FINANCIAL INFORMATION UNIT

BANK OF MONGOLIA

Guidance on the risk-based approach to combat money laundering and terrorism financing

FOR ACCOUNTING AND FINANCIAL CONSULTING SERVICE PROVIDERS

2020

The Financial Information Unit was established alongside the Bank of Mongolia to implement legislation of combating money laundering and terrorism financing in accordance with the Article 16 of the Law on Combating Money Laundering and Terrorism Financing.

For more information about the Financial Information Unit, please visit https://fiu.mongolbank.mn/.

CONTENTS

EXECUTIVE SUMMARY 4
INTRODUCTION 5
ONE. MONEY LAUNDERING AND TERRORISM FINANCING 5
1.1. Money laundering 5
1.2. Terrorism financing 7
1.3. Financing proliferation of weapons of mass destruction 7
1.4. Legal regime 8
1.5. Financial Information Unit 9
1.6. Liability for violation 11
1.7. Why is the AFSPs legally obligated? 11
1.8. CASE STUDIES AND EXAMPLES: 12
1.8.1. **Case study 1. The crime of tax evasion** 12
1.8.2. **Case study 2: A crime detected by undercover investigation of New Zealand** 13
1.8.3. **Case study 3. Accountants provide financial advice to organized criminal group** 14
1.8.4. **Case study 4. Reporting a suspicious transaction** 15
TWO. RESPONSIBILITIES OF AFSP 15
THREE. ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH 17
3.1.1 Customer risk 17
3.1.2 Risks associated with the product and services and its delivery channel 18
3.1.3 Geographical risk 18
FOUR. CUSTOMER DUE DILIGENCE (CDD) 19
FIVE. SUSPICIOUS TRANSACTION REPORT 21
SIX. CONFIDENTIALITY AND PROHIBITIONS 23
EIGHT. TRAINING AND AWERENESS RAISING ACTIVITIES 24
NINE. SOURCES USED 25

GLOSSARY

APG	Asia/Pacific Group on Money Laundering
AFSP	Accounting and financial consulting service providers
UN	United Nations
ML/TF	Money Laundering and Terrorism Financing
AML/CFT	Anti-money laundering / Countering the Financing of Terrorism
RE	Reporting entities
DNFBP	Designated Non-Financial Businesses and Professions
STR	Suspicious Transaction Report
FIU	Financial Information Unit
FATF	Financial Action Task Force
CDD	Customer Due Diligence

EXECUTIVE SUMMARY

1. Designated non-financial and businesses provider which includes dealers in precious metals and stones or products made from precious metals and stones, real estate agents, lawyers, notaries, accountants, and financial advisory services are being used for activities for money laundering, terrorism financing and the financing of proliferation of weapons of mass destruction. Professional services provided by DNFBPs, their professional advice and guidance to exploit of vulnerabilities in the legal system may be used in money laundering and other illegal activities, such as concealment of the proceeds of crime.
2. Due to the intentional and unintentional participation of DNFBPs in activities of money laundering, terrorism financing and the financing of proliferation of weapons of mass destruction, Financial Action Task Force (FATF) has demanded to implement some specific responsibilities.
3. To fulfill the international standard, AML/CFT Law states that DNFBPs are reporting entities (RE) and have an obligation to perform certain duties.
4. The purpose of this guidance is to assist DNFBPs in fulfilling their obligations under the AML/CFT Law and other relevant legal documents.
5. International standard of FATF and the AML/CFT Law states that a risk-based approach will be used to combat ML/TF. Therefore, it is necessary for DNFBPs to assess ML/TF risks to which they are exposed, mitigate the risks, and implement a risk-based approach in their activities. Furthermore, the implementation of a risk-based approach is beneficial for the efficient allocation of resources to combat ML/TF.
6. According to the AML/CFT Law, the DNFBP is responsible for establishing customer due diligence, enhancing the oversight if it identifies certain risks, reporting actions in high risk situations, and keeping the records. Additionally, they are required to implement a ML/TF risk-based approach in their operations and businesses. This guidance has been prepared by the FIU to ensure and support the fulfillment of this obligation, and the FIU is open to further comments and suggestions for improvements to this guidance and, if necessary, is ready to organize relevant events regarding this guidance.
7. This guidance is designed for professional service providers and includes relevant case studies.

8. This guidance is intended solely to provide assistance and methodological assistance to the DNFBPs in fulfilling their legal obligations.

INTRODUCTION

Purpose of this guidance:

This guidance is designed to assist the AFSPs and individuals for preventing ML/TF, managing ML/TF risks, and fulfilling their obligations to report and implement other legal measures in accordance with the relevant laws in Mongolia.

Who shall use this guidance?

The reporting entity, AFSPs specified in Article 4.1.9 of the AML/CFT Law should use this guidance when the REs have prepared, performed, or participated in the following activities related to their customers:

- Buying and selling of real estate;
- managing of customer's assets;
- management of bank, savings, or securities accounts;
- organization of contributions for the creation, operation, or management of companies;
- creating, operating or management of legal persons or arrangements, and buying and selling of business entities.

The following entities shall be included in AFSP:

- Audit company;
- Contract auditor;
- Contract accountant;
- Tax advising service provider individuals or legal entities.

ONE. MONEY LAUNDERING AND TERRORISM FINANCING

1.1. Money laundering

1.1.1. The AML/CFT Law defines "**Money laundering**" as the acquisition, possession or use of income, money and assets knowing that they are proceeds of crime or transfer or conversion of such proceeds to conceal their illicit origins and to assist entities involved

in committing crimes to avoid legal liabilities, or disguise their true natures, origins, locations, administration, ownership, and property rights.

