Bank of Mongolia

Financial Information Unit

SUSPICIOUS TRANSACTION REPORTING GUIDELINE

BANKS

May 2020

GLOSSARY

AML/CFT Law	Law on Combating Money Laundering and Terrorism financing
ATL	Law on Combating Proliferation of Weapons of Mass Destruction a Terrorism
BOM	Bank of Mongolia
CTR	Cash Transaction Report
FATF	Financial Action Task Force
FIU	Financial Information Unit
FRC	Financial Regulatory Commission
FSTR	Foreign Transaction Settlement report
ML/TF	Money laundering and terrorist financing
PMR	Preventive Measures Regulations on Combating Money Laundering and Terrorism Financing
RE	Reporting Entity
STR	Suspicious Transaction Report
UN	United Nations
UNCAC	United Nations Convention Against Corruption
UNSCR	United Nations Security Council Resolution

CONTENT

1 INTRODUCTION 4
1.1 BACKGROUND 4
1.2 PURPOSE 4
1.3 GUIDANCE MATERIAL 4
2 AML/CFT 5
2.1 WHAT IS MONEY LAUNDERING? 5
2.2 THREE STAGES OF MONEY LAUNDERING 5
2.3 DEFINITION OF MONEY LAUNDERING 6
2.4 TERRORIST FINANCING VS MONEY LAUNDERING 6
2.5 WHAT IS A TERRORIST ACT? 6
2.6 DEFINITION OF TERRORIST FINANCING 6
2.7 TARGETED FINANCIAL SANCTIONS 6
2.8 AML/CFT INTERNATIONAL STANDARDS 7
2.9 DOMESTIC LEGISLATION 8
3 SUSPICIOUS TRANSACTIONS 8
3.1 IDENTIFYING SUSPICIOUS TRANSACTIOS 9
3.2 WHO MUST REPORT? 10
3.3 WHAT TO REPORT? 11
3.4 HOW TO REPORT? 11
4 RECORD KEEPING 12
5 MANAGEMENT AND STAFF TRAINING 12
5.1 CONTENT OF TRAINING 13
5.2 TRAINING MODALITIES AND FREQUENCY 13
6 INDICATORS 14
6.1 WHAT ARE INDICATORS? 14
7 REQUESTS FOR INFORMATION 14
7.1 FIU REQUEST FOR INFORMATION UNDER THE AML/CFT lAW 14
8 OFFENCES AND PENALTIES 15
9 TIPPING OFF 15
10 PROTECTION 15
APPENDIX 1. INDICATORS 16
1. COMMON INDICATORS 16
1.1. GENERAL AREAS OF SUSPICION 16
1.2. suspicious indicators related to product and service 19
2. Industry Specific Indicators 29
MONEY SERVICE BUSINESSES (INCLUDING CURRENCY EXCHANGE AND MONEY REMITTANCE) 29
LIFE INSURANCE 29
INVESTMENT 29
CASH COURIERS 30
TRUST AND COMPANY SERVICE PROVIDERS 30
APPENDIX 2. TYPOLOGIES 31

1 INTRODUCTION

This guideline has been issued to provide information and guidance for BANKs as an reporting entity according to Article 4.1.1 of AML/CFT law to submit Suspicious transaction reports to FIU.

Bank employees need to have common knowledge of AML/CFT and preventive measures in order to identify, detect, and report suspicious transactions and attempts of suspicious transaction, activity.

It aims to provide information on legal requirements to report suspicious transactions to the FIU, as well as general information and knowledge related to money laundering and terrorist financing.

1.1 BACKGROUND

In accordance with the AML/CFT Law, the Banks obliged to take a number of measures as identifying and verifying customers, beneficial owners, undertaking enhanced monitoring of transactions, and submitting a report about suspicious transactions, cash and foreign settlement transactions above MNT 20 million to the FIU.

This guideline outlines and explains only the obligation to report suspicious transactions to FIU.

It is developed in accordance with the AML/CFT Law, Law on combating terrorism and proliferation, Preventive measures regulations on combating money laundering and terrorism financing (PMR), Regulation for submitting information electronically from reporting entities to Financial Information Unit and Regulation for implementing sanctions relating to counter terrorism and proliferation.

1.2 PURPOSE

This guideline has three main objectives:

- To explain money laundering and terrorist financing basics;
- To help bank employees to understand and comply with suspicious transaction reporting obligations by specifying who must report, what details to include, when to report, and how to report.
- To help reporting entities to identify suspicious transactions by providing both general and industry specific indicators.

1.3 RELATED REGULATIONS AND GUIDANCES

The FIU regularly issues range of material related to the AML/CFT environment. This material is available on its website at https://fiu.mongolbank.mn/regulation.aspx.

Documents issued for internal use for RE’s not posted on the website can be obtained by contacting the FIU's trough official e-mail fiu@mongolbank.mn.

In addition, the Bank of Mongolia (BoM) and the Financial Regulatory Commission (FRC) regularly issues on their websites manuals, guidelines, information and other relevant legal acts issued for their regulated entities.

2 COMBATING MONEY LAUNDERING AND TERRORISM FINANCING

2.1 WHAT IS MONEY LAUNDERING?

The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money laundering is the process of concealing the illicit source of proceeds of crime and disguising it as legitimate income. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardizing their source. [1]

Illegal arms sales, smuggling, and the activities of organized crime, including drug trafficking and prostitution rings, can generate huge amounts of proceeds. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimize" the ill-gotten gains through money laundering. When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention

This activity of processing of these profits to disguise their illegal origin is known as money laundering. Money laundering offers criminals the ability to openly use the proceeds of crime and to escape sanctions from their illegal activity.

2.2 THREE STAGES OF MONEY LAUNDERING

There are three stages involved in money laundering. These are described below:

1. Placement: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 (checks, money orders, etc.) that are then collected and deposited into accounts at another location.

   Layering: 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.

2. Integration: Having successfully processed his criminal profits through the first two phases the launderer then moves them to the third stage – integration – in

[1] http://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223

which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

A money laundering scheme will typically but not necessarily involve all three stages.

2.3 DEFINITION OF MONEY LAUNDERING

Money laundering is defined in Article 3.1.1 of the AML/CFT Law. The key elements of a money laundering offence are:

"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.".

