

FREQUENTLY ASKED QUESTIONS (FAQs)

(Please note that these FAQs constitute brief guidance and are provided for information only)

A. General FAQs

1. What is Money Laundering?

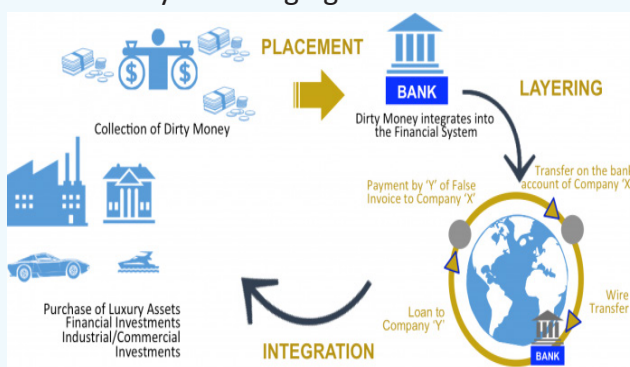
Criminal activities, such as drug trafficking, smuggling, human trafficking, corruption and others, tend to generate large amounts of profits for the individuals or groups carrying out the criminal act. However, by using funds from such illicit sources, criminals risk drawing the authorities' attention to the underlying criminal activity and exposing themselves to criminal prosecution. In order to benefit freely from the proceeds of their crime, they must therefore conceal the illicit origin of these funds.

Briefly described, "money laundering" is the process by which proceeds from a criminal activity are disguised to conceal their illicit origin. It may encompass

- (i) the conversion or transfer, knowing that such property is the proceeds of crime
- (ii) the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime; and
- (iii) the acquisition, possession or use of property, knowing, at the time of the receipt, that such property is the proceeds of crime.

2. How is Money Laundered?

The process of money laundering can be best described by following figure:



Source: UNODC

- a) In the initial - or placement - stage of money laundering, the launderer introduces his illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location.
- b) After the funds have entered the financial system, the second – or layering – stage takes place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channeled through the purchase and sales of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.
- c) Having successfully processed his criminal profits through the first two phases the launderer then moves them to the third stage – integration – in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

3. What is Financial Intelligence Unit, Nepal (FIU-Nepal)?

Financial Intelligence Unit (FIU)-Nepal is a national agency responsible for receiving, processing, analyzing and disseminating financial information and intelligence on suspected money laundering and terrorist financing

activities to the relevant law enforcement/ investigative agencies, regulators/supervisors and foreign FIUs. It was established on 21 April, 2008 under the section 9 of the Assets (Money) Laundering Prevention Act, 2008 within the Nepal Rastra Bank (the central bank) as an autonomous and operationally independent unit. Basically, FIU-Nepal receives TTR, STR/SARs from REs and these reports are analyzed, processed and disseminated to relevant law enforcement/investigative agencies, regulators/supervisors and foreign FIUs in the form of financial intelligence.

4. What is Predicate Offence?

Following offences are classified as predicate offence as per Asset (Money) Laundering Prevention Act (2008).

- Participation in an organized criminal group and racketeering
- Disruptive (terrorist) act and terrorism
- Trafficking in person and migrant smuggling
- Any kinds of sexual exploitation including sexual exploitation of children
- Illicit trafficking of narcotic drugs and psychotropic substances
- Illicit transportation of arms and ammunition
- Illicit transportation of stolen and other goods
- Corruption and bribery
- Fraud
- Forgery
- Counterfeiting of coin and currency
- Counterfeiting of goods and plagiarism or piracy of products
- Environmental related
- Murder, grievous bodily injury
- Kidnapping, illegal restraint or hostage-taking
- Theft or rubbery
- Smuggling (including custom, VAT and tax) related
- Tax (including direct and indirect) related
- Extortion
- Piracy

- Insider Dealing and Market Manipulation in securities and commodities related
- Ancient monument conservation related
- Forest, National park and wild animals related crime
- Money, banking, finance, foreign exchange, negotiable instruments, insurance, cooperatives related
- Black marketing, consumer protection, competition, supply related
- Election related
- Communication, broadcasting, advertising related
- Transportation, education, health, medicine, foreign employment related
- Firm, partnership, company, association related
- Real estate and property related
- Lottery, gambling, donation related
- Citizenship, immigration and passport related
- Offence of terrorist financing or association with terrorist organization
- Human Smuggling
- Hundi
- Virtual Currency
- Undue transaction
- Match fixing
- Unauthorized Casino Operation

5. What is a Money Laundering offence?

Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of an offence of money laundering. As per ALPA 2008, involvements in following offences are regarded as money laundering offence:

- Converting and transferring property by any means knowing or having reasonable grounds to believe that it is proceeds of crime for the purpose of concealing or disguising the illicit origin of property, or assisting any person involved in the offence for evading legal consequences of offender.
- Concealing or disguising or changing the true nature, source, location, disposition,

movement or ownership of property or rights with respect to such property knowing or having reasonable grounds to believe that it is proceeds of crimes.