1.1.2. Money laundering generally has the following main purposes:

- convert or transfer the origins of proceeds of crime
- transfer and conceal the real nature, origins, location, rights of proceeds of crime
- transfer and conceal the nature, source, origin, location, disposal method and property rights of proceeds of crime;
- acquire, possess, use, and get benefit from proceeds of crime
- cooperate, plot, attempt to commit, aid, abet, consult etc. in acts of money laundering

1.1.3. Besides financial professionals, DNFBPs which includes individuals and legal entities who are dealers in precious metals and stones, real estate agents, lawyers, notaries, AFSPs are commonly involved in the activities of money laundering. Therefore, activities to combat this type of crime and detect illicit assets and income requires a wide range of knowledge in many areas. Money launderers try to conceal nature and forms of the proceeds of crime, using payment instruments used in both international and domestic markets, using high-valued metals, jewelry, products, services and new technology.

ML/TF activities consist of three stages: placement, layering, and integration.

- **Placement stage:** The funds and proceeds derived from criminal activities are brought into the financial system. It may include exchanging currency for another currency, transporting cash, or depositing cash into a bank account.
- **Layering stage:** The intention of this stage is to conceal and obscure the origins of the funds obtained from criminal activities. For example, funds can be placed through non-cash transfers, transferred to a different account at another financial institution, shuttled through multiple accounts at different banks and countries to obscure its origins.
- **Integration stage:** Once the origin of the assets and funds has become difficult to follow, and when the assets and funds provided with apparent legitimacy, then the assets and funds are returned under the offender's ownership.

1.1.4. In the above stages of money laundering, criminals become organized and develop a complicated scheme in order to conceal the origin and nature of their illegal funds by

using professional service providers such as the AFSPs, lawyers, and notaries to legalize the proceeds of crimes.

1.2. Terrorism financing

1.2.1. AML/CFT Law defines **"terrorism"** as act of violence, threat of violence, or creation of catastrophic conditions in order to achieve political, religious, ideological, or other similar purposes in order to intimidate government organizations, society, or a particular part of society.

1.2.2. AML/CFT Law defines **"Terrorism Financing"** as direct or indirect collection, transfer, changes, and use of assets with the knowledge that they are to be used to carry out a terrorist act or to finance a terrorist individual or an organization.

1.2.3. The main motive for money laundering is to legalize the proceeds of crime. However, the motive for the financing of terrorism is the use of legal and illegal assets and funds for terrorist activities.

1.2.4. The crimes of money laundering and terrorism financing are closely linked together because these two types of crimes share similar methods. However, in terms of content, these two types of crimes are committed separately. For example, while money laundering seeks to legitimize the proceeds of crime, the financing of terrorism can also be financed through legal funds.

1.2.5. Terrorism is usually funded by the following sources:

- theft of large amount of assets;
- weapons and drugs trafficking;
- illegal immigration and human trafficking;
- kidnapping;
- threatening and extortion;
- making donations from legal and illegal proceeds (individuals, non-governmental organizations, humanitarian organizations etc.).

1.3. Financing proliferation of weapons of mass destruction

1.3.1. AML/CFT Law defines **"Proliferation"** as the acts to develop, manufacture, possess, store, acquire, transport, export, transfer, accumulate, purchase, sell, provide full or partial financial support and services to use for all types of nuclear, chemical, biological or weapons of mass destruction, including their raw materials, items,

equipment, technology and goods and products with dual-use for the purpose of proliferation of weapons of mass destruction that is prohibited by international treaties and laws of Mongolia.

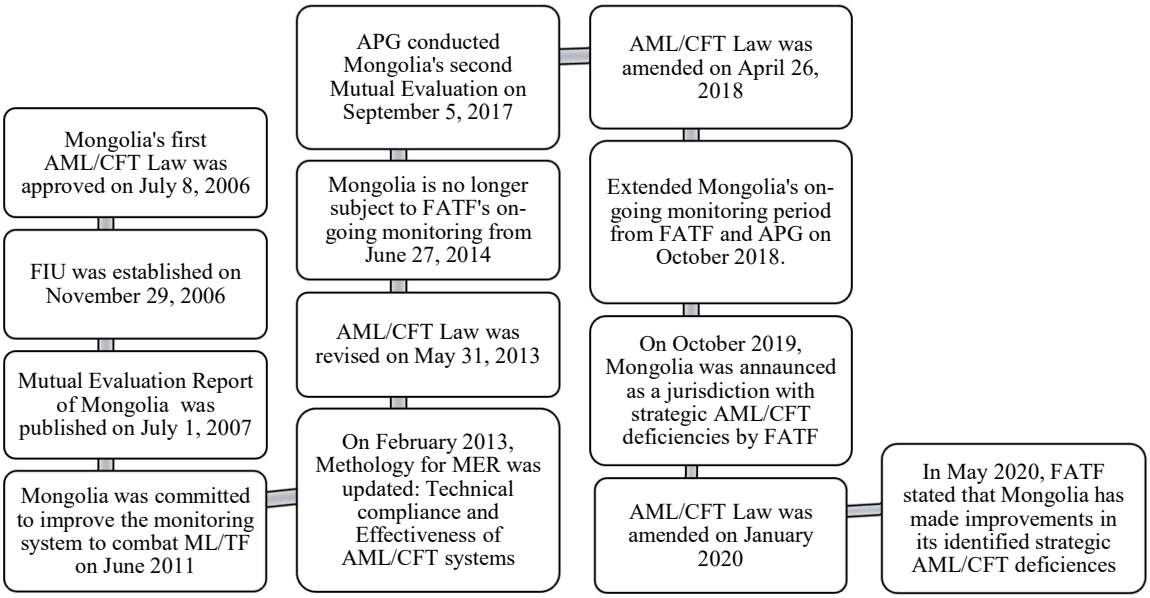
1.4. Legal regime

1.4.1. Mongolia joined the International Convention for the Suppression of the Financing of Terrorism in 2003 and joined Asia/Pacific Group on Money Laundering (APG) in 2004. Thus, Mongolia became obliged to comply with and implement the international standards against money laundering, terrorism financing and proliferation financing related to weapons of mass destruction.

1.4.2. The AML/CFT Law was first approved on July 2006, and was amended in 2013, 2018, 2019 to expand the scope of the law as listing dealers in precious metals and stones, real estate agents, lawyers, notaries, and AFSPs as REs in accordance with international standards and obligations.

1.4.3. Therefore, the above-mentioned REs must conduct Customer Due Diligence (CDD) and report transactional or operational information to the FIU.

