment with unknown source of funds, or a source of fund that does not match what the credit institution knows about the customer.
2. If the customer suddenly repays a problematic/ non-performing loan unexpectedly without any valid or documented reason.
3. If the customer repays a long term loan, such as a mortgage, within a relatively short time period.
4. If the source of down payment is inconsistent with borrower's financial ability, profession and business as per the declaration.
5. If the customer shows income from foreign sources on loan application without providing further details.
6. If the customer does not seem concerned with terms of credit or costs associated with completion of a loan transaction.
7. 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. If the loan is found misused or there is lack of transparency where the funds are going or if loan proceeds are quickly transferred to multiple unrelated accounts or jurisdictions.
9. If the borrower is reluctant to provide necessary information, provides misleading details or tries to conceal the true nature of the transactions.
10. If the borrower tries to avoid due diligence.
11. If there are guarantors or co-signers with no apparent connection to the borrower or the stated purpose of loan.
12. If the borrower makes request for loan disbursement to third parties or disburses directly to unfamiliar or unrelated party.

13. If the borrower tries to bribe or exert undue influence on bank employees.
14. If it seems that the ultimate beneficiary of the loan is taking advantage of the old age or financial illiteracy or improper mental condition of the collateral owner to disburse loan in his\her favor.
15. If a third party with no clear relationship to the borrower makes cash deposit to repay the loan of borrower.
16. If a loan top up is requested immediately after full settlement of previous loan using funds from an unknown source, potentially indicating layering of illicit funds.

3.1.9 Use of Artificial Intelligence and New Technologies

a) Digital Identity and KYC Evasion

1. If the customer's KYC documents appear digitally manipulated, AI-generated (e.g., deepfakes), or submitted through platforms that mask device/location/caller ID.
2. If identity verification is repeatedly attempted using altered images or synthetic biometric data (e.g., AI-altered facial features).
3. If the customer uses anonymization tools or device-cloaking apps (e.g., VPNs, spoofed IMEI numbers) during account creation or transaction execution.

b) Automated or Bot-Based Transaction Patterns

4. If transaction behavior appears bot-like — e.g., transactions executed at precise intervals, across multiple accounts, or following non-human patterns of frequency and timing.
5. If multiple accounts are opened and operated in coordination, with similar metadata (device ID, IP, location spoofing), suggesting automated orchestration.
6. If the customer interacts with financial services via AI-powered apps, Telegram bots, or APIs instead of traditional web/mobile channels — especially where such tools are linked to gambling, betting, or crypto arbitrage.

c) Emerging Platforms and Unregulated Technologies

7. If the customer receives or sends funds to/from AI-integrated platforms such as online gaming apps, unregulated investment bots, or DeFi protocols (*it refers to financial services (like lending, trading, saving, insurance, etc.) that operate without traditional banks or intermediaries — using block-chain and smart contracts instead)* that claim to use AI to manage user portfolios or bets.
8. If transaction references, app logins, or narration fields show mentions like "GPT payout," "AI bot win," "signal-based trading," or "auto-bet result."

9. If users are involved in fundraising through tokenized platforms (e.g., Non-Fungible Token, synthetic asset platforms) without clear regulatory compliance or declared purpose.

d) Behavior Inconsistent with Customer Profile

10. If an individual with no prior investment or tech background suddenly engages in complex AI-enabled platforms like algorithmic trading, token minting, or auto-yield farming.
11. If there is a sudden spike in high-risk transactions, coinciding with the launch of a new AI-based application or "money-making scheme."
12. If large volumes of micropayments (e.g., Rs. 5–50) occur at exact intervals and across multiple linked accounts — a pattern commonly used in AI-based payout gaming or pyramid schemes.

e) Misuse of AI to Facilitate ML/TF or Fraud

13. If a platform or app is used to launder illicit gains through AI-driven casino/betting apps, particularly when paired with proxy wallets, masked phone numbers, or non-resident remitters.
14. If customer funds are moved into AI-based asset management tools or robo-advisors that offer guaranteed returns or advertises "untraceable investing."
15. If transactions support AI-generated scams (e.g., fake loan offers, romance scams, voice synthesis fraud) — especially if victim complaints or charge backs are registered later.

f) Other

16. If customers with no technical or financial background engage in unusual use of AI-driven financial platforms such as automated trading, lending apps, or virtual wealth managers.
17. If transactions involve peer-to-peer lending platforms or crowd-funding portals that are not registered or regulated in Nepal.
18. Ifa customer shows excessive interest in financial products promoting anonymity (privacy coins, zero-knowledge proof technologies, etc.).

Example: A 27-year-old IT technician based in (e.g. Butwal) opens a personal account at a commercial bank, declaring his income as freelance web development. Within a short span, the account begins receiving frequent small-value deposits from digital wallets, remittance agents, and even e-banking transfers from multiple unrelated individuals, primarily located in Koshi Province, Madhesh Province and some from Gulf countries. The customer explains vaguely that these are "client payments" for technical support and e-marketing work. However, the transaction pattern shows round-the-clock activity, including late-night deposits and immediate automated withdrawals.

Upon further review, it is revealed that the individual is operating a Telegram-based betting group and using an unregulated online platform that utilizes AI bots to manage deposits, payout bets, and track user IDs. The bank also observed the use of a mobile application by the customer that concealed device and caller information. During KYC verification, the identity document submitted was found to be digitally altered. Despite claiming freelance income, there was no supporting business registration, and the pattern and volume of transactions were inconsistent with his stated profile. These factors raised suspicion of potential involvement in online betting operations and the use of advanced technologies to obscure identity and facilitate illicit fund flows—triggering red flags under the category of Artificial Intelligence and new technologies.

3.1.10 Involvement of PEPs

1. If large or complex transactions are conducted that are inconsistent with the customer's known legitimate income or business activities.
2. If transactions involve frequent or large cash deposits and withdrawals.
3. If there are transfers to or from high-risk jurisdictions or countries known for corruption or money laundering.
4. If multiple accounts or intermediaries are used to disguise the origin or destination of funds.
5. If there is sudden increase in account activity or transactions after the customer becomes PEP.
6. If the lifestyle of a PEP appears inconsistent with their known income or official salary.
7. If the customer holds senior or sensitive political position or is closely linked to them.
8. If a transaction involves PEPs acting as ultimate beneficial owners or intermediaries.
9. If the customer refuses or is reluctant to provide information about the source of funds or beneficial owners.
10. If there is frequent cross-border wire transfers or use of correspondent banking services in high-risk jurisdictions.
11. If ownership structures appear unnecessarily complex or involve entities across multiple jurisdictions.
12. If shell companies, trusts, or nominee arrangements linked to PEPs are used to obscure ownership or control.

3.1.11 Miscellaneous Ground for Suspicion

1. If a customer/client is linked to adverse media news (national or international).
2. 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.
3. If it is evident that any one is earning wealth (including cash) by evading tax, custom

duty, land revenue, electricity bill, water bill, phone bill and any other revenue or government fees.

4. If anyone lives an unusual lifestyle compared to his/her economic strength, profession/business.
5. If any act or transaction is not found reasonable or is found to have been conducted with an irrelevant party or where the transaction has no justifiable purpose.
6. 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.
7. If it is known or evident that the customer's transaction is under investigation or subject to proceedings by a competent law enforcement agency or regulatory authority of a foreign country.
8. If it is evident that the asset is earned from any offence against or abuse of children, women or destitute or any other individual.
9. 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.
10. If the transaction conducted by a customer comes under suspicion based on the ground provided by regulator or concerned authority.
11. If any customer shows unnecessary interest in suspicious transaction or makes unnecessary and unnatural queries about the internal management of such transaction.
12. If there is a cross transaction between customers who are not related with each other, or any individual transmits or receives an amount from unrelated person or business institution's account.
13. If there is suspicion that any transaction is aiding criminal activities or receiving amount from such activities.
14. If multiple transactions are conducted with the people living in the country, where the AML/CFT regime is poor, for no apparent reason.
15. If anyone tries to complete the transaction by paying more without any reason.
16. If there are multiple claims for the amount received from one person.
17. If anyone denies providing identity information or clear justification of the transfer though there are sufficient grounds to know such information.
18. If the reporting institution finds the grounds for suspicious transaction reporting for any other transaction as per the prevailing law.
19. If there is purchase of non-refundable tourism packages overseas and cancelled for

some reason.

20. If there is existence of triangular and prolonged settlement of transactions.
21. If the website of company shows different business than nature of transaction in the account.
22. If an individual earning a regular salary also owns a similar business enterprise.
23. If multiple employees of a business are engaged in similar types of businesses themselves.

3.2 SECTOR SPECIFIC INDICATORS

Sector-specific indicators are warning signs tailored to particular industries or types of Reporting Entities. These indicators reflect the unique risks and patterns of suspicious activity within different sectors and help Reporting Entities apply more precise detection and reporting measures based on their operational context.

3.2.1 Bank and Financial Institutions (BFIs)

1. If customer attempts to open or operate accounts under an identity that does not appear genuine.
2. 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.
3. If customer conducts series of complicated transfers of funds that seem to be an attempt to hide the source and intended, use of the funds.
4. If transaction involves a country known for highly secretive banking and corporate law.
5. If accounts are opened by customers who's residential or employment addresses are outside the local service area without a reasonable explanation.
6. If there is a sudden change in customer's financial profile, pattern of activity or transactions.
7. If customer uses notes, monetary instruments, or products and/or services that are unusual for such a customer.
8. If customer is suspected for using personal account for business or other purposes, or vice-versa.
9. 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 of high risk jurisdiction and tax haven countries.
10. 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.