- Acquiring, using, possessing property knowing or having reasonable grounds to believe that it is the proceeds of crime.

6. What are Proceeds of Crime?

“Proceeds of crime” means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a predicate offence or the value of any such property.

7. What is Financing of Terrorism?

Terrorist financing involves the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both legal and illicit sources. The primary goal of individuals or entities involved in the financing of terrorism is therefore not necessarily to conceal the sources of the money but to conceal both the financing and the nature of the financed activity.

8. How are efforts to combat Money Laundering and Financing of Terrorism related?

Money laundering is the process of concealing the illicit origin of proceeds of crimes. Terrorist financing is the collection or the provision of funds for terrorist purposes. In the case of money laundering, the funds are always of illicit origin, whereas in the case of terrorist financing, funds can stem from both legal and illicit sources. The primary goal of individuals or entities involved in the financing of terrorism is therefore not necessarily to conceal the sources of the money but to conceal both the funding activity and the nature of the funded activity.

Similar methods are used for both money laundering and the financing of terrorism. In both cases, the actor makes an illegitimate use of the financial sector. The techniques used to

launder money and to finance terrorist activities/terrorism are very similar and, in many instances, identical. An effective anti-money laundering/counter financing of terrorism framework must therefore address both risk issues: it must prevent, detect and punish illegal funds entering the financial system and the funding of terrorist individuals, organizations and/or activities. Also, AML and CFT strategies converge; they aim at attacking the criminal or terrorist organization through its financial activities, and use the financial trail to identify the various components of the criminal or terrorist network. This implies to put in place mechanisms to read all financial transactions, and to detect suspicious financial transfers.

9. How are Corruption and Money Laundering related?

Anti-corruption and anti-money laundering work are linked in numerous ways, and especially in recommendations that promote, in general, transparency, integrity and accountability. The essential connections are: Money laundering (ML) schemes make it possible to conceal the unlawful origin of assets. Corruption is a source of ML as it generates large amounts of proceeds to be laundered. Corruption may also enable the commission of a ML offense and hinder its detection, since it can obstruct the effective implementation of a country’s judicial, law enforcement and legislative frameworks.

When countries establish corruption as a predicate offense to a money laundering charge, money laundering arising as a corrupt activity can be more effectively addressed. When authorities are empowered to investigate and prosecute corruption-related money laundering they can trace, seize and confiscate property that is the proceeds of corruption and engage in related international cooperation. When corruption is a predicate offense for money laundering, AML preventive measures can also be more effectively leveraged to combat corruption.

10. Why is controlling of money laundering necessary?

Since money laundering is a financial crime, it does not serve the interest of any economic actor. Controlling money laundering is necessary for the following reasons:

- Money laundering undermines the integrity of financial institutions and markets, distorting asset and commodity prices, which can lead to economic instability and a loss of confidence in financial systems.
- It is often linked to serious crimes such as drug trafficking, terrorism, corruption, and fraud, and by controlling it, authorities can disrupt the financial networks that support these illegal activities.
- Financial institutions are required to comply with anti-money laundering (AML) laws and regulations, and failure to do so can result in severe penalties, legal consequences, and reputational damage.
- Money laundering can fund terrorist activities and other threats to national security, making effective AML measures crucial for enhancing national security.
- Businesses involved in money laundering often gain an unfair advantage over legitimate ones by offering lower prices or higher returns due to illicit gains, and controlling money laundering helps ensure fair competition.
- The integrity of financial systems is vital for public trust, and when money laundering is prevalent, it erodes trust in financial institutions and the broader economic system, making effective AML measures essential for maintaining and restoring public confidence.
- Money laundering often involves proceeds from activities with significant negative social impacts, such as human trafficking, drug abuse, and corruption, and controlling it helps mitigate these social harms.

- Money laundering is a global issue that requires international cooperation, as countries that fail to control it can become havens for illicit funds, undermining global efforts to combat financial crime.

11. Why Know Your Customer (KYC) is necessary?

KYC is the process of verifying the identity of clients and assessing potential risks of illegal intentions for the business relationship. The objective of KYC guidelines is to prevent banks and other institutions from being used, intentionally or unintentionally, by criminal elements for money laundering activities. Documents collected from the client at the start of business relationship enable banks and other institutions (including online portals) to better understand their customers, their financial dealings and manage their risks prudently. The key components of KYC are as follows:

- Customer Acceptance Policy (CAP)
- Customer Identification Procedures (CIP)
- Monitoring of Transactions
- Risk Management

The application of KYC process by financial institutions and a high degree of transparency is crucial to fight money laundering and the financing of terrorism effectively. Criminals use the financial system to transfer funds to launder money, or to finance terrorism. Financial institutions, in particular banks, are most vulnerable to abuse for that purpose. In order to protect them, it is essential that financial institutions have adequate control and procedures in place that enable them to know the person with whom they are dealing. Adequate KYC and due diligence on new and existing customers is a key part of these controls. Hence, KYC is necessary in today's banking sector.