1.4.4. The following diagram shows the chronological changes in the AML-CFT legal environment



1.4.5. The following laws and international standards shall be complied by the AFSPs to combat and prevent ML/TF:

- Law on Combating Money Laundering and Terrorism Financing;
- Law on Combating Proliferation and a Terrorism;
- "Regulation for the Targeted Financial Sanctions Against Proliferation of Weapons of Mass Destruction and Combating Terrorism" approved by Government of Mongolia Decree No.463 on December 25, 2019
- "Regulation on Preventive Measures in Combating Money Laundering and Terrorism Financing" approved by the Bank of Mongolia's Governor's Decree No. A-26 on January 21, 2019";
- "Regulation for Reporting Entities on Submitting Information Electronically to the Financial Information Unit" approved by the Bank of Mongolia's Governor's Decree No. A-326 on December 25, 2019;
- "Guidance for Filling the Report to be Submitted to the Financial Information Unit"
- FATF Recommendations

1.5. Financial Information Unit

1.5.1. An important requirement of the AML/CFT system is for the REs to report transactions which may have suspected to involved in crime or terrorist activities. The FIU receives and analyzes the suspicious transaction information from the REs and submits it to competent law enforcement authorities for investigation if it is considered to be involved in crime or terrorist activity. Therefore, countries set up a specialized organization, the FIU, to analyze financial information which may have related to crime or terrorist activities.

1.5.2. In accordance with the adoption of the AML/CFT Law on July 8, 2006, Mongolia established the FIU alongside the Bank of Mongolia and set the foundation for AML/CFT measures and its preventive activities. Furthermore, by becoming a member of the Egmont Group in 2009, Mongolia's FIU was able to exchange information and cooperate with other member FIUs of the Egmont Group.

1.5.3. Article 16.1 of the AML/CFT Law states that the FIU is the autonomous and independent agency whose functions is to receive information related to money laundering, related crimes, and financing of terrorism, information about suspicious transactions, cash and foreign settlement transactions that's in excess of thresholds from REs and analyze them, and disseminate it to the competent law enforcement authorities if transactions and transaction attempts are suspected to be related to money laundering and terrorism financing.

1.5.4. The FIU shall have the following functions in accordance with the Article 18 of AML/CFT Law:

- In accordance with the AML/CFT law, if the FIU has grounds to suspect that the given transaction had the purpose of ML/TF, then the FIU can monitor the REs customer's account, freeze the assets, and suspend the transaction;
- To receive, collect, and analyze information reported by REs and to receive and analyze information from local and foreign institutions' database;
- If there are sufficient grounds for the FIU to suspect that the given transaction had the purpose of money laundering or terrorism financing, then it shall be disseminated to competent law enforcement authorities and anti-terrorism agencies according to the regulation and to compile database on reports of suspicious, cash and non-cash transactions submitted to the competent authorities;
- To provide general information on the analysis of suspicious transactions and general types and methods of suspicious transactions in order to support the detection and reporting of suspicious transactions by the REs;
- To inform and organize the implementation of a methodology that verifies information related to the AML/CFT, monitors, and detects suspicious transactions to REs;
- To enhance public awareness to combat and prevent money laundering and terrorism financing;
- To inform and organize the implementation of the sanctions lists to the REs;
- To compile statistics on inspections of the implementation of the AML/CFT Law, as well as conduct inspections, have other authorized entities carry out inspections
- To conduct a National AML/CFT Risk Assessment, develop a national strategy based on the results of the assessment, and organize the discussion of this strategy by the Cooperation Council;
- Organize measures to ensure the implementation of the recommendations issued by the international organizations in charge of AML/CFT.

Liability for the breach of the law

1.5.5. Persons guilty for violating the AML/CFT Law shall be held liable in accordance with the relevant laws.

1.5.6. If a violation of AML/CFT law and regulations issued conform of AML/CFT law; possible violation is discovered during supervision; non-compliance with the

term of the license is not a criminal offense public official of the competent authorities described in the Article 19.1 of the AML/CFT law shall impose following rectification measures:

- Rectification warning notice, rectification orders with deadline;
- To assign task to REs to improve, strengthen structure, operations, risk management, internal monitoring;
- To make proposal of partially or wholly limitation, halting, suspension, cancellation of special licenses of REs;
- To issue order to revoke, suspend and change of the high-level management officials of REs.

1.5.7. If the officials not complaining with the rectification measures described in the Article 23.2 of the AML/CFT law, sanctions imposed under the Law on Infringement should be used.

1.6. Liability for violation

1.6.1. Article 5.10 and Article 11.29 of the Law on Infringement states the penalties for violating the AML/CFT Law, and the Law on combating proliferation and terrorism accordingly.

1.6.2. The state inspector of FIU shall be liable in accordance with the Law on Infringements Procedure and the AML/CFT Law.

1.7. Why is the AFSPs legally obligated?

1.7.1. FATF considers the accounting sector as a risky sector related to ML/TF activity.

1.7.2. Accounting professionals provide a wide range of services to their customers, including audit and assurances services, tax advisory services, financial reporting, and record keeping, all of which increases the risk of using AFSPs for ML/TF activities.

1.7.3. For example, criminals seek advice through financial and tax advisory services, such as tax evasion and avoiding other debts, use accountants to withdraw cash, transfer money between domestic and international accounts that will act as concealment of their illegally acquired assets and income.

1.7.4. Money launderers use professional service providers, such as lawyers, notaries, and AFSPs. According to the FATF's recommendations, accountants act as "gatekeepers" since accountants are the first stage for the money to enter the financial system. Therefore, FATF's Recommendation 22 emphasizes the need for these

professional service providers to take preventive measures against ML/TF risks and fulfill their responsibilities in combating ML/TF.

1.7.5. In order to implement the FATF Recommendations, Mongolia is implementing the AML/CFT Law and the requirements of international standards in a timely manner within the domestic legal environment.

1.7.6. Within this framework, the requirements related to the AFSPs have been defined in the AML/CFT Law and have been implemented since 2018.