11. In case of an account opened in the name of an entity, an organization or association, which is found to be linked or involved with a suspected terrorist organization.
12. 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.
13. If customer has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.
14. 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.
15. If account has close connections with other business accounts without any apparent reason for the connection.
16. If deposits to or withdrawals from a corporate account are primarily in cash.
17. If customer requests movement of funds that are uneconomical without any valid justification.
18. If customer visits the locker (safety deposit box) area immediately before making cash deposits.
19. If customer repeatedly conducts large foreign exchange transactions without valid justification.
20. If customer is found to have used/made or involved with counterfeit coin and currency.
21. If there is frequent deposit of third-party cheques or IPS transfer into business or personal accounts without business sense.
22. If there is a large amount/frequency of transactions in salaried employee, student, housewife, farmer, etc. accounts and significantly different from initial declaration by the customer without valid sources or justification.
23. If an individual repeatedly withdraws funds from his/her own account and deposit them into multiple other accounts without valid justification.
24. If a 'U-turn' transaction occurs, where funds received from a person or company in a foreign country is immediately remitted to another person or entity in the same country.
25. If a person visits the institution daily to deposit funds into various accounts without providing proper justification.
26. If a customer uses an unrelated product or service such as opting for mobile banking without owning a smart phone, or conducting digital transactions despite being illiterate.
27. If picture in the identity card (newly issued) does not match with the person presenting

it.

28. If the photo on the account opening form exactly matches the one on the identity card, despite the identity card being significantly old, indicating possible manipulation.
29. If amounts received from abroad are falsely presented as Foreign Direct Investment (FDI) in sectors where FDI is prohibited, and without obtaining the required approval from the competent authority.

3.2.2 Securities market

1. If accounts that have been inactive for a long period suddenly experience large investments that are inconsistent with normal investment practice of the client or their financial ability.
2. 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.
3. If trading between numerous accounts is controlled by/from the same people or IP address.
4. If a client seeks investment management or administration services using funds whose source is unclear or not aligned with the known financial profile of the client.
5. If client deposits funds into a broker's account and requests repayment within a short period without a valid reason, with little or no trading activity recorded, and the deposit amount is inconsistent with the client's profile.
6. If securities are purchased using cash, transfer, or cheques issued under another person's name or by third parties.
7. 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.
8. If transaction is conducted with the client sanctioned by APG/FATF/United Nations or other Inter-government international organizations.
9. If transaction patterns resemble a form of market manipulation, for example, insider trading and pump and dump.
10. If two or more accounts are used in coordinated buying and selling patterns to artificially increase or decrease the price of a security in an unusual manner.
11. If large amount of wire transfer is used for securities purchase as foreign indirect investment, especially from high-risk countries.
12. If customer is reluctant to provide further information for CDD.

13. If the address of the customer is associated with multiple other unrelated accounts.
14. If large purchase or sales of a securities is made by client shortly before significant price sensitive news is publicly disclosed.
15. If cash deposit is made directly in the stock broker account.
16. If a client requests a fund transfer or withdrawal without any prior trading activity.
17. If a transaction is conducted by director, employee, or family member associated with the same listed company.
18. If nominee accounts are used for trading in unlisted securities.
19. If an account receives a significant amount of cash claimed to be from securities transactions, but no actual trading activity is recorded, and the funds are later transferred to a third party account.

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: -

20. If client (a director, an 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.
21. If the client is known to have friends or family who work at or for the securities issuer.
22. If the client sells his or her position in a security in conjunction with a significant announcement about the security.
23. If there is a significant increase in trading volume for a particular stock without any apparent public news or company related developments.
24. If the customer's trading activity does not align with their stated investment profile or historical behavior (e.g., a customer who never invested in equity securities suddenly makes a large, well-timed equity purchase).

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: -

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

3.2.3 Insurance Sector

1. If the client purchases products which are inconsistent with their age, income, profession or financial history.
2. If the client purchases insurance products using a single large premium payment, especially when the payment is made in cash or through a third party.
3. If the client shows more interest in the cancellation or surrender of the product than in its long-term investment outcomes.
4. If the client is known to purchase several insurance products and uses the proceeds from early policy surrenders to acquire other financial assets.
5. If a high-value insurance policy is surrendered shortly after purchase.
6. If the client purchases an annuity using a lump-sum payment instead of making regular premium contributions over time.
7. If the client funds the policy through payments made by a third party.
8. If the client purchases multiple insurance policies just below the threshold limit instead of a single large policy.
9. If a client terminates product, especially at a loss, or if the original payment was made in cash and/or the refund is issued to a third party.
10. If a client frequently purchases and cancels multiple insurance policies.
11. If a client makes an overpayment of premiums and subsequently requests a refund of the excess amount.
12. If a client intentionally causes, inflates or fabricates insurance claims, including deliberate destruction of assets, in order to access funds that appear legitimate.

13. If a client is found to have involvement in establishment of bogus reinsurers/ insurers to launder the proceeds of crime.
14. If a client repeatedly surrenders existing policies and subscribes to new ones, either with the same or different life insurance companies.
15. If there is a high frequency of insurance policy subscriptions followed by immediate loan withdrawals against those policies.
16. If a client makes a pre-payment of insurance premiums under circumstances that appear unusual or inconsistent with standard practices.
17. If an insurance agent is reluctant to provide information required for updating CDD.
18. If a policy is surrendered immediately after maturity and the proceeds are redirected to a third-party account.
19. If a customer purchases multiple insurance products in cash within a short period or simultaneously, pays large premiums in full, and then surrenders the policies before the due date.

3.2.4 Cooperatives

1. If a member attempts to open or operate accounts under a false name.
2. If a member is reluctant to provide standard information when opening an account, provides minimal or fictitious information, or submits details that are difficult or costly to verify.
3. If an account is opened with an address or employment location outside the local service area without a reasonable explanation.
4. If there is a sudden change in the member's financial profile, transaction pattern, or account activity.
5. If a member uses instruments, products, or services that are unusual for their known profile.
6. If a transaction appears suspicious and the member is blacklisted by the Credit Information Bureau or categorized as high-risk by the reporting institution.
7. If member is suspected for using personal account for business or other purposes, or vice-versa.
8. If member conducts series of complicated transfers of funds that seems to be an attempt to hide the source and intended use of the funds.
9. In case of an account opened in the name of an entity, an organization or association, which is found to be linked or involved with a suspected terrorist organization.
10. If a member frequently deposits funds identified as proceeds from asset sales, but the existence or ownership of such assets cannot be substantiated.

11. If there are large cash withdrawals from a previously dormant or inactive account.
12. If an account is closely connected to other business accounts without any clear or legitimate reason for the relationship.
13. If deposits to or withdrawals from a corporate account are primarily in cash.
14. If member requests movement of funds that are uneconomical or irrational without valid justification.
15. If cheques are regularly returned due to insufficient funds.
16. If a member is found to have used, made, or been involved with counterfeit coins or currency.
17. If there is a large volume or high frequency of transactions in an individual savings account that significantly differs from the customer's initial declaration.
18. If a member repeatedly withdraws funds from their own individual account and deposits them into multiple other accounts without valid reasons.
19. If funds are transferred from a cooperative society to the personal bank accounts of its board members.
20. If dividend payments appear unusual or disproportionate to the actual shareholding.
21. If cooperative staff or employee accounts are used to route funds on behalf of non-members in order to artificially inflate fund balances, conceal true ownership, or bypass cooperative membership restrictions.
22. If digital or mobile payment platforms linked to cooperative accounts are used without clear operational justification or are inconsistent with typical cooperative transaction patterns.
23. If third parties unrelated to the cooperative's members or leadership frequently manage or authorize transactions on cooperative accounts.
24. If documentation related to membership verification, capital contributions, or loan disbursements is inconsistent, incomplete, or missing.
25. If the cooperative conducts cross-border fund transfers or remittances from its account maintained at commercial banks on behalf of a member.
26. If cooperative accounts are used to repeatedly route funds among related accounts without a clear business purpose, indicating potential layering or circular transactions.
27. If cooperative accounts are used for cash-based fundraising campaigns with unclear beneficiaries or unverifiable project outcomes.
28. If loan repayments show unusual patterns, such as early full settlement or installment schedules inconsistent with normal cooperative lending practices.
29. If cooperative accounts are used for real estate or asset purchases without proper

valuation, supporting documentation, or official registration.

3.2.5 Real Estate Business/Agent

1. If there is a discrepancy between the income or occupation and wealth of the buyer and the property as per the declared source of income.
2. If transactions are carried out on behalf of minors, incapacitated persons, or individuals who appear to lack the economic capacity to make the purchases.
3. If a purchaser buys multiple properties within a short time period and show little or no concern about the location, condition or characteristics of the properties.
4. If there is manipulation of the appraisal or valuation of a property, such as undervaluation, overvaluation, or successive sales at increasing values without legitimate justification.
5. If the amount listed on the contract of sale differs significantly from the actual transaction value or the amount stated in the *Rajinama* (Sales Deed).
6. If a customer purchases or sells real estate using a third party or family member—often someone with no criminal record—as the legal owner to conceal actual ownership.
7. If the transaction involves individuals who are being prosecuted or have been convicted for crimes related to money laundering or terrorist financing or proliferation financing, or who are publicly known or reasonably suspected to be linked to criminal activities involving illegal enrichment.
8. If a party requests the payment to be divided into smaller parts over a short period or asks for payments to be made to unrelated third parties.
9. If the property is resold immediately at a significantly higher price without a reasonable explanation.
10. If the purchaser expresses concern about threshold reporting or explicitly requests not to report the transaction.
11. If third parties are involved in the transaction through nominees, trusts, or corporate structures without a clear business rationale.
12. If buyers or sellers are reluctant to disclose their identity or the source of funds.
13. If properties are purchased at significantly above market value without any negotiation.
14. If the purchaser insists on completing the transaction urgently, bypassing normal due diligence procedures.
15. If ownership of a property changes frequently within a short period, accompanied by significant price increases and without a clear economic justification.