12. What is Beneficial Ownership?

Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. Even if the legal

person or arrangement is registered under the name of another person or entity, the beneficial owner is the individual who ultimately exercises control over it or receives the financial benefits.

13. What is Money Mule?

A money mule is an individual that is recruited, knowingly or unknowingly, to transfer or move illegally acquired money on the behalf of criminals as part of a money laundering scheme. Money mules can be used to launder money obtained from illegal activities such as fraud, cybercrime, drug trafficking, or other organized crime. They are often unaware that they are participating in illegal activities, as they may be recruited under false pretenses.

Criminals recruit money mules through various methods, such as online job postings, social media, or even direct contact. They may be promised easy money, work-from-home opportunities, or other incentives. The money mule receives illicit funds into their bank account, often from victims of fraud or other crimes. The mule is then instructed to transfer the funds to another account, often in a different country, or to withdraw the money and send it via other means (e.g., cash, wire transfers, or cryptocurrency). Once the funds are transferred, the criminals sever contact with the mule, leaving them exposed to legal consequences.

14. What influence does money laundering have on economic development?

Money laundering significantly undermines economic development by eroding the integrity of financial institutions, distorting economic data, and encouraging crime and corruption. It reduces tax revenue, exacerbates income inequality, and deters foreign investment due to perceived risks. The need for costly regulatory compliance measures increases operational expenses, while illicit gains distort market competition, hampering legitimate businesses. Additionally, money laundering weakens legal frameworks, facilitates terrorism financing, and contributes to social instability. Addressing these

issues requires strong legal systems, effective enforcement, and international cooperation to mitigate its detrimental impact on economic growth and stability.

15. What is Threshold Transactions Reporting (TTR)?

TTR is a report of transactions that financial institutions and DNFBPs are required to file to FIU-Nepal for deposit, withdrawal, exchange of currency, and payment or transfer exceeding the defined threshold. Regulators of REs have designated different threshold to REs as per the nature of business and risk involved. Such threshold may be reached by a single transaction or by a series of transactions in single account or by a single customer over a prescribed period.

16. What is a STR/SAR?

STR/SAR is a report filed by REs to FIU when a suspicious transaction or activity is identified. REs are required by law to file STR/SAR when they have reasonable grounds to suspect money laundering or terrorist financing.

As per Section 7 Dha(1) of ALPA (2008), RE shall file a STR to the FIU-Nepal immediately after carrying out examination, with respect to any customer, transaction or property if:

- it suspects or has reasonable grounds to suspect that the property (money) is the proceeds of ML/TF/PF or other offence, or
- it suspects or has reasonable grounds to suspect that the property is related or linked to, or is to be used for, financing of terrorism, terrorist acts or by terrorist persons or terrorist organizations.

As per Section 7 Dha(2) of ALPA (2008), RE shall also file SAR to FIU-Nepal even if customer has only attempted to carry out any transactions referred to in Section 7 Dha(1).

REs should take reasonable measures to establish ground of suspicion regarding transactions of a person/entity in relation to ML/TF/PF offense. The general red flags of suspicious financial

transactions/activities are provided in STR/SAR Guidelines of FIU-Nepal. (*Link of STR/SAR Guidelines: <https://www.nrb.org.np/fiu/suspicious-transaction-reporting-suspicious-activity-reporting-str-sar-guidelines/>*)

17. How do REs submit STR/SAR to FIU-Nepal? What should be included in a STR/SAR ?

REs submit STR/SARs using web or XML report format of goAML software. FIU-Nepal has provided two environments in goAML for reporting entities: Test Environment and Production Environment. The Test Environment is a simulation environment of the goAML for practice and testing purposes. The Production Environment is where actual reporting of TTR, STRs/SARs and other financial intelligence activities takes place. ALPA (2008) mandates REs to report any suspicious financial transactions or activities to FIU-Nepal in the format specified by FIU-Nepal.

STR/SARs should include detailed information about transactions that appear to be suspicious or have reasonable ground of suspicion in related to ML/TF or other offense. The quality of a STR/SAR is only as good as the content, therefore, it should include, 'who, what, where, when, why, how and which predicate offence'. It should also include all supporting documents as prescribed by FIU-Nepal in its STR/SAR Guidelines.