1.7.7. The professional service providers can protect themselves from the risks associated with ML/TF crimes by fulfilling their legal obligations.

1.7.8. The role of AFSPs stated in the AML/CFT Law is explained in detail in the guidance issued by the FATF. The AFSPs should review these documents to improve their understanding. For example, the following documents are issued by the FATF:

- FATF 40 recommendations;
- FATF 1, 10, 11, 12, 17, 19-25, 28, 35 recommendations related to AFSPs;
- FATF guidance on Transparency and Beneficial owner;
- FATF Guidance on the Risk-Based Approach for Trust and Company Service Providers;
- FATF Guidance for a Risk-Based Approach for the Accounting Profession

1.8. CASE STUDIES AND EXAMPLES:

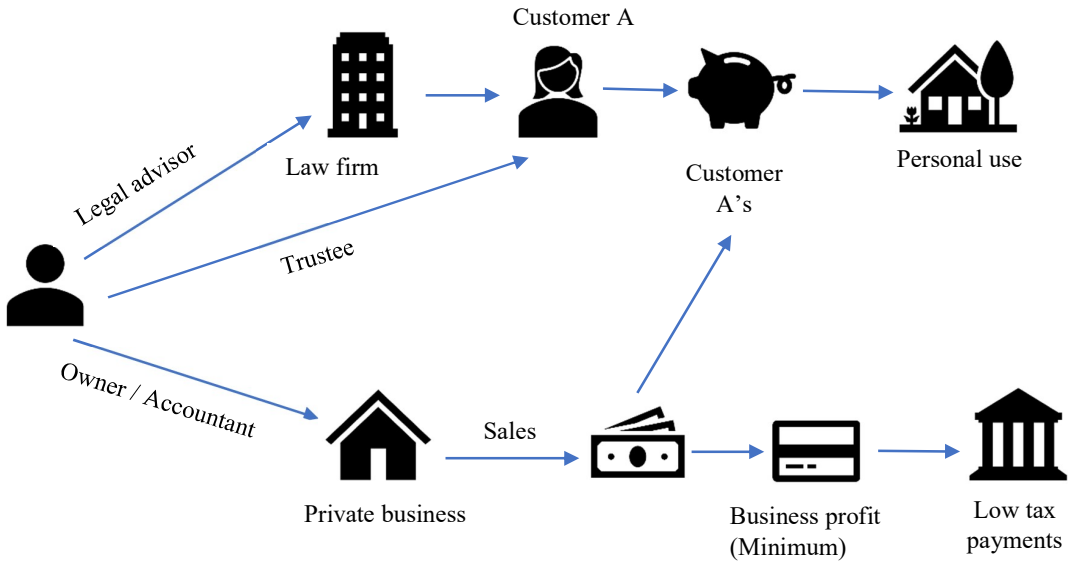
1.8.1. Case study 1. The crime of tax evasion

A law firm and a retailer that operate in the United States has committed tax evasion crime by concealing their business income and profits.

For example, in the course of acting as a consultant for a law firm, the criminal managed his customer's account by an accreditation agreement and engaged in illegal activities by storing and withdrawing his business profits from his customer’s account. This allowed him to keep his tax account balance low, which allowed him to successfully evade the tax authorities and commit the crime of tax evasion. He was able to evade 300,000.00 USD in taxes for over two years.

Investigators discovered the case by examining the suspicious activity reports and identifying a large-scale organized transaction activities.

The criminal was soon found guilty of intentional tax evasion and sentenced to one year in prison, continued with a three-year suspended sentence, as well as sentenced to pay high amount of taxes, interest, and fines.



1.8.2. Case study 2: A crime detected by undercover investigation of New Zealand

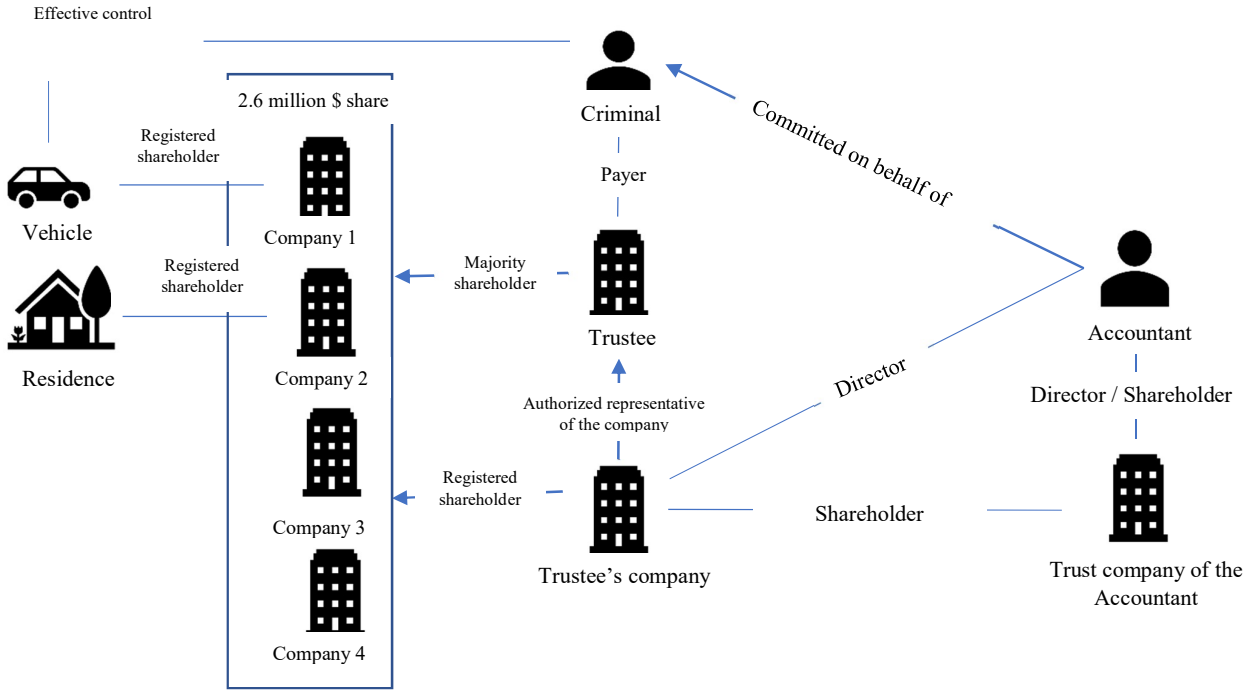
New Zealand's police agency have detected the following crime through an undercover investigation. Drug traffickers set up a complicated legal entity and used professional service providers such as accountants and trustees to conceal the proceeds of their crime. It can be seen from this case that the professional service providers are used in various ways to commit money laundering crimes. For example:

- establish a separate legal entity for the purpose of concealing the control and the beneficial ownership of the company which is managing the assets;
- create a complex structure using professional service providers and use them as intermediaries;
- using trustee services to conceal the transactions related to the crime.