2.4 TERRORISM FINANCING VS MONEY LAUNDERING

Terrorism financing and money laundering both require the movement of funds, preferably, with minimal scrutiny. Therefore, bank employees need to be well-informed and well-monitored, and have the same level of controls and measures to detect and prevent suspicious transactions related to money laundering and terrorist financing.

Unlike money launderers, terrorist organizations can raise funds through legitimate sources as well as criminal activity. Historically, terrorist financiers have utilized specific methods to add complexity or legitimacy to transactions including the use of alternative remittance services, charitable organizations, and cash couriers.

2.5 WHAT IS A TERRORIST ACT?

Terrorist act is defined in Article 3.1.4 of the Law on combating terrorism and proliferation (LCTP). The key elements of this offence are:

"any act of frightening population through demanding government or international organization to act or not to act illegally, or killing, or causing health or material damages to a person, or causing death or injury to a person refusing actively participate in any part of armed conflict in pursuit of political, religious, ideological and other identical goals".

2.6 DEFINITION OF TERRORISM FINANCING

Terrorism financing is defined in Article 3.1.2 of the AML/CFT Law. Under this Article, terrorism financing is defined as:

"means direct or indirect collecting, converting, transferring or disposing any assets knowing such assets are intended to be used by terrorist person for terrorist act or activity".

2.7 TARGETED FINANCIAL SANCTIONS

The LCTP, the AML/CFT Law, and the Regulation for implementing sanctions relating to counter terrorism and proliferation establish a legal framework for the freezing of funds and property of persons, entities and organizations designated by United Nations pursuant to the United Nations Security Council (UNSCR) 1267 and successor resolutions and those designated by Mongolia pursuant to UNSCR 1373 and successor resolutions and for prohibiting the dealing of the funds and property of designated persons (together referred to as targeted financial sanctions).

The requirement to implement targeted financial sanctions is set out in Article 5 of the Regulation for implementing sanctions relating to counter terrorism and proliferation and contains the following elements:

i/ All persons and entities in Mongolia, and all Mongolian nationals and entities incorporated under Mongolian law wherever located, shall freeze, without delay and without prior notice, the assets that are directly or indirectly, owned or controlled by a person or entity designated by UNSCRs, or any other successor resolution, at the request of a foreign authority and the Government and report to the FIU and GIA.

ii/ Financial and business entity is prohibited by financing directly or indirectly, or to give him/her economic source, and provide financial and other services to person, entity or a person related to or entity acting on behalf of designated by UNSCRs, or any other successor resolution, at the request of a foreign authority and the Government.

iii/ In fulfilling its obligations specified in i/ii of this guideline, a financial or business entity shall freeze the following assets:

- assets that wholly or jointly, owned or controlled by a designated person or entity, and not just those assets that can be tied to a particular act, plot or threat;
- all assets that wholly or jointly, directly or indirectly, owned or controlled by the designated person or legal entity;
- assets generated from the assets specified in the first 2 of part iii of the guideline, as well as assets of the person or legal entity acting on behalf on the instructions of the person or legal entity designated by UNSCR;
- watercraft designated by the relevant UNSCR.

2.8 AML/CFT INTERNATIONAL STANDARDS

2.8.1 INTERNATIONAL STANDARDS

Key AML/CFT standards include:

- *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) 40 Recommendations - revised February 2012.*

2.8.2 FINANCIAL ACTION TASK FORCE - FATF

The Financial Action Task Force (FATF) is an inter-governmental body founded in 1989 that sets international standards against which most countries measure their ability to combat money laundering and terrorist financing.

FATF sets international standards of laws, regulations and procedures for combating ML/TF ad proliferation and other illicit activities which harms the international financial system. Jurisdictions accept the FATF Recommendation as AML/CFT Standard.

In other words, The FATF Recommendation set out a comprehensive framework for the jurisdictions' comprehensive action to combat ML/TF and the proliferation of weapons of mass destruction. As countries have different legal, administrative, social, economic, and financial systems, the ways to deal with these threats are also different. Therefore, the FATF Recommendation can be understood as setting international standards for countries to adapt to their specific circumstances.

Mongolia a member of the Asia Pacific Group on Money Laundering which is a FATF Style Regional Body.

PS: FATF Recommendation is available for download on the FATF website[2]. Also, the Mongolian translation is available at FIU website and at FATF website.[3]

2.9 DOMESTIC LEGISLATION

Key AML/CFT laws and regulations in Mongolia that need to be complied with and of which implementation is necessary:

- ✓ *AML/CFT Law*
- ✓ *Law on Combating Terrorism and Proliferation*
- ✓ *Preventive Measures Regulations on Combating Money Laundering and Terrorism Financing*
- ✓ *Regulation for submitting information electronically from reporting entities to Financial Information Unit*
- ✓ *Regulation for implementing sanctions relating to combating terrorism and proliferation*

3 SUSPICIOUS TRANSACTIONS

[2] **FATF Recommendations 2012**
http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

[3] http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Mongolian%20Translation%20FATF%20Recommendations%20mng.pdf

Pursuant to Article 7.2 of the AML/CFT Law, banks are required to report suspicious transactions when:

"A reporting entity suspects or knows that an asset, income or transaction, or attempted transaction is related to money laundering or terrorism financing, or is related to proceeds of crime".

SUSPICIOUS TRANSACTION REPORT (STR)

The FIU relies on reporting entities to fulfil their obligation to report transactions where it is suspected that the transaction is linked to money laundering, terrorist financing or is the proceeds of crime.

STRs are the main source of information available to the FIU to detect suspected offences. A STR can indicate that suspected criminal activity is occurring through a transaction or series of transactions.

Reports received by the FIU are analyzed for activities and patterns that may indicate criminal offending. Various resources are used including law enforcement, partner agencies and open-source data.

Often, additional information is required from reporting entities to help establish whether the suspicious activity reported in a STR merits further investigation. This additional information can be vital in determining whether the suspicion of offending translates into actual criminal activity.

Where criminal activity appears to be occurring, cases may be referred to investigative agencies involved in law enforcement.

IMPORTANT: The requirement to report STRs applies to completed or attempted transactions and there are no monetary thresholds for reporting.

3.1 IDENTIFYING SUSPICIOUS TRANSACTIOS

As a general rule, a suspicious transaction will often be one which is inconsistent with a customer's known activities and profile or with the normal business expected for that type of Customer.

