Da Afghanistan Bank (Central Bank)
Financial Transactions and Report Analysis Center of Afghanistan (FinTRACA)

Suspicious Transactions Reporting (STR) Guideline

August-2016

Table of Contents

ACRONYMS

a) **AML/CFT:** Refers to Anti Money Laundering and Combating the Financing of Terrorism.
b) **AML/PC Law:** Refers to Anti Money Laundering and Proceeds of Crime Law.
c) **CFT Law:** Refers to Combating the Financing of Terrorism Law.
d) **DAB:** Refers to Da Afghanistan Bank (Central Bank of Afghanistan).
e) **FinTRACA/FIU:** Refers to Financial Transactions and Reports Analysis Center of Afghanistan / Financial Intelligence Unit.
f) **FATF:** Refers to Financial Action Task Force.
g) **UNSCR:** Refers to United Nations Security Council Resolution.
h) **STR:** Refers to Suspicious Transaction Report.
i) **Money Laundering (ML):** Refer to sub-paragraph 11, paragraph 1 of article 3 of Anti Money Laundering and Proceeds of Crimes (AML/PC) Law.
j) **Financing of Terrorism (CFT):** Refer to article 4 of Counter Financing of Terrorism (CFT) Law.
k) **FSD:** Refers to Financial Supervision Department of Da Afghanistan Bank.
l) **Predicate Offence:** Means any criminal acts resulted in funds or properties whether directly or indirectly.
m) **Proceeds of Crimes:** Means any funds or property derived from or obtained directly or indirectly through the commission of a predicate offence. This also includes income or benefits derived from such proceeds, proceeds obtained from the investment of such funds or the funds or property that have been transferred into other types of assets, whether partially or in whole**.**

INTRODUCTION

This guideline has been issued to clarify the obligation to report suspicious transactions under the Anti-Money Laundering and Proceeds of Crime Law (AML/PC Law).

It aims to generate knowledge on indicators of suspicious activity and inform reporting entities about the technical requirements to report suspicious transactions.

This guideline is provided for information only and cannot be relied on as evidence of complying with the requirements of the AML/PC law. It does not constitute legal advice and cannot be relied on as such.

1. BACKGROUND

If you are a reporting entity, as defined in Article 5 of the AML/PC Law, you are required to undertake customer due diligence measures, report suspicious transactions and transaction equal or above a threshold specified in relevant regulations, keep records of transactions and establish, implement, and maintain an AML/CFT compliance program.

According to Article 19 of the AML/PC law, reporting entities are required to develop internal policies, procedures and controls relating to reporting obligations for the purpose of AML compliance program.

1.1 PURPOSE

This guideline has three main objectives:

- To explain money laundering and terrorist financing.
- To help reporting entities understand and comply with Suspicious Transaction
- Reporting (STR) obligations.
- To help reporting entities to identify suspicious transactions by providing both General and industry specific indicators.

In many cases reporting entities will be unaware of what the actual criminal activity is. However, by screening transactions for known indicators and typologies, a suspicion of criminal offending may arise.

1.2 SCOPE

In addition to reporting suspicious transactions, reporting entities are required to undertake a number of other obligations as prescribed in the AML/PC Law.

Reporting entities are encouraged to submit the suspicious transaction reports electronically via the method referenced in section 3.5 below.

For all reporting entities, the previous Guidelines on STR Data Content Specification, STR Data Entry Form and STR XML Schema, provide guidance on form and content of suspicious transactions reports.

AML/CFT

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. The processes of money laundering is of critical importance, as it enables the criminal to enjoy these profits without revealing jeopardizing their source.

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 is the attempt to conceal or disguise the nature, location, source, ownership, or control of illegally obtained money. 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:
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. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.

Integration: Having successfully processed his criminal profits through the first two phases the launderer then moves them to the third stage – integration – in which the funds re-enter the legitimate economy. The launderer might choose to invest the

funds into real estate, luxury assets, or business ventures. A money laundering scheme will typically but not necessarily involve all three stages.

2.3 TERRORIST FINANCING VS MONEY LAUNDERING

Terrorist financing and money laundering both require the movement of funds, preferably, with minimal scrutiny. The controls established to detect money laundering are applicable to detect and prevent terrorist financing.