The criminal used the proceeds of the drug sales to buy shares of a magazine company and its business using trustee services. The criminal's car was later registered in that magazine company's name, which was an attempt to avoid registering assets in his own name.

The criminal also used his accountant as an intermediary, adding another layer of concealment. Finally, the criminal used the accountant as his trustee to conceal the

magazine company's and vehicle's beneficial owner. For example: The criminal's residence was registered under another company which was a shareholder of his accountant's trust company. The accountant's trust company owned the shares on behalf of the criminal through trustee services.



1.8.3. **Case study 3. Accountants provide financial advice to organized criminal group**

Law enforcement agencies identified an accountant Mr. U, who is a part of the criminal organization involved in money laundering and re-investment of illicit proceeds derived from drug trafficking led by Mr. X.

Mr. U is an expert in international and domestic banking procedures, and complex international financial instruments. He was the main financial officer for investing the proceeds of Mr. X's criminal activities.

Mr. U's task was to analyze the technical and legal aspects of these investments planned by the organization and identify the most appropriate financial techniques to make these investments legitimate from an accounting stance. For example, he made loan, commercial and investment contracts and made financial transactions with the proceeds of crime among the international companies and financial institutions through electronic transfers to make it appear legitimate.

1.8.4. **Case study 4. Reporting a suspicious transaction**

Accountant A provided service to the criminal and transferred $50,000 to the customer's account through his company's account. Initially, the accountant didn't know the illegal origins of the money, but later reported the suspicious transaction to the relevant authorities and continued to provide his services to the criminal. The court found that the accountant was used for organized crime and found not guilty.

1.8.5. From the examples mentioned above, it can be seen that the person and legal entity of AFSPs have a significant role in the implementation and prevention from the ML/TF activities. It is important to note that if the AFSPs hadn't foreseen its potential ML/TF risks and fail to fulfill its obligation to conduct CDD and report suspicious activities on ML/TF operations, then the AFSP will be targeted by criminals, and their business will be harmed by criminal actions.

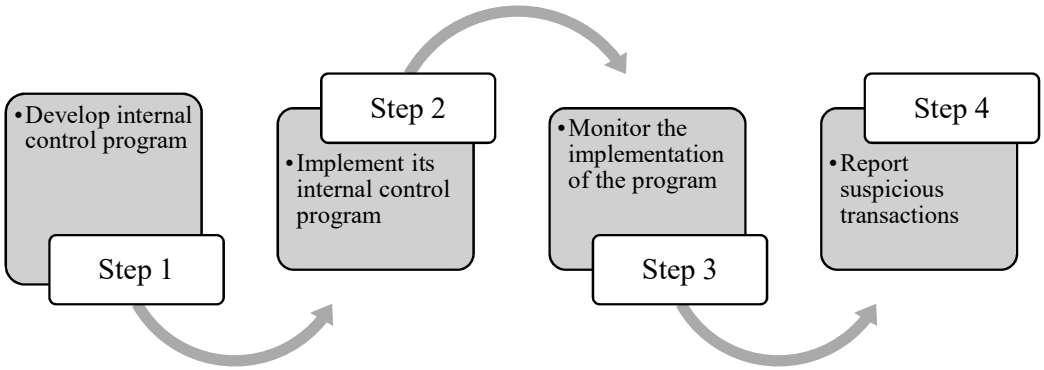
1.8.6. There are some instances where accountants do evade taxes and conspire with other taxpayers to falsify financial documents. These accountants increase the risk of money laundering through engaging in unethical practices by concealing taxable activities, reducing the reporting amounts, artificially inflating costs, and falsifying financial and tax reports.

1.8.7. Therefore, it is important for the AFSPs to have a high level of professional ethics, to implement risk-based activities to prevent ML/TF, and to report suspicious transactions.

TWO. RESPONSIBILITIES OF AFSP

2.1. The risks associated with ML/TF vary from country to country and depend on various factors for each REs, such as the products and services, the type of delivery channels, geographic location, and type of customers. AFSP need to take steps to manage and mitigate potential risks. These measures are important to prevent from being exploited by criminals and to prevent illegal money from entering the financial system. Hence, the AML/CFT Law details the importance of responsibilities as implementing risk management, CDD and reporting suspicious transactions.

2.2. REs must have internal control and risk management program for ML/TF activities approved by its management, and the responsibilities of management and staff at all levels must be clarified. A system for monitoring the program should be established and, if necessary, the effectiveness of its implementation should be assessed by an independent body.



2.3. The Mongolian Institute of Certified Public Accountants (MONICPA) is a self-regulatory body responsible for overseeing the implementation of an effective supervisory program of AFSPs under the AML/CFT Law. The AML/CFT related documents and regulations must comply with the requirements of regulatory bodies such as the MONICPA and the FIU.

2.4. AFSPs must have an internal control program, whether it is an individual or a legal entity. If it is a legal entity with lots of subsidiaries, then all its subsidiaries and branches must implement an internal control program.

2.5. Internal control is the policy document of the REs to prevent, manage and comply with ML/TF risks. The internal control program must be consistent with the size, nature, structure, and organization of the REs and must be able to take effective measures to mitigate and prevent ML/TF risks.