In many cases, reporting entities will be unaware what the actual criminal activity is. However, by screening transactions for indicators, typologies, and unusual activity, a suspicion of criminal offending may arise. A transaction may have many factors that, considered individually, do not raise a suspicion, but, considered collectively, suggest criminal activity.

Reporting entities can seek guidance as to what could constitute an STR from the list of indicators provided by the FIU. However, this list of indicators is for guidance only. What is a STR will ultimately be determined by the reporting entity's knowledge of its customers and information collected for KYC procedures.

3.1.1 GROUNDS FOR SUSPICION

A suspicious transaction must be reported when a reporting entity has formed a suspicion which is a subjective belief of the reporting entity and, amongst others, will be based on the reporting entity's knowledge of the customer, namely his or her profile.

Customer due diligence measures undertaken by the reporting entity will provide it with information and knowledge on the customer and will be crucial to enabling the reporting entity to identify a STR.

All STRs should contain grounds for suspicion explaining why the transaction (or proposed transaction) is considered suspicious. For example, stating that a transaction is suspicious because the transaction is large without any supporting grounds is not sufficient on its own. A large transaction may be considered suspicious where it does not fit with the customer's financial or transactional profile. Comparing the transaction to previous account records may prove helpful and demonstrate reasonable grounds. In other words, prior to reporting a STR about any customer or transaction, the bank employee should examine the customer and transaction, make a preliminary analysis of the information available to him or her, and carefully examine the signs of suspicion to determine whether there are sufficient grounds for suspicion. In this case, the bank employee will have good reason to believe that the customer or transaction may be related to money laundering, terrorist financing, or illegal activities or crime.

Furthermore, attaching this information to the STR will assist the FIU to understand your grounds for suspicion. This information can demonstrate how the suspicious transaction in question is unusual and whether any patterns indicating criminal activity exist.

Suspicion may be raised by staff or by account monitoring processes. Where frontline staff have formed a suspicion, it is important that the basis for this suspicion is recorded and supplied in any subsequent STR. Liaison between frontline staff and reporting entity's AML/CFT compliance officer may assist in verifying the basis of suspicion. It is expected that before STRs are submitted to the FIU they will go through internal screening to ensure the matter satisfies the requirements of the law.

3.2 WHO MUST REPORT?

If you are a reporting entity, as defined in Article 4.1 of the AML/CFT Law, any transactions conducted (or attempted) using your services that are considered suspicious must be reported to the FIU. REs as:

4.1.1. **BANK**;
4.1.2. non-bank financial institutions;
4.1.3. insurance companies and insurance licensed entities;
4.1.4. investment funds; investment management company;
4.1.5. licensed securities market entities;
4.1.6. savings and credit cooperatives;
4.1.7. real estate agents who are involved in any activity of buying and selling of real estate;

4.1.8. Dealers of precious metals and precious stones and parties engaged in sales of those manufactured items – when they engage in cash transaction equal to or above the threshold specified in article 5.1.2 of AML/CFT Law;

4.1.9. notaries, lawyers, accountants and other financial management counsellors – when they prepare, conduct and involved in following activities in relation to a customer:

4.1.9.a. buying and selling of real estate;

4.1.9.b. managing of client's assets;

4.1.9.c. management of bank, savings or securities accounts;

4.1.9.d. organizing of contributions for the creation, operation or management of companies;

4.1.9.e. creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

If a decision is made to complete a STR, the person directly involved in the transaction need not necessarily submit the report to the FIU. Reports can be made by supervisors, managers, compliance officers or others tasked with submitting STRs to the FIU. It is the responsibility of that person to submit the report to the FIU.

3.3 WHAT TO REPORT?

Pursuant to Article 9 of the AML/CFT Law, a STR submitted to the FIU must contain:

- *Name and addresses of the entities specified in Article 4.1 of this law and the identity of the officials who submitted the information;*
- *Information on customers and beneficiaries;*
- *Information on purpose, value, form, date, account number, account holder and other participants of the transaction;*
- *Brief explanation of grounds and circumstance to suspect the transaction;*
- *Other related documents.*

If bank suspects or knows that an asset, income or transaction, or attempted transaction is related to ML/TF, or related to proceeds of crime it shall submit a STR to the FIU within 24 hours in accordance with approved procedures and formats.

Once the requisite suspicion is formed, the 24-hour requirement commences.

After an initial STR has been submitted, a reporting entity may continue to conduct business with the Customer. However, they must comply with all relevant provisions of the AML/CFT Law, including the requirement to submit additional STRs where appropriate. In other words, it is important to note that the law prohibits RE from disclosing, notifying, transmitting, or disclosing information about suspicious transactions to customers other than those authorized by law enforcement and counterterrorism agencies. .

If necessary, the bank is obliged to provide additional information related to the FIU to the FIU and comply with other relevant provisions of the AML/CFT Law.

3.4 HOW TO REPORT?

Reporting entities must transmit reports to the FIU as required by the Regulation for submitting information electronically from reporting entities to Financial Information Unit. Instruction on how to fill out the Suspicious Transaction Report is described on the Guidance for Completing Reports (CTR, FSTR and STR).

4 RECORD KEEPING

As a reporting entity for purposes of Article 8 of the AML/CFT Law you must keep and maintain records of all transactions, including STRs, for at least 5 years after the transaction made.

STR records to keep include suspicious transactions executed and those attempted.

The 5-year period commences after the transaction has been attempted or executed. You also need to maintain records in a manner and form such it is readily available to FIU or other competent authorities.

5 MANAGEMENT AND STAFF TRAINING

Bank must ensure that appropriate personnel are trained in applicable aspects of relevant legislation, regulations, guidelines and the institution's own internal policies and procedures pertaining to AML/CFT.

REs obliged to have the internal control program in accordance with the Article 14 of the AML/CFT Law as "Internal Training Program to Ensure the Implementation of the Law on Combating Money Laundering and Terrorism Financing and other relevant regulations". Training should be designed to improve the knowledge, performance and skills of employees by enhancing their understanding of relevant laws and regulations, the reporting entities internal controls etc. The training should be tailored to the person's specific responsibilities within the institution.

For STR reporting, the relevant staff should be trained in identifying transactions that are suspicious. In this regard, staff members should be familiar with the indicators set out in the guidelines. In addition, reporting entities should ensure that staff are trained on the internal processes and procedures upon forming a suspicion that a transaction should be reported as an STR.