3.2.6 Non-Profit Organizations (NPOs)

1. If the beneficial ownership is obscure *(unclear, hidden or difficult to understand /identify)*.
2. If there are inconsistencies between the pattern or size of financial transactions and the stated purpose or declared objectives of the organization.
3. If there is a sudden increase in the frequency and amounts of financial transactions, or if the organization holds funds in its account for an unusually long period.
4. If the account shows signs of unexplained increase in deposits and transaction activities.
5. If the account of NGO/INGOs receives foreign funds without the knowledge of its regulator.
6. If the use of funds by a non-profit organization is not consistent with the purpose for which it was established.
7. If the funds for the organizational use comes in the name of individuals instead of the organization's account.
8. If funds are withdrawn from an NPO account, deposited into a personal account, and then channeled to other persons' or organizations' accounts.
9. If the organization has operations or funds from, or transactions to, high-risk jurisdictions.
10. If an NPO frequently changes it's declared area of operation, board members, or affiliated local partners, especially during periods of large fund flows.
11. If field-level disbursements or project expenditures are routed through personal accounts of staff, volunteers, or intermediaries without clear justification or audit trail.
12. If grant disbursements processed via AI-based scoring or third-party applications without proper human oversight.
13. If the organization raises donations in an unofficial or unregistered manner.
14. If there is lack of proper information regarding donors of foreign countries, especially of high-risk ones.
15. If there is a sudden change in donation channels (e.g., switching from traditional banking to informal, mobile-based platforms or cash-intensive drives) without proper reason.
16. If the same donor repeatedly contributes to multiple organizations operating under similar name, location, or governance structure indicating possible misuse of NPO layering or front organizations.
17. If social media-led donation drives are conducted without any registered affiliation to the named Non-Profit Organization (NPO).

18. If donation campaigns are launched online (e.g., GoFundMe-like platforms) with foreign backing, but there is no identifiable local beneficiary or no reporting to the Social Welfare Council (SWC).
19. If the organization receives unusually high-value in-kind donations (e.g., gold, luxury items, land, vehicles) that are difficult to trace, verify, or audit.
20. If NPOs are involved in organizing high-profile mass events with unclear sponsors or fund sources, especially in politically or socially sensitive regions.
21. If there is apparent misuse or misappropriation of domestic or international financial aid and emergency funding.
22. 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.
23. If the organization plans or commits act of terrorism, which may include the use of weapons of mass destruction and fosters extremism.
24. If the act of donor, beneficiaries or partner is found to be suspicious with the suspect of Money laundering or Terrorist financing.
25. If the organization has the donors from the countries identified as lacking appropriate anti-money laundering or counter terrorist financing regulation.
26. If the organization or its representatives are linked to third parties that support or are engaged in terrorist activity or procure dual-use equipment.
27. If the organization merges with another organization believed to support terrorist activities.

3.2.7 Trust (Guthi)

1. If previously inactive trust account is now used intensively without a plausible reason for such use.
2. If the purpose or motivation for establishing trust in Nepal is unconvincing or unclear.
3. If personal accounts of trustees or board members are used for digital fundraising linked with unexplained expenditures.
4. If the bank accounts of the organization are used by entity/person whose own accounts are under restrictions.

3.2.8 Approved Retirement Funds (also including EPF[1], CIT[2], SSF[3])

1. If large cash sums are deposited in a retirement fund by members, particularly when followed by substantial withdrawals of funds without a valid reason.
2. If the type or volume of the transaction is untypical of the client's economic activity and raises suspicion.
3. If an unrelated third party pays contributions on behalf of a member of the retirement fund.
4. If funds or assets deposited into a retirement fund do not align with the client's known financial profile, declared income, or typical contribution behavior.
5. If credible media reports link the client to illegal activity.
6. If a self-employed or unemployed person, or any third party on their behalf, makes usually high contributions to a retirement fund account.
7. If sudden contributions are made by the employee just before retirement age.
8. If a small or newly established organization makes unusually large contributions to employees' provident funds or retirement policies.
9. If significant inconsistencies are observed in the deposit amount and timing without valid reasons.
10. If the documentation is questionable (e.g. fake or unverifiable employment histories, forged KYC Documents, use of third-party accounts).

3.2.9 Casinos

1. If activities are inconsistent with the customer's profile.
2. If false identity is used to open and operate casino accounts.
3. If the client provides inconsistent identity information or refuses to provide required identification.
4. If client is known to have used multiple names.
5. If there is a dramatic or rapid increase in size and frequency of transactions.
6. If the client requests that a winning cheque be issued in the name of a third party.
7. If noticeable changes are observed in spending/betting pattern.
8. If clients request cheques not related to gaming winnings, often purchasing chips with large amounts of cash and then exchanging them for cheques at the end.
9. If a client purchases a large volume of chips with cash, participates in limited gambling

[1]Employees Provident Fund
[2]Citizen Investment Trust
[3]Social Security Fund

activity to create the appearance of significant gambling, and then cashes the chips for a casino cheque.

10. If the client purchases and cashes out casino chips with little or no gaming activity.
11. If the client shows no concern for winning or losing, but displays unusual interest in casino policies on payouts.
12. If client exchanges small denomination bank notes for large denomination bank notes.
13. If any deviation in transactions or suspicious activities is identified by casino business.
14. If funds are withdrawn from account shortly after being deposited.
15. If there is lack of proper sources of deposited amount.
16. If transactions involve PEPs and high net worth individuals who are linked to each other.
17. If players are from high-risk countries.

3.2.10 Dealers in precious metals and stones

1. If customers or their associates are linked to negative news, ongoing law enforcement investigations, or appear on sanctions lists.
2. If payments are received from or made to a third party who is not the actual buyer/seller or lacks a legitimate business purpose for being involved.
3. If multiple individuals are used to conduct transactions, often with amounts structured just below reporting thresholds.
4. If precious metals/stones are delivered to a third party who is not the owner or payer of the funds.
5. If customers are reluctant to provide identification documents or information about the source of funds or wealth.
6. If a customer shows excessive interest in AML/CFT policies and reporting thresholds.
7. If individuals or businesses make purchases or sales disproportionate to their typical business activity or stated purpose (e.g., a non-profit organization suddenly buying significant amounts of diamonds).
8. If there are significant deviations in pricing from market rates (e.g., over or under-invoicing).
9. If payments are made in large amounts of cash or through non-standard instruments such as third-party payments, traveler's cheques, or cashier's cheques.
10. If there is an unusual hurry to complete the transaction.
11. If a customer shows willingness to buy or sell at unusually high or low prices without negotiation.
12. If there are large or frequent transactions in foreign currency.

13. If the consignment size or type of precious metals/stones shipped appears inconsistent with the exporters' or importers' capacity.
14. If there are inconsistencies between transaction details and commercial invoices.
15. If goods described as scrap appear to be of higher quality—or vice versa.

3.2.11 Money Value Transfer Service (MVTS) / Remittance

1. If there is an unusual frequency of remittance transactions that does not align with the sender's known occupation or income level.
2. If the customer refuses to provide sufficient documentation or explanation for large-volume remittances to multiple unrelated beneficiaries abroad.
3. If third-party remittances are conducted through personal accounts with no clear relationship to the sender or receiver.
4. If the customer attempts to send money using different IDs or under different names at multiple locations.
5. If cash is deposited into the operating account by the agent without valid business justification.

3.2.12 Money Changers

1. If numerous agent locations are used for no apparent reason to conduct transactions.
2. If multiple low-value international funds transfers are carried out, possibly indicating a large amount of funds broken down into smaller amounts.
3. If several customers request transfers either on the same day or over a period of two to three days to the same recipient.
4. If the customer does not seem to know the recipient of the transfer.
5. If 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.
6. If the customer exchanges currency and requests the largest possible denomination bills in a foreign currency.
7. If the customer requests that a large amount of foreign currency be exchanged to another foreign currency.
8. If large amounts of currency are exchanged for traveler's checks.
9. If the customer exchanges small denominations of bills for larger denominations.
10. If the customer has limited knowledge of the payee's address or contact details, is reluctant to disclose this information, or requests the use of a bearer instrument.
11. If the customer instructs that funds be picked up by a third party on behalf of the payee.

12. If remittance or donation funds are received in a personal account, and the use of the funds is unclear — for example, if the funds appear to be intended for daily operations of institutions like a religious school.
13. If there are frequent international wire transfers from bank accounts that appear inconsistent with the stated business activities of the customer.
14. If there are frequent deposits by multiple individuals into a single bank account, followed by international wire transfers and /or international withdrawals through ATMs.
15. If there is a sudden change in pattern of financial transactions from low value international fund transfers to large value transfers by a money remitter.
16. If amount is being frequently credited in account of a person returned from foreign employment through wire transfer.
17. If money transfers business persons are found running other unrelated businesses simultaneously without clear justification.
18. If MVTSPs communicate only limited information about the customer& beneficiary in individual transactions, providing just enough detail to ensure delivery but not sufficient for due diligence.
19. If there are unusual transactions to a digital wallet account from multiple different wallet accounts without a clear business or personal rationale.
20. If online platforms are used for payment of trading transactions like PayPal balance, Bitcoin, etc.
21. If forged or suspicious identity documents are used, or the customer appears to be acting on behalf of another without a legitimate explanation.
22. If a customer requests currencies not commonly used locally or without a reasonable purpose (e.g., requesting Swiss Francs without a travel or business need).
23. If customers are overly anxious or refuse to answer simple questions, avoid or refuse to provide standard identification, provide suspicious documents, or if the same transaction type or amount is conducted by different people at different times (indicating possible structuring or mule activity).
24. If customers consistently mask their real location when conducting transactions through use of VPNs or proxy servers.
25. If there are spikes in transactions during late-night hours or weekends (non-business hours) without business justification, or if payments are initiated from sanctioned or FATF-blacklisted countries.