2.6. Under the AML/CFT Law, AFSP must send its internal control program to the MONICPA for registration. The internal control program should include the following:

- methodology for assessing risks associated with customers and the delivery channel of products and services;
- regulation of measures to mitigate risks associated with new technologies and high-risk products and services, as well as methods of their delivery channel;
- CDD and enhanced CDD procedure;
- implementation of procedure for enhanced CDD for ML/TF high risks;
- procedures for conducting CDD process by third parties;
- procedures for detecting suspicious transactions, ensuring the confidentiality of information, providing information to the FIU and other authorities, and transferring and storing documents (record keeping);
- procedures to implementing sanctions imposed by the UN Security Council, other relevant governmental and international organizations;

- procedures for special monitoring activities;
- procedures for the appointment and dismissal of officials authorized to monitor the implementation of the AML/CFT Law and the internal control program, as well as their rights and obligations;
- internal training program for implementing the AML/CFT Law and other relevant regulations;
- other acts and requirements specified in the administrative regulation issued in accordance with the relevant law.

2.7. AFSP shall appoint a compliance officer to ensure the implementation of the ML/TF risk-based approach. The compliance officer has a specific role to play in preventing, detecting, suspending, and taking effective action against ML/TF related crimes. Therefore, it is important that the compliance officer has relevant experience, knowledge and skills and has appointed by the top management of the organization.

2.8. The compliance officer performs specific functions in the AML/CFT are. Such as, monitoring compliance with the AML/CFT Law and internal control programs, supporting the development and implementation of an AML/CFT culture in the organization, supervising the analysis of suspicious transaction reports, reporting suspicious transactions to the FIU, and organizing AML/CFT trainings for staff.

THREE. ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH

3.1. REs stated in the Article 4.1 of the AML/CFT Law should implement a risk-based approach for combating ML/TF and the following risks should be assessed in accordance with the specifics and scope of the activities realistically:

- Customer risk;
- Risks associated with the product and services and its delivery channel;
- Geographical risk.

3.1.1 Customer risk

Before providing any services, an AFSPs should assess the ML/TF risks pf its customers and their beneficial ownership. Customer risk is the overall ML/TF risk posed by the customer. Identifying customer-related risks helps to determine the extent to which business structures are evaluated. The complex organizational structure of the client and the policy of excessive information confidentiality may increase the ML/TF risks and can be the basis to carry out an enhanced CDD measure. For example, if the

customer or the beneficial owner is a politically exposed person then it is necessary to conduct an enhanced CDD measure.

Customer risk factors

- Customers conducting their business relationship in an unusual or unconventional circumstances (for example, starting a business relationship not in person);
- Non-resident customers;
- a customer who is responsible for and manages the assets on a contractual basis;
- a customer which is a legal entity with a complex form of ownership.

3.1.2 Risks associated with the product and services and its delivery channel

Risks associated with the product and services are an expression of the vulnerability of using a particular product or service for ML/TF activities. AFSPs should assess the risk of a product or service being used for ML/TF activities before recommending it to their customers. They should enhance their monitoring and supervision over high-risk ML/TF product or service.

Factors affecting to the risks associated with the product and services and its delivery channel:

- a service that allows the information of beneficial owner to be obscured from the authorities
- services that rely on new technologies;
- financial or tax advisory services that can be provided without sufficient customer information;
- management and storage of accounts and funds without verification.

3.1.3 Geographical risk

Before establishing any business connections, AFSPs should so some research on the customer's country of origin and assess whether he/she comes from a ML/TF high-risk country. Geographical risks are determined by the country's corruption rate, crime statistics and regulatory regimes on AML/CFT etc.

Geographical risk factors:

- Countries/jurisdictions identified by FATF as having weak AML/CFT regimes (FATF and APG, EAG's mutual evaluation report should be considered);

- Countries/jurisdictions designated in the financial sanctions, restrictions or similar measures issued by international organizations;
- countries/jurisdictions identified by credible sources as having significant levels of corruption, bribery, and criminal activities
- countries/jurisdictions identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within their country.

3.2 Like other REs, AFSPs must conduct risk assessments, keep the records and regularly update the information, and make it available to the competent authorities. Based on the results of the risk assessment, AFSPs should have appropriate measures to manage and mitigate corresponding risks that should be included in its AML/CFT internal control strategies, policies, and procedures. Additional risk management and mitigation measures must be taken for high-risk customers.

3.3 Based on the risk assessment, risks can be managed by implementing the following measures:

3.3.1 collecting additional information related to the customer, its beneficial owner, and their corresponding transactions;

3.3.2 having sufficient information about the person, the customer, and its beneficial owners who's making the transaction, In this context, it is necessary to obtain information on the purpose of the business relationship established with the REs, origin of the assets and income, employment, and the scope of the business of the customer;

3.3.3 carrying out enhanced CDD activities for high risk customers in accordance with the customer, delivery channel and geographical risks;

3.3.4 Regularly monitor whether the financial, business relations and transactions established with the customer are in accordance with the relevant information about the customer and the source of funds;

FOUR. CUSTOMER DUE DILIGENCE (CDD)

4.1. CDD is the process of customer identification which uses official documents, government databases and other credible sources to verify the information such as who they represent, what they do, and for what purpose they carry out activities from the

customer. It is intended to identify and verify information about the beneficiaries, management, beneficial owner and their representatives.

4.2. The AFSPs and other REs have the following benefits from implementing CDD:

4.2.1 AFSP can prevent ML/TF risks from its operations, and to protect the financial system from such risks;

4.2.2 Avoid committing or attempting to commit a crime using the products and services provided by the AFSPs to its customers;

4.2.3 Detect and report suspicious transactions and actions that could damage the reputation of the AFSPs and lead to financial losses;

4.2.4 AFSP can continue its business operations stable.

4.3. As specified in the Article 5 of the AML/CFT Law, the AFSPs and other REs are obliged to identify customers using official sources, documents, information, and credible information sources in the following cases:

4.3.1 prior to establishing a business relation;

4.3.2 prior to conducting occasional transactions equal to or more than 20 million togrogs (or equivalent foreign currency) of entity who has not established consistent business relations and who has no permanent bank account;

4.3.3 if the total sum of several inter-related transactions made within 24 hours is 20 million togrogs (equivalent foreign currency) or above even the individual value of any of these transactions is less than the threshold;

4.3.4 if there are doubts about the authenticity and accuracy of previously obtained information on customer;

4.3.5 if there are grounds to suspect that the customer or the transaction is involved with money laundering or terrorism financing.