Training should be an ongoing process that should be updated regularly to reflect current developments and changes to laws and regulations and the reporting entities' business environment and the type of customers and products.

Training will focus on employee consciousness and understanding of AML requirements, internal policies and processes and STR indicators and the potential consequences of an employee's failure to comply that could cause potential civil and criminal liability and penalties for both the institution and the employee..

Training is one of the most important ways to ensure that AML/CFT measures are being implemented within the institution. However, institutions should avoid adopting a 'one size fits all' approach as this will result in some staff not benefiting as they are exposed

to material that is not relevant to their role, whilst others can end up being under-trained for their role and responsibility.

5.1 CONTENT OF TRAINING

As a minimum, the content of training delivered to management and staff should include:

- The background and history pertaining to AML/CFT controls, what money laundering and terrorist financing are, how and why they happen and why detecting and preventing them is important;
- International standards that drive domestic requirements;
- Predominant AML/CFT typologies in the country and the financial sector in which the institution operates;
- Domestic AML/CFT legislation, regulation and any guidelines issued by regulatory authorities;
- National Risk Assessment of the ML/TF;
- The potential ML/TF risks to the institution that have been determined from the institution's risk assessment;
- Feedback on AML/CFT issues arising from audit or regulatory reports;
- The AML/CFT duties and responsibilities assigned to the various roles of staff in the institution e.g. administrators, front line staff, sales staff, back office staff compliance staff, AML/CFT officer(s), senior managers and the board of directors including:
  - How to react when faced with a suspicious client or transaction;
  - How to respond to customers who want to circumvent reporting requirements;
  - Internal policies, such as customer identification and verification procedures and CDD policies;
  - What the legal recordkeeping requirements are;
  - Suspicious transaction reporting requirements;
  - Cash and foreign settlement transaction reporting requirements;
  - Duties and accountability of employees;
  - The details of the institution's AML/CFT programme and the internal processes that have been implemented.

5.2 TRAINING MODALITIES AND FREQUENCY

Training should not just be a "one off", formal process although this approach can be applied to new staff when they join the institution. Beyond that training should take many forms and be an almost continuous process. There are various ways training can and should be delivered including:

- Formal face to face or online AML/CFT training and assessment modules that all staff would complete in a phased approach;
- Emails and newsletters that are read by all staff. These may remind staff of systems, processes and risks;
- Periodic team meetings that will discuss specific issues relevant to that team;
- Compliance officers (either internal or external to the institution) providing comment and guidance;

- Management providing briefings that include AML/CFT comment;
- Organizational strategies that regularly address AML/CFT issues being communicated to management and staff.

6 INDICATORS

6.1 WHAT ARE INDICATORS?

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

It is important for bank employees to be aware of these symptoms, especially suspicious and disturbing symptoms related to the industry, product or service in which their organization operates. This will help determine if the customer's transaction or attempt to make a transaction is suspicious.

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

A list of internationally established indicators is provided in Appendix 1. This list is divided into (1) common and (2) industry specific indicators. The indicators are based on literature from the FATF, overseas FIU's , and domestic partner agencies.

NOTE:
The list of indicators in Appendix A is offered as a guide and it is not an exhaustive list of every possible indicator. Staff should be aware that criminals and organized crime groups regularly adapt their behavior to exploit weaknesses within different industries to launder funds.

7 REQUESTS FOR INFORMATION

Often, additional information is required from reporting entities to help establish whether the suspicious activity reported in a STR merits further investigation. This additional information can be vital in determining whether the suspicion of offending translates into actual criminal activity and whether further resources are deployed.

7.1 FIU REQUEST FOR INFORMATION UNDER THE AML/CFT LAW

Pursuant to Article 9.2 of the AML/CFT Law, FIU has a right request additional information to assist it to make a determination as to whether the reporting entity's suspicion is valid or to determine whether there is any criminal offending.

"Regulation for submitting information electronically from reporting entities to Financial Information Unit" covers the detailed information about the methods and

form of submitting a request to the banks and method of receiving response from banks is specified on.

8 OFFENCES AND PENALTIES

Banks should have clear and understandable internal policies, procedures, operational guidelines and control mechanisms related to the processing, detection and reporting of information on suspicious transactions..

Reporting entities should ensure they have adequate internal policies, procedures and controls for detecting, reporting and handling information related to suspicious transactions. A number of offences and penalties are specified in Article 23 of the AML/CFT Law, Article 11.29 of the Infringement Law, the Criminal Code and other applicable laws.

9 TIPPING OFF

Under Article 13.1 of the AML/CFT Law, reporting entities, their management and employees shall not disclose any information related to the transaction reported to the FIU to other entity other than those specified in in Article 7.4 of the AML/CFT Law.

10 PROTECTION

Under the AML/CFT Law, a number of protections exist for persons and entities reporting suspicious transactions. These include:

Article 12.1. The submitting of reports by entities described in Article 4.1 to the Financial Information Unit and competent authorities, in accordance with provision of this Law, shall not be deemed as a breach of banking, professional, customer, business entity or organization, business or other secrecy confidentiality

Article 12.2. If information submitted by entities described in Article 4.1 has not been proven to be relating to money laundering and terrorism financing shall not serve as ground to impose civil, criminal and other liability on the person and entity submitted such an information.

Article 12.3. Any harm, caused to a citizen or a legal person, whose specific transaction was suspended according to Article 11 of this Law, shall not serve as ground to impose civil, criminal and other liability on management and employees of entities described in Article 4.1 of this Law and on employees of the Financial Information Unit.

_____oOo_____

APPENDIX 1. INDICATORS

1. COMMON INDICATORS

The following are examples of common indicators that may point to a suspicious transaction, whether completed or attempted. This list of examples is provided for guidance only and is not mandatory nor exhaustive.