3.2.13 Trust or Company Service providers (TCSP)

1. If complicated legal or ownership structures are created without any legitimate economic or business reason.
2. If an intermediary is used in a transaction without a valid justification.
3. If funds are received from high-risk jurisdictions (e.g., countries with weak AML/CFT controls or under sanctions).
4. If the customer uses nominee directors or shareholders to conceal the true identity of the beneficial owner(s).
5. If the director or controlling shareholder(s) of a company cannot be located or contacted.
6. If the customer is unwilling to provide personal identification or details of the beneficial owner(s) of a trust or company.
7. If the source or destination of funds is unknown, unclear, or unverifiable.
8. If a customer conducts bulk transactions in cash without a clear and legitimate business purpose.
9. If a non-resident incorporates a company in a jurisdiction where they have no economic, social, or business ties.
10. If the money flow or financial activity of a company does not align with its stated business operations.
11. If the company claims to operate as a commercial business but cannot be found on the internet, social media, or professional directories.
12. If the business is registered at an address that does not match its profile or cannot be found on internet mapping services.
13. If the customer uses an email address with an unusual or suspicious domain (e.g., not tied to the claimed business or using free, obscure services).
14. If a customer uses multiple bank accounts without a valid economic or business reason.

3.2.14 Payment Service Provider (PSPs) and Payment System Operator (PSOs)

1. If multiple small value transactions are conducted within a short duration of account opening, or there is a large number of inbound or outbound low-value transactions that are inconsistent with customer's profile.
2. If the same IP address, device, or geo-location is used to access multiple accounts or phone numbers, or if an account is accessed from multiple IP addresses or geo-locations that are inconsistent with the customer's stated residence without proper justification.
3. If multiple accounts are accessed from a single device.

4. If multiple wallet accounts are created across different PSPs using the same mobile number but with different names.
5. If anonymization tools (e.g., Tor, VPN) are used to obscure origin.
6. If accounts are used frequently to fund or withdraw from online gambling or betting, especially when the account or associated mobile number is found listed on illicit websites such as *1xBet, Metabet, Fifiya*, etc.
7. If terms like *1xBet, Metabet, Himalbet, crypto, Hyper Fund* or other betting related-words appear in the description field during fund transfers.
8. If huge cash is deposited in the PSP's account held in bank by its agents without proper justification.
9. If dormant accounts suddenly show high activity or transactions.
10. If there is a rapid movement of funds through multiple wallets/accounts (layering).
11. If multiple accounts are used without clear business purpose.
12. If there is frequent use of cash-in and immediate cash-out services or frequent deposit in small size and withdraw in large amount without proper justification (indicative of mule accounts).
13. If there are frequent bank transfers to multiple bank accounts, especially originating from international IP addresses.
14. If there are unusual patterns of fund inflow and outflow involving specific, often repeated, and uncommon amounts.
15. If there is high volume of wallet-to-wallet transfers among multiple users, even if the amounts are small but occur numerous times.
16. If there is adverse media news about the customer.
17. If compliant is made by a bank or an individual regarding the account being used to receive fraud related transaction.
18. If transactions are related to crowd funding or donations without proper disclosures or accountability.
19. If high volume of transactions is processed by unregistered or seemingly suspicious merchants, such as a small auto workshop or grocery store *(kirana)* showing unusually high transaction spikes on certain days without a reasonable explanation.
20. If merchants are involved in high-risk sectors such as gambling, adult entertainment, gaming, or similar industries.
21. If merchant accounts used as a pass-through, meaning they process payments without actually delivering goods or services.

22. If transactions are conducted to or from high-risk or sanctioned countries, particularly in relation to remittance activities.
23. If there is a sudden change in transaction destination or source without business rationale.
24. If the customer has a high-risk profile (e.g. PEP or person from high-risk jurisdictions).
25. If a card-based wallet is used for loading funds followed by immediate cash-out.
26. If there are frequent reversals or refund requests on wallet or top-up transactions, suggesting attempts to confuse audit trails.
27. If the customer receives recurring micro payments from multiple random wallet IDs without known business activity.

3.2.15 Auditors and Accountants

1. If the client offers to pay unusually high fees for the auditing/accounting service.
2. If the auditing or accounting engagement is conducted remotely, and the client appears to avoid face-to-face meetings or is reluctant in providing relevant information.
3. If the clients appear to be acting on someone else's instructions i.e. there seems to be a hidden beneficial owner.
4. If the client receives unusual payments from unlikely sources which is inconsistent with their business.
5. If the entity makes large payments to its subsidiaries or other entities within the group that do not seem to have done within normal course of business.
6. If there is repeated transaction between parties over a period of time without valid reason.
7. If fictitious employees are created under payroll list.

3.2.16 Hire Purchase Companies

1. If a customer shows little interest in loan terms, interest rates, or repayment schedule, suggesting asset acquisition is not the true goal.
2. If the customer is a subject of negative/adverse news.
3. If there are any publicly available criminal records.
4. If suspicion arises due to complex ownership structures, or the possible use of shell companies or a recently formed company with no operational history or a non-existent business address.
5. If the business customer operates in unusual sectors or has an ambiguous or inconsistent business purpose.
6. If the business accounts show minimal legitimate business activity but regular large transactions.

7. If the assets financed are immediately resold or transferred, suggesting use for layering or integration.
8. If the individual and their family and associates are identified as PEPs.
9. If payments are split into multiple smaller transactions to stay under reporting limits or show unusual concern about threshold reporting or other reporting.
10. If a customer uses multiple bank accounts or financial instruments to make loan repayments.
11. If there are unexplained payments from third parties.
12. If a customer provides incomplete or inconsistent information or is reluctant to provide identity or financial documents.
13. If client's profession is non-income generating such as housewife, student, unemployed etc.
14. If frequent changes to the address, telephone/mobile no., address of office or authorized signatories is observed.
15. If lump-sum prepayment is made within a few months or within first year of availability of loan or sudden change in repayment behavior, such as a large lump-sum repayment after missed payments.
16. 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).
17. If the down payments or repayments are made in large amounts, particularly when inconsistent with the customer's income profile, financial ability, profession and business as per the declaration.
18. If a customer suddenly repays a problematic loan unexpectedly without a valid reason.
19. If funds transferred from high-risk jurisdictions or tax havens to settle the loan or pay off early.
20. If there are attempts to disguise the real owner of the asset (i.e. vehicle).
21. If there are frequent changes in the underlying asset/collateral.

3.2.17 Automobile Selling Companies

1. If individuals with no visible means of support purchase luxury vehicles without a clear source of funds or legitimate income.
2. If high-value vehicles are exported soon after purchase to high-risk or non-cooperative jurisdictions.
3. If a customer frequently buys and resells vehicles within short periods, possibly as a layering technique.

4. If the vehicle is paid for by someone other than the buyer, especially with no apparent relationship between them.
5. If a customer frequently pays for vehicles with large amounts of cash, especially when the transaction does not match their financial profile.
6. If same individual or related parties purchase several vehicles in a short timeframe, sometimes with minimal negotiation.
7. If there are repeated payments just below the threshold for mandatory reporting (structuring/smurfing).
8. If buyers use newly formed or inactive companies to purchase vehicles without clear business rationale.
9. If the sale prices are significantly over- or under-valued compared to market prices, with the difference potentially laundered.
10. If complex, complicated, or third-party financing structures are used that are not in line with the customer's credit profile.
11. If a customer shows little interest in the vehicle's condition, price, or features—suggesting the car is merely a medium for moving funds.
12. If customer provides inconsistencies or falsified documents (IDs, proof of income, address), or shows reluctance to provide complete information.
13. If customer shows reluctance to use traditional banking methods and prefers cash or other non-traceable means.

3.2.18 Lawyers / Notaries

a) Client Behavior and Instructions

1. If the client refuses to provide complete information, including identity, purpose of transaction, or beneficial ownership.
2. If the client seeks anonymity, uses aliases, or insists on unusual secrecy or avoidance of documentation.
3. If the client is unusually defensive or evasive when asked about the source of funds.
4. If the client provides information that seems false, inconsistent, or cannot be verified through normal means.

b) Transaction Characteristics

5. If the size, complexity, or frequency of transactions is not consistent with the client's known legal, commercial, or personal profile.
6. If the client requests legal structuring that appears intended to conceal ownership, obscure source of funds, or avoid disclosure obligations.

7. If the client proposes to pay for legal services using large amounts of cash or virtual-currency, especially for activities where such methods are not typical.
8. If the client shows an interest in tokenization, offshore incorporation, or digital fundraising without clear justification.

c) Nature of Legal Service Requested

9. If the client seeks to form multiple legal entities, trusts, or foundations with no clear economic or philanthropic purpose.
10. If the client requests services to buy/sell high-value assets (e.g., land, art, vehicles) in rapid succession or without logical business reasoning.
11. If asked to hold or transfer client funds in a way that doesn't correspond to any legal case or contractual obligation.
12. If the client insists on using the lawyer's client account as a conduit for third-party transactions or structuring payments to multiple recipients.

d) Involvement of High-Risk Elements

13. If the transaction involves PEPs (Politically Exposed Persons), sanctioned individuals, or jurisdictions with weak AML/CFT controls.
14. If the legal structure appears designed to evade regulatory oversight, defraud creditors, or obscure ownership for illicit reasons.
15. If the legal services requested are linked to high-risk sectors such as gambling, unregulated virtual currency exchanges, or foreign donations without authorization.

e) Unusual Use of Legal Privilege

16. If the client insists on using legal privilege to shield suspicious financial arrangements, especially when not genuinely related to legal advice or litigation.
17. If the lawyer is being used to interpose a layer of confidentiality between suspicious activity and scrutiny by financial or government institutions.

3.3 INDICATORS RELATED TO PREDICATE OFFENCES AND OTHER LAWS

If it is evident that the asset is earned from the predicate offences as per ALPA, 2008 and/or linked with 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.

We have listed possible red flags related to major predicate offences and/or liked with offences under the major prevailing laws, as below: -

3.3.1 Hundi/Illegal MVTS

1. If funds are regularly deposited into an individual's account followed by immediate cash withdrawals or transfers, with no economic justification.