18. Should the business relationship with the customer be terminated after lodging STR/SAR to FIU-Nepal?

Whether to terminate a business relationship with a customer after lodging a STR/SAR with FIU-Nepal depends on several factors, including legal obligations, regulatory requirements, and the specific circumstances of the case.

Unless instructed otherwise by the relevant authorities, it is usually wise to continue the business relationship with the customer after filing an STR/SAR. Prematurely terminating the relationship could tip off the customer, potentially compromising ongoing investigations.

However, REs should conduct a thorough risk assessment to determine whether continuing the relationship poses a significant risk based on the nature and severity of the suspicious activity and the potential impact on the institution's reputation. Enhanced due diligence and ongoing monitoring of the customer's transactions and activities are essential to detect further suspicious behavior and ensure adherence to regulatory requirements. The institution should follow its internal policies and procedures, including criteria for terminating a business relationship, which should be aligned with regulatory requirements and best practices. REs should maintain proper documentation of all actions taken, including the rationale for any decision to continue or terminate the relationship. Also, any decision to terminate a relationship should be communicated appropriately within the organization to avoid any inadvertent disclosure that could alert the customer or compromise an investigation.

As per ALPA(2008) REs shall terminate the business relationship with an existing customer who does not provide documents and details required for the customer identification and verification or whose identification and verification cannot be made on the basis of the documents, information and details provided by the customer.

19. What is difference between Information, Intelligence and Evidences?

Information refers to processed data that provides meaning and understanding, while **intelligence** is the result of analyzing and further processing of information to generate evidence-based knowledge. Intelligence involves the ability to comprehend, understand patterns, and make informed decisions based on prior experiences. It incorporates context, corroboration, and value to provide guidance and resolve uncertainty. Intelligence is the collection of relevant aggregated information directed by an individual's experiences and understanding. For example, in AML/CFT, information could be transaction records, and intelligence would involve analyzing

those records to detect suspicious patterns or behaviors, ultimately guiding decision-making and action. **Evidence**, on the other hand, is the culmination of a rigorous investigation, whether based on information or intelligence. It is legally admissible proof, meticulously collected and verified to support legal actions against financial criminals.

FIU-Nepal receives information from REs in the form of SAR/STR/TTR and additional information. After analysis, such information is converted into actionable intelligence by FIU-Nepal. Any dissemination from FIU-Nepal should be treated as intelligence, not evidence. It is responsibility of LEAs to convert intelligence to evidence.

20. What is 'Tipping Off'?

Tipping off refers to the act of alerting or informing a customer or third party that a STR/SAR has been filed about them with the Financial Intelligence Unit (FIU) or relevant authorities. This disclosure can compromise ongoing investigations by giving the individual or entity an opportunity to alter their behavior, hide evidence, or move illicit funds.

Tipping off is prohibited by law, and REs or individuals who engage in it may face severe legal penalties, including fines or criminal charges. The purpose of this prohibition is to maintain the integrity of AML/CFT efforts, ensuring that suspicious activities can be investigated without interference.

21. What is Mutual Evaluation?

Mutual Evaluation is a peer review process in which country are assessed to determine the levels of compliance with the international AML/CFT standards. It has two aspects: technical compliance and effectiveness compliance.

a) **Technical Compliance Assessment:** A desk-based technical compliance analysis assesses compliance by an APG member with the specific requirements of each of the 40 FATF recommendations- the relevant legal and institutional framework

of the jurisdiction, and the powers and procedures of competent authorities. These recommendations represent the building blocks of an AML/CFT system. The technical compliance analysis is undertaken by an assessment team prior to an on-site visit of the member being evaluated.

b) **Effectiveness Assessment:** The main component of a mutual evaluation is effectiveness. It assesses the extent to which an APG member achieves a defined set of outcomes that are central to a proper functioning and effective AML/CFT system with expected results based on the ML and TF risk profile of that jurisdiction. The effectiveness analysis is not only based on information exchanged with the assessment team but also after the exchange of information, the team will visit the member under evaluation (usually for two weeks, sometimes longer) and interview government and private sector officials to gain a comprehensive understanding of how the AML/CFT system is working. Effectiveness assessment is done based on the FATF's 11 Immediate Outcomes (IOs).

22. What are the consequences of low compliance in mutual evaluation?

Country with low compliance in mutual evaluation is subject to FATF review and may be put in the global Negative List as non-cooperative country. Negative listed jurisdictions may face following consequences:

- Harder situation for banks to conduct international transactions
- Increase in cost of funds or delay or limitation
- Loss of credit lines or correspondent relationships
- Decrease in receiving assistance, loan and other facilities from international organizations and countries

- Restrictions on inward remittance, aid, capital and other flows
- Inability of institutions to expand overseas
- Withdrawal of foreign banks
- Loss of investor confidence

(Please note that these FAQs constitute brief guidance and are provided for information only)