1.1. GENERAL AREAS OF SUSPICION

- Customer admits or makes statements about involvement in criminal activities,
- You are aware that a Customer is the subject of a criminal investigation,
- Customer does not want correspondence sent to home address,
- Customer appears to have accounts with several financial institutions in one area for no apparent reason,
- Customer conducts transactions at different physical locations in an apparent attempt to avoid detection,
- Customer repeatedly uses an address but frequently changes the names involved,
- Significant and/or frequent transactions in contrast to known or expected business activity,
- Significant and/or frequent transactions in contrast to known employment status,
- Ambiguous or inconsistent explanations as to the source and/or purpose of funds,
- Where relevant, money presented in unusual condition, for example damp, odorous or coated with substance,
- Where relevant, nervous or uncooperative behavior exhibited by employees and/or Customers,
- Customer shows uncommon curiosity about internal systems, controls and policies,
- Customer has only vague knowledge of the amount of a deposit,
- Customer presents confusing details about the transaction or knows few details about its purpose,
- Customer appears to informally record large volume transactions, using unconventional bookkeeping methods or “off-the-record” books,
- Customer over justifies or explains the transaction,
- Customer is secretive and reluctant to meet in person,
- Customer is nervous, not in keeping with the transaction,
- Customer is involved in transactions that are suspicious but seems blind to being involved in money laundering activities,
- Customer’s home or business telephone number has been disconnected or there is no such number when an attempt is

made to contact the customer shortly after opening account,
- Normal attempts to verify the background of a new or prospective Customer are difficult,
- Customer appears to be acting on behalf of a third party but does not tell credit institution staff,
- Customer is involved in activity out-of-keeping for that individual or business,
- Customer insists that a transaction be done quickly,
- Inconsistencies appear in the Customer's presentation of the transaction,
- The transaction does not appear to make sense or is out of keeping with usual or expected activity for the Customer,
- Customer appears to have recently established a series of new relationships with different financial entities,
- Customer attempts to develop close rapport with staff,
- Customer uses aliases and a variety of similar but different addresses,
- Customer spells his or her name differently from one transaction to another,
- Customer uses a post office box or General Delivery address, or other type of mail drop address, instead of a street address when this is not the norm for that area,
- Customer provides false information or information that staff of the bank or financial institution believe is unreliable,
- Customer offers credit institution staff money, gratuities or unusual favors for the provision of services that may appear unusual or suspicious,
- Customer pays for services or products using financial instruments, such as money orders or traveler's checks, without relevant entries on the face of the instrument or with unusual symbols, stamps or notes,
- The bank/financial institution is aware that a Customer is the subject of a money laundering or terrorist financing investigation,
- The bank/financial institution is aware or becomes aware, from a reliable source (that can include media or other open sources), that a Customer is suspected of being involved in illegal activity,
- A new or prospective Customer is known as having a questionable legal reputation or criminal background,
- Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reason to exist).

Knowledge of reporting or record keeping requirements

- Customer attempts to convince employee not to complete any documentation required for the transaction,
- Customer makes inquiries that would indicate a desire to avoid reporting,
- Customer has unusual knowledge of the law in relation

to suspicious transaction reporting,

- Customer seems very conversant with money laundering or terrorist activity financing issues,
- Customer is quick to volunteer that funds are "clean" or "not being laundered",
- Customer appears to be structuring amounts to avoid record keeping, Customer identification or reporting thresholds,
- Customer appears to be collaborating with others to avoid record keeping, customer identification or reporting thresholds,
- Customer performs two or more cash transactions of less than the thresholds specified seemingly to avoid the reporting requirement/,

Identity documents

- Customer provides doubtful or vague information,
- Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate,
- Customer refuses to produce personal identification documents,
- Customer only presents copies rather than originals,
- Customer uses foreign, unverifiable identity documents,
- Customer wants to establish identity using something other than his or her personal identification documents,
- Customer's supporting documentation lacks important details such as a phone number,
- Customer inordinately delays presenting corporate documents,
- All identification presented is foreign or cannot be checked for some reason,
- All identification documents presented appear new or have recent issue dates,
- Customer presents different identification documents at different times,
- Customer alters the transaction after being asked for identity documents,
- Customer presents different identification documents each time a transaction is conducted,
- Customer avoid giving detailed information about the business activities.

Economic purpose

- Transaction seems to be inconsistent with the customer's apparent financial standing or usual pattern of activities,
- Transaction appears to be out of the normal course for industry practice or does not appear to be economically viable for the customer,
- Transaction is unnecessarily complex for its stated purpose,
- Activity is inconsistent with what would be expected from declared business,

- A business customer refuses to provide information to qualify for a business discount,
- No business explanation for size of transactions or cash volumes,
- Transactions or financial connections between businesses that are not usually connected (for example, a food importer dealing with an automobile parts exporter)
- Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

1.2. SUSPICIOUS INDICATORS RELATED TO PRODUCT AND SERVICE

Cash transactions

- Customer starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the Customer in the past,
- Customer frequently exchanges small bills for large ones,
- Customer uses notes in denominations that are unusual for the Customer, when the norm in that business is different,
- Customer frequently changes large amounts of cash with foreign currency in contrast to his/her employment status and business activity,
- Customer presents notes that are packed or wrapped in a way that is uncommon for the Customer,
- Customer deposits musty or extremely dirty bills,
- Customer consistently makes cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold
- Customer presents uncounted funds for a transaction. Upon counting, the Customer reduces the transaction to an amount just below that which could trigger reporting requirements,
- Customer conducts a transaction for an amount that is unusual compared to amounts of past transactions,
- Customer frequently purchases traveler's checks, foreign currency drafts or other negotiable instruments with cash when this appears to be outside of normal activity for the Customer,
- Transactions with several types of cash and payment instruments with consecutive serial numbers,
- Customer asks a clerk at the credit institution to hold or transmit large sums of money or other assets when this type of activity is unusual for the Customer,
- Shared address for individuals involved in cash transactions, particularly when the address is also for a business location, or

does not seem to correspond to the stated occupation (i.e., student, unemployed, self-employed, etc.),
- Stated occupation of the Customer is not in keeping with the level or type of activity (for example a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area).
- Cash is transported by a cash courier,
- Large transactions using a variety of denominations,
- Cash transactions with customers in a business or personal relationship with a region engaged in illicit drug cultivation, production, or trade;
- Regular return of checks for insufficient funds,
- Attempting to make transactions on counterfeit banknotes.