4.4. There are three different levels of CDD:

4.4.1 Customer due diligence for all customers;

4.4.2 Simplified CDD for customers with low risk;

4.4.3 Enhanced CDD for customers with high risk (for example, politically exposed persons, citizens, and legal entities on the list of countries designated in the sanctions, etc.).

4.5. Verification of customer information should be carried out within the requirements in the Preventive measures regulation on ML/TF approved by the Governor of the Bank of Mongolia's decree No. A-26 in 2019. The purpose of this process is to identify,

verify, and document the information of the REs' customers, its beneficial owner, or clarify the entity that owns, manages, or benefits. If the customer has a multi-level structure, it is necessary to identify and document the persons at each level of ownership until the beneficial owner and management are identified.

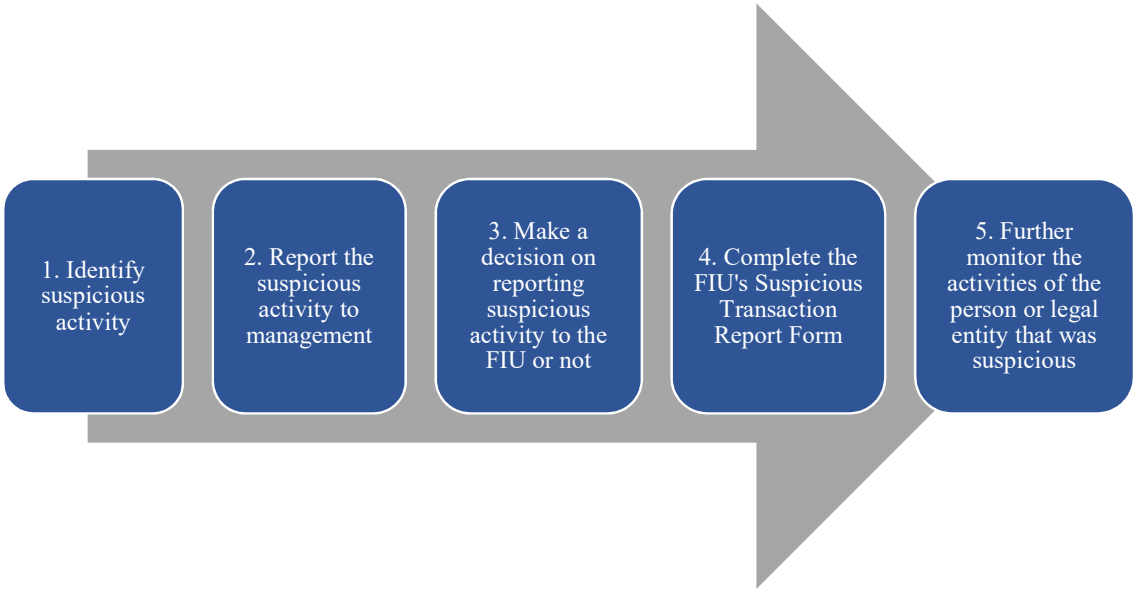
FIVE. SUSPICIOUS TRANSACTION REPORT

5.1. A transaction or activity is considered suspicious if the AFSP suspects or finds out that the transaction or activity is related to the ML/TF or the proceeds of crime while providing activities specified in the AML/CFT Law to the customer.

5.2. Suspicious transactions and activities may vary depending on the type of customers, financial situation, and the nature of the business. AFSPs and other REs shall detect the grounds for suspicion and assess the ML/TF risks whether the transaction, activity, or attempt was made or are about to make.

5.3. There are no threshold amount for suspecting transactions, activities, and attempts that may be related to the ML/TF activities or the proceeds of crime, and these should be reported to the FIU regardless of the amount.

5.4. The AFSPs shall report and monitor suspicious transactions and activities in accordance with the following steps:



5.5. Although it is not possible to identify suspicious transactions by common characteristics, the following attributes are common in the AFSP sector:

5.5.1 customers who own assets more than their income and the source of funds is not clear;

5.5.2 regular transactions are inconsistent with his/her employment status;

5.5.3 regularly refuses or obviously annoys when asked to provide information in accordance with the laws and regulations;

5.5.4 changes in the frequency, type, and size of previous regular transactions for unknown reasons;

5.5.5 transactions made on false (suspected to be false) documents;

5.5.6 attempting to make a transaction/activity by influencing the employee who provides financial services illegally;

5.5.7 transaction made through a country/jurisdiction with no established AML/CFT mechanism;

5.5.8 fees for services and sales of products that are too unrealistic;

5.5.9 various individuals making significant amounts of deposit into one account without providing sufficient information;

5.5.10 transactions which are inconsistent with its corresponding agreement or contract;

5.5.11 transactions which are returned in full within a short period of time after receiving from a foreign country;

5.5.12 incomplete information of transferor and recipient;

5.5.13 customers who have changed their accountants every year;

5.5.14 customers who don't know the location of their organizations' document storage, and the location of the documents are not clear;

5.5.15 companies that regularly reflects receivables and payables in their current financial statements, but the accounts are inconsistent or non-existent;

5.5.16 companies that have no employees and their business activities are uncommon;

5.5.17 companies that pay an offshore company an unusual and excessive amount of consulting fees;

5.5.18 companies that report their expenses more than their income and pretend to have a loss, but continue to operate without justification;

5.5.19 companies that do not make a profit, and it is not clear how they continue to operate their activities regularly.

5.6 When submitting information to the FIU, the AFSP shall follow the Guidance for REs for filling out the report and submitting it to the FIU.

5.7 The FIU has the right to obtain additional information as the copy of the account of the customer involved in the suspicious transaction, a copy of the documents used to open account, and a document assessing the risk of the customer from the AFSP.