2. If an individual routinely deposits cash into various accounts maintained across different branches of the same or multiple BFIs on a daily basis.
3. If cash is deposited into a personal account, and subsequently, these funds are digitally transferred to multiple distinct bank accounts.
4. If consistent cash deposits are observed in accounts belonging to remittance companies and PSPs. These deposits originate from various sources, including remittance agents and individual depositors.
5. If a remittance receiver acknowledges receipt of funds purportedly sent from foreign countries; however, investigations reveal that the originating cash deposit for these funds occurred domestically.
6. If individuals in Nepal receive large remittance amounts through unofficial channels (e.g., hand-delivered cash) and no record exists in the formal banking system.
7. If a remittance agent or individual is operating without registration from NRB and still facilitates cross-border transfers.
8. If the same beneficiary receives frequent low-value remittances from different senders in short intervals (structuring/smurfing), particularly in rural or border areas.
9. If individuals in Nepal claim remittance without being able to identify or explain the relationship with the sender abroad.
10. If there is a mismatch between an individual's income or occupation and the volume of foreign currency received (e.g., students or housewives receiving large foreign remittances).

3.3.2 Fraud and Cyber Enabled Fraud

1. If an account shows frequent or immediate transactions soon after opening that are inconsistent with the stated purpose of the account, or if abnormal activity is observed in bank accounts or wallets, including transactions with persons suspected of online gambling or illegal virtual asset dealings.
2. If immediate cash withdrawals or large transfers are made following the receipt of funds, consistently keeping the account balances near zero.
3. If frequent and large transactions occur that are inconsistent with the account holder's economic profile such as sudden international transfers or cash withdrawals using cards at border cities in India.
4. If digital transactions are being performed frequently in accounts of illiterate persons or to persons with low knowledge of digital payment methods.
5. If small payment is initially made to a beneficiary, and once successfully completed, it is rapidly followed by larger value payments to the same beneficiary.

6. If regular small-value debit transactions are conducted to check whether an account is frozen, indicating that the sender may change the destination account if freezing occurs or if common wallet accounts or mobile numbers are frequently loaded or topped up from mobile banking accounts.
7. If a customer consistently reaches the maximum ATM cash withdrawal limit on a card on a regular basis, without a clear business or personal justification.
8. If the user is seen accompanied by another individual (by being physically present or communicating over the phone) during transaction as observed by bank staffs or through Closed Circuit Television (CCTV) footage.
9. If transaction remarks for account transfers contain different language, timing, or amounts than previous transaction patterns, especially when they include language suggesting urgency or confidentiality, indicating possible covert instructions or illicit fund movement.
10. If a customer presents poorly formatted messages/emails with spelling and/or grammar mistakes as justification of a transaction.
11. If the beneficiary's account information differs from what was previously used, the name mentioned in the transaction description does not match the actual account holder at the beneficiary bank, indicating possible use of proxy or mule accounts.
12. If transactions are carried out repeatedly with same remarks such as Payment, Borrowings etc.
13. If RE is unable to contact the account holder or faces non-co-operation during Customer Due Diligence (CDD), indicating potential intent to avoid identification or monitoring.
14. If the account holder is accompanied and assisted by an unrelated person during account opening, and appears unaware of the source of funds or acts on behalf of another individual, suggesting possible use of a proxy or mule account.
15. If the customer displays inadequate knowledge about the nature, amount, or purpose of transactions, and provides unrealistic or inconsistent explanations, suggesting that the customer may be acting as a money mule.
16. If a seemingly illiterate person subscribes to advanced digital payment products like mobile banking, internet banking, connectIPS, or wallets.
17. If the customer is completely unaware of the purpose of the transaction.
18. If the account holder attempts to hide their identity by using shared, falsified, stolen, or altered identification (e.g., address, telephone number, email), or if the phone numbers provided during account opening are unreachable.
19. If the email address appears incompatible with the name of the account holder or seems to belong to another person, or if similar email patterns are observed across

multiple accounts, including the same mobile number, email, or other credentials being shared by two or more account holders.

20. If IP addresses or GPS coordinates originate from other jurisdictions, or if there is use of Virtual Private Networks (VPNs) to mask the user's IP address; or if multiple IP addresses or electronic devices are associated with a single online account; or if a single static IP address or electronic device is associated with multiple accounts of various account holders.
21. If the user's audit trail shows multiple failed transaction attempts before a successful transaction, or if multiple successful transactions are followed by another successful transaction in a suspicious pattern.
22. If there is adverse media or negative news on the customer or counterparties, such as the account being linked to a known scammer, money mule, or someone involved in identity takeover activity.
23. If there is a fraud report or a wire transfer recall request received from a correspondent institution.
24. If there is presence of adverse information provided by FIUs or LEAs about persons involved in a transaction.

3.3.3 Virtual Assets

1. If large transactions that are inconsistent with the customer's profile are followed by rapid deposits or withdrawals.
2. If there is frequent movement of funds into and out of wallets with no clear economic or business purpose.
3. If large transactions appear to be structured or broken down into smaller amounts, often just below reporting or record-keeping thresholds.
4. If multiple accounts are conducting transactions within a short period without a logical or legitimate business explanation.
5. If an account is used to send or receive Crypto currency from multiple countries, including high-risk jurisdictions or countries subject to international sanctions.
6. If funds originate from or are sent to unknown or non-identifiable individuals or entities.
7. If transactions are associated with dark web markets, ransom ware, or known scams.
8. If transactions are linked to high-yield investment programs that promise unusually high or guaranteed returns using Crypto currency.
9. If there is evidence of aggressive marketing or solicitation of investment schemes, particularly those offering unrealistic returns or lacking regulatory approval.

10. If entities are operating an exchange or wallet service without proper registration or licensing.
11. If transactions involve sanctioned entities or individuals, or those listed on international watch lists.
12. If transactions are conducted with service providers that lack proper Customer Due Diligence (CDD) or Know Your Customer (KYC) processes.
13. If multiple accounts are created under different names or IP addresses to bypass restrictions.
14. If transactions originate from suspicious or sanctioned IP addresses.
15. If there are frequent account access attempts from different IP addresses.
16. If there are frequent changes in identification information of the customers, such as email address, IP address, linked bank accounts, or wallet addresses.
17. If the customers cannot explain source of funds or purpose of transaction and refuse to answer basic compliance questions.
18. If multiple fund transfers between accounts include the term "crypto" in the transaction remarks.
19. If a customer declares income from “freelancing" or "digital marketing,” but the funds are routed from crypto-related wallets or P2P exchanges.
20. If funds are received from individual or entity accounts with references to crypto assets or Virtual Asset Service Providers (VASPs), and those funds are immediately moved to another account maintained at other banks.
21. If incoming transactions are received from several unrelated wallets in relatively small amounts, followed by subsequent transfers to another wallet, especially when such transactions are carried out by a number of related accumulating accounts that may initially use crypto assets.
22. If the SWIFT message fields contain language indicative of the transaction being conducted in support of illicit activity or for the purchase of crypto assets.

3.3.4 Corruption and bribery

1. If transactions are inconsistent with the known source of income of a politically exposed person (PEP).
2. If customer classified as PEP deposits large cash amounts inconsistent with their declared salary and job responsibilities.
3. If unusual transactions are conducted involving current or former PEPs without a clear source of funds or a legitimate purpose for the transaction.
4. If transaction description field includes words like advisory fee, donation, commission,

service charge, advance payment, gift or approval charge, especially when funds are deposited into a PEP's account by a third party.

5. If transactions are conducted in the immediate family member of PEP without proper justification.
6. If frequent deposits are made from government-linked accounts without corresponding business activities.
7. If an amount is received from consumer groups (*Upabhokta Samiti)* in the PEP's account including their spouse and personal accounts.
8. If unexplained amounts are received from foreign jurisdiction without proper justification in accounts of PEPs.
9. If intermediaries or shell companies are used to obscure the identity of final beneficiaries.

3.3.5 Tax evasion

1. If large or frequent cash transactions are observed that are not aligned with the nature of the business.
2. If there are significant discrepancies between declared income and actual lifestyle or assets.
3. If multiple bank accounts are used or transactions are layered to conceal audit trails.
4. If fake or inflated invoices and receipts are submitted to reduce taxable income.
5. If transfers are made to or received from tax havens without clear economic justification.
6. If shell companies or nominee shareholders/directors are used to hide the true ownership or control of assets or accounts.
7. If goods and services are misclassified, under-invoiced, or over-invoiced in customs or accounting records without legitimate justification.
8. If assets are frequently bought and sold in a manner inconsistent with the customer's declared income sources.
9. If a customer or business lacks proper or complete accounting records and financial statements.
10. If there are delayed, incomplete, or missing tax filings without reasonable cause.
11. If there is refusal or delay in providing documents during tax audits or investigations.
12. If complex ownership structures are used with unclear ultimate beneficial owners.
13. If donations or sponsorships made by an entity or an individual are disproportionate to declared income.
14. If transactions are structured to avoid reporting thresholds (Structuring).

3.3.6 Trade Based Money Laundering

(Some of the indicators of trade based money laundering have been adapted from FATF's Trade Based Money Laundering Indicators)

1. If the customer submits fake documents or engages in false reporting, such as commodity misclassification, commodity over- or under-valuation, or double-invoicing.
2. If fraudulent trade circuits are identified, such as exporters claiming duty drawback on inflated export bills or for non-existent imports.
3. If no goods are shipped and all documentation is completely falsified to move funds in the guise of trade (Phantom Shipping).
4. If shipping of products of no value as a saleable good.
5. If the corporate structure of a trade entity appears unusually complex and illogical, such as the involvement of shell companies or companies registered in high-risk jurisdictions.
6. If a trade entity is registered or has offices in a jurisdiction with weak AML/CFT compliance.
7. If a trade entity is registered at an address that is likely to be a mass registration address, e.g. high-density residential buildings, post-box addresses, commercial buildings or industrial complexes, especially when there is no reference to a specific unit.
8. If the business activity of a trade entity does not appear to be appropriate for the stated address, e.g. a trade entity appears to use residential properties, without having a commercial or industrial space, with no reasonable explanation.
9. If a trade entity lacks an online presence or the online presence suggests business activity inconsistent with the stated line of business, e.g. the website of a trade entity contains mainly boilerplate material taken from other websites or the website indicates a lack of knowledge regarding the particular product or industry in which the entity is trading.
10. If a trade entity displays a notable lack of typical business activities, e.g. it lacks regular payroll transactions in line with the number of stated employees, transactions relating to operating costs, tax remittances.
11. If the owners or senior managers of a trade entity appear to be nominees acting to conceal the actual beneficial owners, e.g. they lack experience in business management or lack knowledge of transaction details, or they manage multiple companies.
12. If a trade entity, or its owners or senior managers, appear in negative news, e.g. past money laundering schemes, fraud, tax evasion, other criminal activities, or ongoing or past investigations or convictions.
13. If a trade entity maintains a minimal number of working staff, inconsistent with its

volume of traded commodities.