Transactions involving accounts

- Opening accounts when the customer's address is outside the local service area,
- Opening accounts in other people's names,
- Opening accounts with names very close to other established business entities,
- Attempting to open or operating accounts under a false name,
- Account with a large number of small cash deposits and a small number of large cash withdrawals,
- Funds are being deposited into several accounts, consolidated into one and transferred outside the country,
- Customer frequently uses many deposit locations outside of the home branch location, and its inconsistent with their employment status,
- Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers,
- Customer frequently make transaction which is inconsistent with his/her account type and purpose,
- Children's accounts being used for the benefit of parents/guardians,
- Establishment of multiple accounts, some of which appear to remain dormant for extended periods,
- Account that was reactivated from inactive or dormant status suddenly sees significant activity,
- Reactivated dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed,
- Unexplained transfers between the customer's products and accounts,
- Large transfers from one account to other accounts that appear to be pooling money from different sources,
- Multiple deposits are made to a customer's account by third parties,
- Frequent deposits of bearer instruments (for example,

checks, money orders or bearer bonds) in amounts just below the threshold amount,
- Correspondent accounts being used as "pass-through" points from foreign jurisdictions with subsequent outgoing funds to another foreign jurisdiction,
- Multiple personal and business accounts are used to collect and then funnel funds to a small number of foreign beneficiaries, particularly when they are in locations of concern, such as countries known or suspected to facilitate money laundering activities.

Transactions involving areas outside Mongolia

- Customer and other parties to the transaction have no apparent ties to Mongolia,
- Transaction crosses many international lines,
- Use of a credit card issued by a foreign bank that does not operate in Mongolia by a customer that does not live and work in the country of issue,
- Cash volumes and international remittances in excess of average income for migrant worker customers,
- Excessive demand for migrant remittances from individuals or entities based on migrant worker population,
- Transactions involving high-volume international transfers to third party accounts in countries that are not usual remittance corridors,
- Transaction involves a country known for highly secretive banking and corporate law,
- Foreign currency exchanges that are associated with subsequent wire transfers to locations of concern, such as countries known or suspected to facilitate money laundering activities,
- Deposits followed within a short time by wire transfer of funds to or through locations of concern, such as countries known or suspected to facilitate money laundering activities,
- Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money laundering system,
- Transaction involves a country known or suspected to facilitate money laundering activities.

Transactions related to offshore business activity

Any bank/financial institution that conducts transactions internationally should consider the following indicators:

- Accumulation of large balances, inconsistent with the known turnover of the customer's business, and subsequent transfers to overseas account(s),
- Frequent requests for traveler's checks, foreign currency drafts or other negotiable instruments,
- Loans secured by obligations from offshore banks,
- Loans to or from offshore companies,
- Offers of multimillion-dollar deposits from a confidential

source to be sent from an offshore bank or somehow guaranteed by an offshore bank,
- Transactions involving an offshore "shell" bank whose name may be very similar to the name of a major legitimate institution,
- Unexplained electronic funds transfers by customer on an in-and-out basis,
- Use of letter-of-credit and other methods of trade financing to move money between countries when such trade is inconsistent with the customer's business,
- Use of a credit card issued by an offshore bank.

Personal transactions

- Customer appears to have accounts with several financial institutions in one geographical area,
- Customer has no employment history but makes frequent large transactions or maintains a large account balance,
- The flow of income through the account does not match what was expected based on stated occupation of the account holder or intended use of the account,
- Customer makes one or more cash deposits to general account of foreign correspondent bank (i.e., pass-through account),
- Customer makes frequent or large payments to online payment services,
- Customer runs large positive credit card balances,
- Customer uses cash advances from a credit card account to purchase money orders or drafts or to wire funds to foreign destinations,
- Харилцагч кредит картнаас бэлэн мөнгө авч хадгаламж эсхүл харилцах дансандаа орлогодох,
- Customer takes cash advance to deposit into savings or checking account,
- Large cash payments for outstanding credit card balances,
- Customer visits the safety deposit box area immediately before making cash deposits,
- Customer wishes to have credit and debit cards sent to international or domestic destinations other than his or her address,
- Customer has numerous accounts and deposits cash into each of them with the total credits being a large amount,
- Customer deposits large endorsed checks in the name of a third-party,
- Customer frequently makes deposits to the account of another individual who is not an employee or family member,
- Customer frequently exchanges currencies,
- Customer frequently makes automatic banking machine deposits just below the reporting threshold,
- Customer's access to the safety deposit facilities increases substantially or is unusual in light of their past usage,
- Many unrelated individuals make payments to one account without rational explanation,

- Third parties make cash payments or deposit checks to a Customer's credit card,
- Customer gives power of attorney to a non-relative to conduct large transactions,
- Customer has frequent deposits identified as proceeds of asset sales, but assets cannot be substantiated,
- Customer acquires significant assets and liquidates them quickly with no explanation,
- Customer acquires significant assets and encumbers them with security interests that do not make economic sense,
- Customer requests movement of funds that are uneconomical,
- High volume of wire transfers are made or received through the account,
- Frequent deposits of winning gambling checks followed by immediate withdrawal or transfer of funds,
- Use of jurisdictions with weak AML/CFT framework.

Corporate and business transactions

Some businesses may be susceptible to the mixing of illicit funds with legitimate income. This is a very common method of money laundering. These businesses include those that conduct a significant part of their business in cash, such as restaurants, bars, parking lots, convenience stores and vending machine companies. On opening accounts with the various businesses in its area, a financial institution would likely be aware of those that are mainly cash based.

- Unusual or unexplained increases in cash deposits made by those entities may be indicative of suspicious activity,
- Accounts are used to receive or disburse large sums but show virtually no normal business-related activities, such as the payment of payrolls, invoices, etc,
- Cash or wire transactions in contrast to customer's business activity,
- Accounts have a large volume of deposits in bank drafts, cashier's checks, money orders or electronic funds transfers, which is inconsistent with the customer's business,
- Accounts have deposits in combinations of monetary instruments that are atypical of legitimate business activity,
- Accounts have deposits in combinations of cash and monetary instruments not normally associated with business activity,
- Business does not want to provide complete information regarding its activities,
- Financial statements of the business differ noticeably from those of similar businesses,
- Representatives of the business avoid contact with the branch as much as possible, even when it would be more convenient for them,
- 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,