SIX. CONFIDENTIALITY AND PROHIBITIONS

6.1. The submitting of reports by AFSPs to the FIU and competent authorities, in accordance with provision of the AML/CFT Law, shall not be deemed as a breach of banking, professional, customer, business entity or organization, business or other secrecy confidentiality.

6.2. The management and employees of AFSPs are prohibited from disclosing any information related to transactions reported to the FIU to any person or legal entity other than authorized law enforcement and counterterrorism agencies under the AML/CFT Law.

6.3. It is prohibited to notify the customer, individual, and legal entity about the information of them has prepared, is going to be reported or has been reported.

6.4. If information submitted by AFSPs has not been proven to be relating to ML/TF shall not serve as ground to impose civil, criminal and other liability on the person and entity submitted such an information.

SEVEN. RECORD KEEPING

7.1. Under the Article 8.1 of the AML/CFT Law, AFSPs should shall retain information and records of transactions, accounts and information of customers obtained in accordance with Article 5 and 6 of the AML/CFT law for at least five years after the date of transaction or the closure of the account:

7.1.1. Records relating to the establishment of a customer relationship including account opening documents and documents relating to CDD procedures, including copies of identification document should be kept for 5 years after the customer relationship has ended, or where such documents have arisen from an occasional transaction.

7.1.2. Records and documents relating to enhanced CDD procedure; the updates of customers' information; agreement on correspondence relationship, memorandum, and records used to identify ML/TF risk, documents on analysis of ongoing CD, analysis of enhanced monitoring of transactions, information

and documents relating to suspicious transaction reports should be stored for at least 5 years after the customer relationship has ended.

7.1.3. Cash and non-cash transaction documents must be kept for at least 5 years from the date completion of the transaction.

7.2. According to the AML/CFT Law and regulation on preventive measures against ML/TF, the storage of documents shall contain all information related to the transaction and shall keep records and information in a way that they can be made available on timely basis to competent authorities.

7.3. Under the AML/CFT Law, the documents shall be archived and should comply with relevant standards to be used for evidence.

EIGHT. TRAINING AND AWERENESS RAISING ACTIVITIES

8.1. Under the AML/CFT Law and Recommendation 18 from FATF, the AFSPs will have internal training program for ensuring the implementation and compliance with AML/CFT Law and other relevant regulations as part of their internal control program.

8.2. Trainings on AML/CFT should be organized regularly and contents of the training should be updated regularly by the legal environment, circumstances, risk assessment and staff responsibilities. Thus, the employees will be able to understand the latest information and trends and be able to perform their duties in AML/CFT procedures effectively.

NINE. SOURCES USED

AML/CFT Guidance for Accountants, Financial Intelligence Unit of Trinidad and Tobago, 2015, https://www.fiu.gov.tt/wp-content/uploads/AMLCFT-Guidance-for-Accountants-Revised-as-at-September-2015-2.pdf

Anti-money laundering guidance for accountancy sector, CCAB-Accountants for Growth, 2018, https://www.ccab.org.uk/documents/FinalAMLGuidance2018Formattedfinal.pdf

APG Yearly typologies report 2015: Methods and Trends of Money Laundering and Terrorism Financing, Asia Pacific group on Money Laundering - Sydney Australia : APG Secretariat, 2015, http://www.apgml.org/documents/searchresults.aspx?keywords=APG+Yearly+typologies+report+2015

Case Studies on Fighting Money laundering, Terrorism Financing and Economic Crime, ICPAC, 2018, https://www.icpac.org.cy/zePortal/WebFiles/SELK/WebDocuments/Members/Specialized%20Technical%20Material%20-%20Guides/Anti%20Money%20Laundering/Case%20studies%20Pack%202018.pdf

FATF Report on Money Laundering Typologies, FATF, 2003-2004, http://www.apgml.org/documents/search-results.aspx?keywords=FATF+Report+on+Money+Laundering+Typologies

Helping professional accountants recognize and fight economic crime, CCAB, 2016, https://www.ccab.org.uk/documents/CCABEconomicCrimeCaseStudiesFINAL.pdf

Risk-based Approach for the Accounting Profession, FATF, 2019, https://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Accounting-Profession.pdf

Guidance for preventing ML/TF for non-bank financial institutions, Financial Regulatory Commission.

Combating money laundering and terrorist financing, Bank of Mongolia, 2019, https://www.mongolbank.mn/documents/financialliteracy/publications/23.pdf

AML/CFT Law, 2013, https://www.legalinfo.mn/law/details/9242

Prevention of money laundering and terrorism financing, Bank of Mongolia, Public Education, Information Center, 2018, https://www.mongolbank.mn/documents/financialliteracy/publications/16.pdf

International standard on AML/CFT, FATF, Bank of Mongolia, 2012-2019, https://www.mongolbank.mn/documents/cma/20180531F2.pdf

Guidelines for the implementation of risk-based approaches in AML/CFT, Bank of Mongolia, 2018, https://www.mongolbank.mn/documents/regulation/control_check/20180206_A32.pdf

Preventive Measures Regulation on ML/TF, Bank of Mongolia, 2019, https://www.mongolbank.mn/documents/regulation/control_check/20160920_terrorism.pdf

Regulation on submitting reports to FIU, Bank of Mongolia, 2019, https://www.mongolbank.mn/documents/regulation/control_check/20191225_A326.pdf

What is a Suspicious transaction?, Bank of Mongolia, 2020, https://www.mongolbank.mn/listCMA.aspx?id=2

The role of the tax administration in detecting tax evasion crime, Galbadrakh. B, S.Tugsjargal, Mongolian Association of Criminologists, 2014, http://criminology.mn/post/188

Analysis of the circumstances of the tax evasion crime, its causes and factors, Zolboo.G, 2017, page number 6-8, http://legaldata.mn/b/396

Law on combating proliferation and terrorism, 2019, https://www.legalinfo.mn/law/details/14696

Regulation for financial sanctions against the proliferation of weapons of mass destruction and terrorism, 2019, https://www.legalinfo.mn/annex/details/10532?lawid=15003