14. If the name of a trade entity appears to be a copy of the name of a well-known corporation or is very similar to it, potentially in an effort to appear as part of the corporation, even though it is not actually connected to it.
15. If a trade entity has unexplained periods of dormancy.
16. If an entity is not compliant with regular business obligations, such as filing VAT returns.
17. If trade activity is inconsistent with the stated line of business of the entities involved, e.g., a car dealer is exporting clothing or a precious metals dealer is importing seafood.
18. If a trade entity engages in complex trade deals involving numerous third-party intermediaries in incongruent lines of business.
19. If a trade entity engages in transactions and shipping routes or methods that are inconsistent with standard business practices.
20. If a trade entity makes unconventional or overly complex use of financial products, e.g. use of letters of credit for unusually long or frequently extended periods without any apparent reason, intermingling of different types of trade finance products for different segments of trade transactions.
21. If a trade entity consistently displays unreasonably low profit margins in its trade transactions, e.g. importing wholesale commodities at or above retail value, or re-selling commodities at the same or below purchase price.
22. If a trade entity purchases commodities allegedly on its own account, but the purchases clearly exceed its economic capabilities, e.g. the transactions are financed through sudden influxes of cash deposits or third-party transfers to the entity's accounts.
23. If a newly formed or recently re-activated trade entity engages in high-volume and high-value trade activity, e.g. an unknown entity suddenly appears and engages in trade activities in sectors with high barriers to market entry.
24. If there are inconsistencies across trade documents (e.g., contradictions between the name of the exporting entity and payment recipient; differing prices on invoices and contracts; or discrepancies in quantity, quality, volume, or value of commodities described).
25. If contracts, invoices, or other trade documents show fees or prices that are inconsistent with commercial norms, deviate significantly from market value, or fluctuate unusually compared to previous comparable transactions.
26. If contracts, invoices, or other trade documents contain vague or generic descriptions of traded commodities, lacking specific details about the goods involved.
27. If trade or customs documents supporting a transaction are missing, counterfeit, contain false or misleading information, are resubmissions of previously rejected documents, or

are frequently modified or amended.

28. If contracts supporting complex or regular trade transactions appear unusually simple, such as resembling generic "sample contract" templates found online.
29. If the value of the registered imports of an entity significantly mismatches with the volume of its foreign bank transfers for imports, or if registered exports significantly mismatch with incoming foreign bank transfers.
30. If commodities imported under temporary importation or inward processing regimes are later exported using falsified documents.
31. If shipments of commodities are routed through a number of jurisdictions without economic or commercial justification.
32. If a trade entity makes very late changes to payment arrangements for a transaction, e.g. the entity redirects payment to a previously unknown entity at the very last moment, or the entity requests changes to the scheduled payment date or payment amount.
33. If an account displays an unexpectedly high number or value of transactions that are inconsistent with the stated business activity of the client.
34. If an account of a trade entity appears to be a "pay-through" or "transit" account with a rapid movement of high-volume transactions and a small end-of-day balance without clear business reasons, including:
    a. If an account displays frequent deposits in cash which are subsequently transferred to persons or entities in free trade zones or offshore jurisdictions without a business relationship to the account holder.
    b. If incoming wire transfers to a trade-related account are split and forwarded to non-related multiple accounts that have little or no connection to commercial activity.
35. If the payment for imported commodities is made by an entity other than the consignee of the commodities with no clear economic reasons, e.g. by a shell or front company not involved in the trade transaction.
36. If cash deposits or other transactions of a trade entity are consistently just below relevant reporting thresholds.
37. If transaction activity associated with a trade entity increases in volume quickly and significantly, and then becomes dormant after a short period of time.
38. If payments are sent or received in large round amounts for trade in sectors where such transactions are unusual.
39. If payments are routed in a circle – funds are sent out from one country and received back in the same country, after passing through another country or countries.

40. If a business involved in portable or handheld electronics, construction materials, plant and machinery, scrap metal, fuel and energy products, or alcoholic and soft drinks is suspected of mischaracterizing goods to circumvent controls or commit other customs and tax violations.
41. If a new supply chain and related financial intermediaries are developed in a sector where no pre-existing commodity supply chain existed to exploit.
42. If the name of importer and exporter is the same without proper justification such as being subsidiaries, joint ventures, or having another legitimate relationship.
43. If Documents Against Acceptance (DAA) remain unsettled for many days beyond the agreed payment terms.
44. If trade in services or other intangibles is used to disguise and justify the movement of illicit proceeds.
45. If goods that are difficult for authorities to examine and have dual uses (e.g. hazardous materials, chemicals, poisonous substances, inflammable items, etc) are traded.
46. If relaxations in laws or import restrictions for necessary medical equipment and medicines are misused or exploited.
47. If the 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.
48. If goods not produced domestically are exported, indicating possible transshipment (e.g. export of used vehicles to developed countries from Nepal).

3.3.7 Misuse of Legal Persons/Legal Arrangement

1. If the legal person, its beneficial owner, or key associates have links to high-risk or sanctioned jurisdictions, or appear on terrorism financing or international sanction lists.
2. If transactions occur with, or invoices are received from, entities in offshore jurisdictions known for secrecy, weak AML controls, or tax havens, especially when such dealings lack economic rationale.
3. If unnecessarily complex company structures are used that obscure the identity of the beneficial owner or are not consistent with the scale or nature of the business.
4. If multiple companies are registered with the same address, contact details, or beneficial owners without a legitimate business explanation.
5. If there is an inability to verify, or inconsistencies in, the relationships between the beneficial owner, directors, authorized signatories, or employees.
6. If a long-dormant legal entity suddenly becomes active with a high volume of financial transactions that do not align with its prior or declared business profile.

7. If frequent transactions occur that are inconsistent with the nature of the business, such as high cash volumes in non-cash industries, structured payments below reporting thresholds, or round-tripping.
8. If suspicious, altered, or forged identity or incorporation documents are submitted during on boarding or KYC/EDD processes.
9. If business and personal accounts or transactions are mixed without a clear and legitimate explanation, suggesting attempts to disguise the source of funds.
10. If frequent or large transactions occur with entities sharing the same beneficial owner or with no obvious commercial relationship, possibly indicating layering or trade-based money laundering.

3.3.8 Human Trafficking/Human Smuggling

1. If a customer is always accompanied by another person who appears to control them, speaks for them, or prevents them from speaking freely (potential victim under coercion).
2. If there is any adverse media or public information linking the customer or associated parties to human trafficking, smuggling, or related criminal activities.
3. If transactions involve countries or regions identified as sources, transit points, or destinations for human trafficking or smuggling.
4. If customers pay large sums to unknown third parties or intermediaries.
5. If a transaction is inconsistent with the customer's known profile or business activities.
6. If customers show reluctance or refusal to provide identification or submit incomplete/inconsistent documentation.
7. If customers appear nervous, fearful, or hesitant during transactions.
8. If multiple transfers of small amounts occur to or from high-risk countries.
9. If frequent cash deposits or withdrawals occur in amounts just below reporting thresholds (structuring).
10. If customers use multiple or forged identification documents.
11. If remittance or money transfer services are used for sending funds to or from regions known for trafficking.

3.3.9 Cross- border Crimes

1. If there are frequent or large inflows/outflows of funds from high-risk or sanctioned jurisdictions without a clear business or personal reason.
2. If the customer is known or suspected to be linked to human trafficking, drug trafficking, or smuggling networks.

3. If repeated transactions occur with individuals/entities in conflict zones, sanctioned, or non-cooperative countries.
4. If funds are transferred through shell companies, trusts, or offshore accounts with no identifiable beneficial owner.
5. If multiple countries are used in a transaction chain with no economic or business rationale.
6. If transactions are structured to avoid reporting thresholds across multiple jurisdictions.
7. If money mules are used to move funds across borders in small amounts.
8. If border towns or regions known for smuggling or trafficking routes are involved in transactions.
9. If ransom payments are made within the home country on behalf of individuals located in a foreign jurisdiction.
10. If suspicious movements of cash, gold, or bearer instruments occur across borders.
11. If there are regular cross-border cash declarations near threshold amounts.
12. If incoming funds are labeled as "investment," "loan," or "gift" without supporting documentation.
13. If transactions involve unrelated third parties or entities not known to the customer.
14. If fraud is committed in a foreign country using remote access or other methods, with proceeds transferred subsequently to the home country.
15. If the customer provides inconsistent or vague explanations about business activities in foreign countries.
16. If the customer shows reluctance to provide information about foreign business dealings or sources of funds.
17. If the customer shows undue interest in cross-border transaction thresholds or AML policies.
18. If there is evidence or suspicion of Trade Based Money Laundering (TBML).

2.3.10 Environment Related Crimes

1. If there is unusual financial activity for a nature-based business (e.g., large cash deposits or wire transfers, frequent cross-border transactions) that does not match the scale or nature of the business.
2. If trade-based red flags are observed, such as inconsistent or forged customs documents, under-invoicing or over-invoicing, or payments to/from unknown third parties.