- Customer maintains a number of trustee or customer accounts that are not consistent with that type of business or not in keeping with normal industry practices,
- Customer operates a retail business providing check - cashing services but does not make large draws of cash against checks deposited,
- Customer pays in cash or deposits cash to cover bank drafts, money transfers or other negotiable and marketable money instruments,
- Customer deposits large amounts of currency wrapped in currency straps,
- Customer makes a large volume of seemingly unrelated deposits to several accounts and frequently transfers a major portion of the balances to a single account at the same bank or elsewhere,
- Customer makes a large volume of cash deposits from a business that is not normally cash intensive,
- Customer makes large cash withdrawals from a business account not normally associated with cash transactions,
- Customer consistently makes immediate large withdrawals from an account that has just received a large and unexpected credit from abroad,
- Customer makes a single and substantial cash deposit composed of many large bills,
- Small, one-location business makes deposits on the same day at different branches across a broad geographic area that does not appear practical for the business,
- There is a substantial increase in deposits of cash or negotiable instruments by a company offering professional advisory services, especially if the deposits are promptly transferred,
- There is a sudden change in cash transactions or patterns,
- Customer wishes to have credit and debit cards sent to international or domestic destinations other than his or her place of business,
- There is a marked increase in transaction volume on an account with significant changes in an account balance that is inconsistent with or not in keeping with normal business practices of the Customer's account,
- Asset acquisition is accompanied by security arrangements that are not consistent with normal practice,
- Unexplained transactions are repeated between personal and commercial accounts,
- Activity is inconsistent with stated business,
- Account has close connections with other business accounts without any apparent reason for the connection,
- Activity suggests that transactions may offend securities regulations, or the business prospectus is not within the requirements,
- A large number of incoming and outgoing wire transfers take

place for which there appears to be no logical business or other economic purpose, particularly when this is through or from locations of concern, such as countries known or suspected to facilitate money laundering activities.

Wire/funds transfer activities

- Customer is reluctant to give an explanation for the remittance,
- Customer orders wire transfers in small amounts in an apparent effort to avoid triggering identification or reporting requirements,
- Customer transfers large sums of money to overseas locations with Regulations to the foreign entity for payment in cash,
- Customer receives large sums of money from an overseas location and the transfers include Regulations for payment in cash,
- Customer makes frequent or large funds transfers for individuals or entities who have no account relationship with the institution,
- Customer receives frequent funds transfers from individuals or entities who have no account relationship with the institution,
- Customer receives funds transfers and immediately purchases monetary instruments prepared for payment to a third party which is inconsistent with or outside the normal course of business for the Customer,
- Customer requests payment in cash immediately upon receipt of a large funds transfer,
- Immediately after transferred funds have cleared, the Customer moves the funds to another account or to another individual or entity,
- Customer shows unusual interest in funds transfer systems and questions the limit of what amount can be transferred,
- Customer transfers funds to another country without changing the currency,
- Large incoming wire transfers from foreign jurisdictions are removed immediately by company principals,
- Customer sends frequent wire transfers to foreign countries but does not seem to have connection to such countries,
- Wire transfers are received from entities having no apparent business connection with customer,
- Size of funds transfers is inconsistent with normal business transactions for that customer,
- Rising volume of remittances exceeds what was expected from the customer when the relationship was established,
- Several customers request transfers either on the same day or over a period of two to three days to the same recipient,
- Different customers request transfers that are all paid for by the same customer,
- Several customers requesting transfers share common

identifiers, such as family name, address or telephone number,
- Several different customers send transfers that are similar in amounts, sender names, test questions, free message text and destination country,
- A customer sends or receives multiple transfers to or from the same individual,
- Stated occupation of the customer or the customer's financial standing is not in keeping with the level or type of activity (for example a student or an unemployed individual who receives or sends large numbers of wire transfers),
- Migrant remittances made outside the usual remittance corridors,
- Personal funds sent at a time not associated with salary payments,
- Country of destination for a wire transfer is not consistent with the nationality of the individual customer,
- Customer requests transfers to a large number of recipients outside Mongolia who do not appear to be family members,
- Customer does not appear to know the recipient to whom he or she is sending the transfer,
- Customer does not appear to know the sender of the transfer from whom the transfer was received,
- Beneficiaries of wire transfers involve a large group of nationals of countries associated with terrorist activity,
- Customer makes funds transfers other businesses abroad that are not in line with the customer's business,
- Customer conducts transactions involving countries known as narcotic source countries or as trans-shipment points for narcotics, or that are known for highly secretive banking and corporate law practices,
- Customer does not communicate with the bank in person, but only make high-value transactions using internet / electronic banking (payment) services,
- Regular transaction using internet banking service from foreign countries to account opened by Mongolian bank or financial institutions.

Loan

- Customer suddenly repays a problem loan unexpectedly,
- Customer makes a large, unexpected loan payment with unknown source of funds, or a source of funds that does not match what the credit institution knows about the customer,
- Customer repays a long-term loan, such as a mortgage, within a relatively short time period,
- Source of down payment is inconsistent with borrower's background and income,
- Down payment appears to be from an unrelated third party,
- Down payment uses a series of money orders or bank drafts from different financial institutions,
- Customer shows income from "foreign sources" on loan

application without providing further details,

- Customer's employment documentation lacks important details that would make it difficult for the credit institution to contact or locate the employer,
- Customer's documentation to ascertain identification, support income or verify employment is provided by an intermediary who has no apparent reason to be involved,
- Customer has loans with offshore institutions or companies that are outside the ordinary course of business of the Customer,
- Customer offers the credit institution large dollar deposits or some other form of incentive in return for favorable treatment of loan request,
- Customer asks to borrow against assets held by another financial institution or a third party, when the origin of the assets is not known,
- The loan transaction does not make economic sense (for example, the Customer has significant assets, and there does not appear to be a sound business reason for the transaction),
- Customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction,
- Customer applies for loans on the strength of a financial statement reflecting major investments in or income from businesses incorporated in countries known for highly secretive banking and corporate law and the application is outside the ordinary course of business for the Customer,
- Down payment or other loan payments are made by a party who is not a relative of the Customer,
- Reluctance to use favorable facilities, for example, avoiding high interest rate facilities for large balances,
- Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using Customer accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other Customer company and trust accounts,
- Make regular or intermittent payments to the loan account in excess of the loan repayment schedule for no apparent reason.