3. If transactions or business activities involve high-risk sectors or locations, such as protected areas, buffer zones, or high-deforestation regions.
4. If an account is linked to unregulated mining operations (e.g., sand, gravel, or riverbed stone extraction).
5. If there is a lack of, or expired, environmental permits, forestry licenses, or mining certificates.
6. If front companies or shell firms are repeatedly used to hold environmental permits.
7. If firms suddenly diversify into wildlife or timber trading without any prior history in those sectors.
8. If politically exposed persons (PEPs) or government officials are involved in environment-linked businesses.
9. If legal professionals or intermediaries are used to shield ownership of land, extraction rights, or environmental permits.
10. If there is rapid and unexplained wealth accumulation by individuals working in forestry, national parks, or border trade.
11. If common containers, consignees, transporters, clearing agents, or exporters are used repeatedly, as seen in other suspected illegal wildlife trade cases.
12. If shipments of legal wildlife (fauna and flora) come with anomalous, incomplete, or suspicious CITES certificates (Convention on International Trade in Endangered Species).
13. If transactions use names of ingredients or products in the traditional medical trade that refer to CITES species.
14. If bills of lading are switched by traders previously implicated in criminal activity involving wildlife trafficking or trade fraud investigations.
15. If payments for wildlife shipping are masked as payments for gold or to gold trading businesses.
16. If transactions occur between licensed pet shop suppliers/breeders and known wildlife poachers or traffickers.
17. If international wire transfers from known wildlife traffickers are sent to relatives' accounts as tuition, allowance, or family support payments.

3.3.11 Foreign Exchange Abuse

1. If there are large or frequent foreign exchange transactions with no clear business purpose.
2. If transactions are inconsistent with the customer's known business or financial profile.

3. If cross-border forex transactions are linked to countries known for money laundering or terrorist financing risks.
4. If offshore accounts or shell companies are used to conduct forex transactions.
5. If multiple currency conversions occur within a short time period, especially involving high-risk jurisdictions.
6. If forex trades are structured to avoid regulatory reporting thresholds.
7. If funds are routed unusually through multiple foreign exchange deals or intermediaries.
8. If there are requests to convert cash proceeds into foreign currency without clear justification.
9. If documentation supporting forex transactions is inconsistent or incomplete.
10. If there is reluctance or refusal to provide information or identification during forex dealings.
11. If frequent amendments or cancellations of forex contracts occur, suggesting attempts to obscure transactions.
12. If transactions take place at exchange rates significantly above or below the market rate.
13. If sudden spikes in foreign exchange trading volume occur without a clear reason.

3.3.12 Undue Transactions

1. If the customer is reluctant to provide complete KYC information.
2. If false identities or inconsistent personal data are used.
3. If the customer shows unusual nervousness or evasiveness when questioned about transactions.
4. If the customer is overly secretive or protective about business or source of funds.
5. If structuring (smurfing) is used to break large amounts into smaller ones to avoid reporting thresholds.
6. If sudden and unexplained large deposits occur that are inconsistent with the customer's profile.
7. If frequent cash transactions occur without a valid business purpose.
8. If transfers happen between unrelated accounts with no clear reason.
9. If round-number transactions occur repeatedly (e.g., Rs. 999, 1,000, 10,000 multiple times).
10. If transactions are made to or from high-risk or sanctioned jurisdictions.
11. If frequent cross-border transfers occur without logical business reasons.
12. If offshore accounts in secrecy jurisdictions are used.

13. If dormant accounts suddenly become active with large transfers.
14. If accounts show high-volume activity but low balance retention.
15. If repeated early withdrawals occur shortly after large deposits.
16. If third-party transactions occur where the origin or beneficiary is unrelated to the customer.
17. If there is a mismatch between declared business and transaction volume.
18. If companies have no physical presence or online footprint.
19. If shell companies or trusts with unclear ownership are used.
20. If complex company structures are overused without a valid business rationale.

3.3.13 Match Fixing

1. If large amount gets deposited into the accounts of players and sports clubs, sports officials and their relatives just before and after the sports events without proper sources.
2. If players get sponsorship and financial supports with huge amount from the betting companies.
3. If the payments without proper reason and purpose made to agents involved in player transfer and match arrangements.
4. If huge cash deposits or withdrawals are made by players or officials and their relatives immediately before or after suspicious matches.
5. If multiple small cash transactions just below the threshold transaction report (TTR) are made by players, officials or club officials to conceal the detection of ML.
6. If property, precious metals with high value are purchased by players, officials or club officials using cash without proper income sources.
7. If players, officials or club officials do not want to provide detailed information regarding account opening, high amount deposit and payment with no proper purpose.
8. If fake or unverifiable documents are presented or submitted by players, officials or club officials to open accounts.
9. If any unusual performance by the players, and ampere or referee is observed or noticed.
10. If a match is unexpectedly won or lost.
11. If there is doubtful player selection, auction processes, or match arrangements.

3.3.14 Sexual Exploitation Including Sexual Exploitation of Children

1. If orphanages, shelters, or NGOs receive large or frequent foreign donations with little transparency and provide minimal supporting documentation.

2. If frequent international wire transfers occur from/to high-risk or known trafficking/child exploitation jurisdictions.
3. If bank or mobile wallet accounts held by minors receive frequent deposits from unknown or foreign sources.
4. If repeated transactions come from different senders to the same child or caregiver.
5. If the transaction description field includes words like “gift,” “support,” “love,” or ambiguous nicknames—especially when sent to minors.
6. If there are regular transfers from adult foreign nationals to children or youth in rural or tourist-heavy areas.
7. If cash withdrawals occur soon after receiving donations, particularly when funds are not used for documented educational or health expenses.
8. If adults make regular payments to minors or young individuals without justified familial relationships.
9. If unaccompanied minors frequent financial institutions making large cash withdrawals or deposits.
10. If transactions are linked to hotels, travel, or lodging, often involving minors or individuals with minimal income.
11. If individuals claiming to be in the modeling, entertainment, or massage industry have large unexplained income.
12. If frequent transactions occur with adult websites, escort services, or content subscription platforms.

3.3.15 Narcotic Drugs and Psychotropic Substances

1. If there are discrepancies between the stated source of income and the actual transaction patterns of the customer.
2. If cash-intensive businesses (e.g., nightclubs, massage parlors) or NGOs are used as fronts for channeling funds abroad or supporting drug trafficking activities.
3. If there is sudden, unexplained movement of funds to/from high-risk countries known for drug production or trafficking.
4. If transactions involve countries identified by the UNODC or FATF as major drug-producing or trafficking regions.
5. If there is negative news or public information linking the customer or their associates to criminal activity, especially drug-related offenses.
6. If deposits are made in multiple locations over a short period and frequent international wire transfers occur without legitimate purpose.

7. If payments are made by or to unrelated third parties without a clear business relationship.
8. If businesses have minimal legitimate operations but high cash flows.
9. If companies in unrelated industries transact frequently with each other with huge amounts of advance payments.
10. If there is refusal or hesitation to provide complete KYC documentation.
11. If customers are unable to explain the nature of their business or transactions.
12. If customers frequently travel to drug-producing or transit countries with no clear reason.
13. If shipments are routed through known drug-trafficking regions with no logistical rationale.
14. If trade documents and transactions are manipulated to disguise illicit funds through over- or under-invoicing, multiple invoicing, significant price deviations, or falsely described goods.
15. If multiple bank accounts are opened and closed within a short period.
16. If transactions involve numerous third parties who appear unrelated to the customer's legitimate business or personal profile.
17. If cash deposits occur in locations where the customer does not reside or conduct business, or multiple deposits come from foreign nationals or border areas without plausible reasons.
18. If foreign currency exchanges by non-residents occur over short periods, especially through non-banking remittance systems.
19. If frequent large transactions occur through money transmitters and currency exchange companies with less stringent AML/CFT controls.

3.3.16 Lottery, Gambling, Donation Related

a) Lottery Related

1. If a lottery win is declared without actually winning (false claim of winning).
2. If a single person or members of the same household receive unusually large amounts from lottery winnings.
3. If lottery results are manipulated or rigged in a planned or coordinated manner.
4. If a large number of lottery tickets are purchased or exchanged excessively.
5. If the claimed lottery winnings are unusually high and inconsistent with normal payout amounts.

b) Gambling Related

6. If the customer's identity is unclear, and their financial activity appears unusual or inconsistent.
7. If funds are deposited and immediately converted to casino credit or withdrawn without genuine gambling.
8. If there are repeated cash transactions that exceed normal gambling behavior.
9. If chips or tokens are bought and exchanged without actual gaming activity.
10. If multiple exchanges occur in a short timeframe without significant play.
11. If customer requests for credit transfers to others or use of proxies to buy chips/tokens.
12. If a person engages in high-stakes gambling without a visible source of wealth, or is listed on a sanctions list.

c) Donation Related

13. If the true beneficial owner or controller of the funds is not clearly identified.
14. If the organization or individuals involved are listed on UN or other international sanctions lists.
15. If donors' identities are unknown or unverifiable, and a high volume of anonymous donations is observed.
16. If funds collected through donations are transferred abroad without a clear or legal purpose.
17. If the majority of donations are received in cash, raising concerns about traceability.
18. If collected funds are deposited into savings accounts of unknown individuals instead of organizational accounts.
19. If individuals receiving high compensation from publicly raised donations or aid have unclear or suspicious tax status.
20. If the charity runs multiple mobile wallet accounts for fund collection that are not disclosed in registration records.
21. If unusual or excessive operational expenses occur, such as salaries or administrative costs that appears disproportionate.
22. If educational institutions receive bulk foreign donations but show minimal student or teaching activity.
23. If temples or monasteries receive consistent cash deposits from unrelated donors without disclosure of purpose.

3.3.17 Terrorist Financing and Proliferation Financing (TF/PF)

1. If the client is linked to terrorist activities or proliferation financing.
2. If any person or entity is involved in providing, receiving, collecting, or arranging funds, whether from legitimate or illegitimate sources, directly or indirectly, to carry out terrorist activities or proliferation of weapons of mass destruction.
3. If the customer is linked to illicit trafficking of arms, ammunition, nuclear, chemical, biological weapons, related materials, or their means of delivery.
4. If it is evident that assets are earned from offenses relating to arms and ammunition under prevailing law.
5. If transactions involve certain high-risk jurisdictions such as locations in or near armed conflict zones where terrorist groups operate or jurisdictions with weak ML/TF controls.
6. If amounts are received from high-risk jurisdiction countries without proper justification.
7. If an I/NGO receives funds for welfare but uses them in illegal radicalization that may lead further to terrorist activities.
8. If donations are raised in an unofficial or unregistered manner, and the ultimate use is unclear.
9. If transactions involve individuals or entities identified by media and/or sanctions lists as linked to terrorist organizations or activities.
10. If law enforcement information indicates individuals or entities may be linked to terrorist organizations or activities.
11. If clients are identified by media or law enforcement as having traveled, attempted to travel, or intended to travel to high-risk jurisdictions, especially conflict or terrorist-supporting areas.
12. If clients conduct travel-related purchases (airline tickets, visas, passports) linked to high-risk jurisdictions.
13. If an individual or entity's online presence supports violent extremism or radicalization.
14. If a client donates to a cause subject to publicly available derogatory information (e.g., crowd funding, charities, NGOs).
15. If dual-use goods are received or imported for manufacturing weapons of mass destruction.
16. If use of the social media, instant messaging applications and streaming platforms (SMSPs) economy for fundraising campaigns,
17. If use of fake charities and/or humanitarian campaigns,
18. If sale of goods/services to raise funds for violent extremism
19. If suspicious promotion of crowdfunding campaigns,

20. If use of vulnerable and obscure in-app payments of digital wallets,
21. If suspicious instruction and/or coordination of VAs transactions
22. If using vulnerable mobile payment apps or mobile money services, In-app payment tools, pre-paid cards or gift vouchers.
23. If payments to vulnerable and obscure type-photo and media sharing platforms
24. If payments to and from microblogging, discussion platforms and peer to peer lending platforms.
25. If payments to and from obscure and vulnerable online marketplaces, social commerce apps where social interaction is integrated with e-commerce and payments.
26. If payments to and from obscure and vulnerable Gaming/chat applications (with build-in chats): gaming environments with social features, virtual goods, and payment systems (i.e., Discord, Roblox, Fortnite)
27. If payments to and from obscure and vulnerable Creator economy/ subscription-based content platforms enable creators (influencers, artists, adult content providers, educators, etc.) to monetize their audience directly through subscriptions, tips, and pay-per-view content and often integrate payment systems (credit cards, digital wallets, crypto in some cases) (i.e., Buy Me a Coffee, Only Fans, Patreon)
28. If payments which can be linked to Large-networked organizations relying on regional and domestic affiliates
29. If transaction linkage with Non-affiliated regional and domestic terrorist groups (i.e. groups operating at regional or domestic level without any affiliation to a large-networked organization)
30. If transaction linkage with Ethnically or racially motivated terrorism groups
31. If transactions with Individual terrorists, including foreign terrorist fighters and small terrorists' cells
32. If social media accounts posting bank account details, payment links, or cryptocurrency addresses for donations
33. If payments to account using certain slogans, symbols, or coded language hinting at terrorist fundraising drives.
34. If a surge of small online donations or payments following extremist propaganda posts or events
35. If payments which can be linked to Purported charitable campaigns on social media with vague or no clear legitimate purpose.
36. If fundraising efforts targeting or originating from areas with known terrorist activity or conflict zones

37. If anonymous or unverified accounts requesting financial support for causes linked to militancy

Examples of Attempted Suspicious Activities that may trigger SAR: -

- 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.
- Using multiple signatories on a personal account holder without apparent connection or relation to the account holder
- Customers presenting unverifiable or unreliable sources of income, such as freelance work, personal savings, family funds, etc.
- Customer showing extreme urgency to receive a transaction without a logical reason, especially when receiving identification or information is an issue.
- An attempted transaction where the customer abandons the transaction when asked for additional information or a valid ID, which would not normally be required for a basic transaction
- The recipient's details (name, address, phone number) are frequently changed or appear to be invalid or incomplete.

CHAPTER 4: MISCELLANEOUS

4.1 EMERGING ISSUES AND MITIGATION

4.1.1 Emerging issues

Perspectives of red flags differ for individual institutions as they have own sector-wide vulnerabilities, systemic risk and transaction patterns. So, it is quite challenging to cover all those matters in one frame. These challenges are often aroused from the evolving nature of financial crimes, resource constraints, and the need for robust collaboration. Here are some emerging issues in identification and management of red flags: -

1. Criminals are constantly innovating and quickly adopting new methods, techniques to escape from suspicious transaction reporting. This makes it challenging to set overall red flag typologies and guidance up to date.
2. Emergence of novel layering techniques and complex cross border structures for obfuscating.
3. Technological disparity among different reporting entities like some financial institutions have heavy investment in advanced technologies and other may have some compromised technology, may lag in their technological capabilities in identifying red flags which may result inconsistent and ineffective detection of red flags. Furthermore, lacking of information sharing within reporting entities, FIU, regulatory and supervisory institutions hinder a holistic view of emerging threats.
4. Discrepancy in the number or quality of STRs/SARs reporting by REs of similar size and risk profile, potentially indicating either under reporting by some or lacks in identification of red flags.
5. Limited integration of data from various sources such as company registrar, custom, *malpot*, PEPs list, sanction list etc. making it difficult in detection of red flags.
6. Inability of REs to track full chain of transaction involving complex structure.
7. Lack of strong collaboration with all the stakeholders of AML/CFT to share information and develop joint red flag indicators.
8. Adoption of digital financial services such as mobile banking, wallets present new avenues for illicit financial flows. So, detecting red flags in this high frequency and high-volume transactions is challenging.
9. Identifying red flags for TF, PF risk is quite challenging due to lack of knowledge, information, resources and real scenarios.

4.1.2 Mitigation measures

1. Enhanced training and awareness program should be extended for REs on emerging typologies, red flags focusing on some risky areas.
2. All the stakeholders of AML/CFT need to invest in advanced analytical tools, artificial intelligence to process large volume of data, identify complex structure.
3. Foster strong collaboration between stakeholders of AML-CFT for information sharing and make joint effort.
4. Conduct regular workshops and awareness programs for financial institutions and designated non-financial businesses and professions (DNFBPs) on identifying red flags specific to their sectors, understanding their reporting obligations.
5. Encourage and support REs in implementing and continuously upgrading their transaction monitoring systems with artificial intelligence/machine learning capabilities to detect unusual patterns, anomalies, and complex layering techniques more effectively.
6. Explore secure and efficient mechanisms for data sharing between FIU-Nepal, REs, regulatory, supervisory institutions and other stakeholders to create a more comprehensive view of financial transactions and identify cross-sector red flags.
7. Regularly publish and disseminate reports on new and evolving ML/TF typologies and associated red flags identified through domestic and international analysis.
8. Emphasize and support the implementation of a robust risk-based approach by REs, enabling them to focus resources on higher-risk customers, products, and geographies, thereby improving the efficiency of red flag identification.
9. Regularly update Nepal's National Risk Assessment to identify and prioritize key ML/TF threats and vulnerabilities, which in turn informs the development of targeted red flag indicators and mitigation strategies.

By implementing a comprehensive approach that combines technological advancements, human capacity building, strong inter-agency collaboration, and a robust legal framework, FIU-Nepal can significantly enhance its ability to identify and manage red flags, thereby strengthening Nepal's AML/CFT regime.

4.2Tipping Off and Penalties

As per section 44(A) (1) of ALPA, 2008*(amendment, 2024),* no reporting entity or nor any office-bearer or employee thereof shall disclose to their customers or any other persons that any of the following reports, documents, records, notices or intelligence concerning the offence of money laundering or terrorist financing or predicate offences will be, is being or has been

submitted:

1. Reports on suspicious transactions or transactions within or beyond the thresholds determined under this Act,
2. Reports relating to on-going monitoring orders under Section 19A,
3. Documents, records or intelligence provided to the Financial Intelligence Unit, investigation officer, authority to investigate into an offence pursuant to the prevailing laws, or to the regulatory body,
4. Any other details or intelligence to be provided by reporting entities under this Act or the rules framed, guidelines issued or directions given under this Act, or
5. Description of identity of the office-bearers or employees providing the reports, records, documents, notices or intelligence set forth in clauses (a) to (d).

   As per section 44(A) (4) of ALPA, 2008*(amendment, 2024)*, following authority shall impose following punishment on a person who acts contrary to section 44 (A) (1 to 3) as follows:
6. A fine of up to one million rupees by the regulatory body on a bank and financial institution or casino,
7. A fine of up to two hundred thousand rupees by the regulatory body on a designated non-financial business or profession,
8. Departmental punishment under the law of such body by such body on its office-bearer or employee, if the reporting entity is a corporate body,
9. Departmental punishment by the concerned competent authority on the Chief of the Department, an investigation officer or employee of the Department or authority to investigate into offences under the prevailing laws, notwithstanding anything contained in the prevailing laws relating to constitution and operation of service,
10. Departmental punishment by the concerned competent authority on the Chief or an employee of the Financial Intelligence Unit, notwithstanding anything contained in the prevailing laws relating to constitution and operation of service,

If REs form a suspicion that transactions related to ML/TF, they should taking into account the risk of tipping-off when performing the CDD process. If the RE reasonably believes that performing CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR/SAR. Res should ensure that their employees are aware of, and sensitive to, these issues when conducting CDD

NOTE

- While referring Sector-specific indicators or red flags, REs is prescribed to follow General indicators (such as Economically Irrational transaction, Use of Third party, Behavior of the customer, Cash and so on) as well as Predicate-offence related indicators.
- REs should submit the report as per the goAML Operational Guidelines.
- REs should also consider AML/CFT directives issued by their respective regulators while submitting the STR/SAR.
- For further information, please contact the Financial Intelligence Unit-Nepal (FIU-Nepal).

STR/SAR Guidelines

(Updated July 2025)

FINANCIAL INTELLIGENCE UNIT, NEPAL
(FIU-Nepal)

Nepal Rastra Bank, Baluwatar, Kathmandu
Tel: +977-1-5719653 (Ext. 2842/2418/2841)
Email: fiu@nrb.org.np
Website: www.nrb.org.np/departments/fiu