Transactions for non-profit organizations (including registered charities)

- Known or suspected criminal entities establishing trust or bank accounts under charity names,
- Inconsistencies between the pattern or size of financial transactions and the stated purpose and activity of the organization,
- Sudden increase in the frequency and amounts of financial transactions for the organization, or the inverse, that is, the organization seems to

hold funds in its account for a very long period,
- Large and unexplained cash transactions by the organization,
- Absence of contributions from donors located in Mongolia,
- Large number of non-profit organizations with unexplained links,
- The non-profit organization appears to have little or no staff, no suitable offices or no telephone number, which is incompatible with their stated purpose and financial flows,
- The non-profit organization has operations in, or transactions to or from, high-risk jurisdictions,
- Inconsistencies between apparent modest sources of funds of the organization (e.g., communities with modest standard of living) and large amounts of funds raised,
- Inconsistencies between the pattern or size of financial transactions and the stated purpose and activity of the organization,
- Sudden increase in the frequency and amounts of financial transactions for the organization, or the inverse, that is, the organization seems to hold funds in its account for a very long period,
- Large and unexplained cash transactions by the organization,
- Absence of contributions from donors located in Mongolia,
- The organization's directors are outside Mongolia, particularly if large outgoing transactions are made to the country of origin of the directors and especially if that country is a high-risk jurisdiction.

2. INDUSTRY SPECIFIC INDICATORS

MONEY SERVICE BUSINESSES (INCLUDING CURRENCY EXCHANGE AND MONEY REMITTANCE)

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

LIFE INSURANCE

- Large single payments and payouts,
- Customer changes the beneficiary of policies.

INVESTMENT

- Securities accounts opened to trade in shares of only one listed company,
- Transaction patterns resemble a form of market manipulation, for example, insider trading,
- Unusual settlements, for examples, checks requested for no apparent reason to third parties хийх,
- Funds deposited into stockbroker's account followed immediately by request for repayment,

- Limited or no securities transactions recorded before settlement requested.

CASH COURIERS

- Transactions involving locations with poor AML/CFT regimes or high exposure to corruption,
- Significant and/or frequent cash deposits made over a short period of time,
- Significant and/or frequent currency exchanges made over a short period of time.

TRUST AND COMPANY SERVICE PROVIDERS

- Creation of complicated structures where there is no legitimate economic reason,
- Use of an intermediary without a legitimate reason,
- Funds received from high risk jurisdictions,
- Customers use nominee directors /shareholders,
- Customers address is a virtual office.

APPENDIX 2. TYPOLOGIES

Based on the Asia Pacific Group on Money Laundering and terrorist financing methods, techniques and schemes and instruments.[4]

The following examples taken from APG research provide a few key money laundering and terrorist financing methods, techniques, schemes and instruments.

Association with corruption (bribery, proceeds of corruption & instances of corruption undermining AML/CFT measures): Corruption (bribery of officials) to facilitate money laundering by undermining AML/CFT measures, including possible influence by politically exposed persons (PEPs): e.g. investigating officials or private sector compliance staff in banks being bribed or influenced to allow money laundering to take place.

Currency exchanges / cash conversion: used to assist with smuggling to another jurisdiction or to exploit low reporting requirements on currency exchange houses to minimize risk of detection - e.g. purchasing of travelers checks to transport value to another jurisdiction.

Cash couriers / currency smuggling: concealed movement of currency to avoid transaction / cash reporting measures.

Structuring (smurfing): A method involving numerous transactions (deposits, withdrawals, transfers), often various people, high volumes of small transactions and sometimes numerous accounts to avoid detection threshold reporting obligations.

Use of credit cards, checks, promissory notes etc: Used as instruments to access funds held in a financial institution, often in another jurisdiction.

Purchase of portable valuable commodities (gems, precious metals etc.): A technique to purchase instruments to conceal ownership or move value without detection and avoid financial sector AML/CFT measures – e.g. movement of diamonds to another jurisdiction.

Purchase of valuable assets (real estate, race horses, vehicles, etc.): Criminal proceeds are invested in high-value negotiable goods to take advantage of reduced reporting requirements to obscure the source of proceeds of crime.

Commodity exchanges (barter): Avoiding the use of money or financial instruments in value transactions to avoid financial sector AML/CFT measures - e.g. a direct exchange of heroin for gold bullion.

Use of Wire transfers: to electronically transfer funds between financial institutions and often to another jurisdiction to avoid detection and confiscation.

Underground banking / alternative remittance services (hawala / hundi etc.): Informal mechanisms based on networks of trust used to remit monies. Often work in

[4] http://www.apgml.org/methods-and-trends/page.aspx?p=a4a11dca-75f2-4dae-9c25-6215103e56da

parallel with the traditional banking sector and may be outlawed (underground) in some jurisdictions. Exploited by money launderers and terrorist financiers to move value without detection and to obscure the identity of those controlling funds.

Trade-based money laundering and terrorist financing: usually involves invoice manipulation and uses trade finance routes and commodities to avoid financial transparency laws and regulations.

Gaming activities (casinos, horse racing, internet gambling etc.): Used to obscure the source of funds – eg buying winning tickets from legitimate players; using casino chips as currency for criminal transactions; using online gambling to obscure the source of criminal proceeds.

Abuse of non-profit organizations (NPOs): May be used to raise terrorist funds, obscure the source and nature of funds and to distribute terrorist finances.

Investment in capital markets: to obscure the source of proceeds of crime to purchase negotiable instruments, often exploiting relatively low reporting requirements.

Mingling (business investment): A key step in money laundering involves combining proceeds of crime with legitimate business monies to obscure the source of funds.

Use of shell companies/corporations: a technique to obscure the identity of persons controlling funds and exploit relatively low reporting requirements.

Use of offshore banks/businesses, including trust company service providers: to obscure the identity of persons controlling funds and to move monies away from interdiction by domestic authorities.

Use of nominees, trusts, family members or third parties etc.: to obscure the identity of persons controlling illicit funds.

Use of foreign bank accounts: to move funds away from interdiction by domestic authorities and obscure the identity of persons controlling illicit funds.

Identity fraud / false identification: used to obscure identification of those involved in many methods of money laundering and terrorist financing.

Use "gatekeepers" professional services (lawyers, accountants, brokers etc.): to obscure identity of beneficiaries and the source of illicit funds. May also include corrupt professionals who offer 'specialist' money laundering services to criminals.

New Payment technologies: use of emerging payment technologies for money laundering and terrorist financing. Examples include cell phone-based remittance and payment systems.