Understanding key differences between the two is important. Unlike money launderers, terrorist organizations can raise funds through legitimate sources as well as criminal activities. 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.

2.4 TARGETED FINANCIAL SANCTIONS

The CFT law establishes 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, 1988 and successor resolutions and those designated by Afghanistan 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 11 of the CFT law and contains the following elements:

- All persons, including any reporting entity shall without delay freeze the funds or properties of persons designated;
- All persons, including any reporting entity are prohibited from making available any such funds or property, economic resources or financial or other related services available directly or indirectly to or for the benefit of designated persons.

The Counter Financing of Terrorism Regulations clarifies other obligations and aspects of the requirement to implement and apply targeted financial sanctions.

2.5 AML/CFT INTERNATIONAL STANDARDS

2.5.1 INTERNATIONAL STANDARDS

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

- UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances – Vienna Convention – 1988;
- UN Convention Against Transnational Organized Crime - Palermo Convention – 2000;
- UN Convention Against Corruption - UNCAC – 2005;
- Financial Action Task Force (FATF) 40 Recommendations - revised February 2012.

2.5.2 FINANCIAL ACTION TASK FORCE

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

The 40 Recommendations of FATF are recognized as the international standard on AML/CFT.

The purpose of the FATF Recommendations it to lead/direct international efforts against money laundering and terrorist financing. The FATF assesses countries against a set of recommendations (the 40 Recommendations) that represent best practices for AML/CFT systems.

The Asia Pacific Group (APG) deals with Anti Money Laundering and Combating the Financing of Terrorism and is a FATF Style Regional Body (FSRB). FSRB's perform a similar function as the FATF on a regional basis. Afghanistan is a member of the APG and is subject to the assessment of its AML/CFT framework by the APG.

2.6 DOMESTIC LEGISLATION

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

- AML/PC Law
- CFT Law
- AML Responsibilities and Preventative Measures Regulation
- Money Service Providers (MSPs) Regulation
- Foreign Exchange Dealers (FXDs) Regulation
- Electronic Money Institutions Regulation (EMI)
- FinTRACA (FIU) and/or FSD Circulars
- Other relevant laws and regulations

3. SUSPICIOUS TRANSACTIONS

Pursuant to Article 18 of the AML/PC Law, Reporting entities are required to report suspicious transactions when they have formed a suspicion based on reasonable grounds that a transaction or an attempted transaction is involved in, linked to, or may be related to one of the following:

- Money laundering
- Terrorist financing
- Proceeds of crime
- Terrorists
- Terrorist organization(s)
- Terrorism or a terrorist act
- Predicate offences

This list of offenses also applies to offenses committed within Afghanistan or in a foreign jurisdiction.

Suspicious transaction report should be filed with necessary supporting documents, correct identifiers and after the initial analysis of the authorized officer (s) of the reporting entity.

SUSPICIOUS TRANSACTION REPORTS (STRs)

FINTRACA relies on reporting entities to fulfill their obligation to report transactions where it is suspected that the transaction is linked to money laundering, terrorist financing, any of the predicate offences, the proceeds of crime, a terrorist, a terrorist organization or terrorist act.

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

Reports received by the FINTRACA are analyzed for activities and patterns that may indicate criminal offending. Various resources are used including partner agencies and open-source databases.

Often, additional information is required from reporting entities to help establish whether the suspicious activity reported in an 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, asset recovery, taxation, and national security.

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

3.1 IDENTIFYING SUSPICIOUS TRANSACTIONS

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. Therefore, the KYC/Account Opening forms of the customers should at least be updated annually.

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 in Appendix A. However this list of indicators is for guidance

only. What is an STR will ultimately be determined by the reporting entity's knowledge of its customers, their business and historical pattern of transaction.

Further guidance may be obtained from typologies and case studies provided in the typology report produced by the FIU. This report is available for download on the FIU website. A list of typologies is included in Appendix A.

3.2 SUSPECTS ON REASONABLE GROUNDS

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.

A suspicious transaction must also be reported when a reporting entity has formed a suspicion based on reasonable grounds. If any reasonable person in your circumstances would consider the transaction suspicious then it is suspicious and an STR must be submitted.

In both circumstances, the customer due diligence measures as specified in AML/CFT Responsibilities and Preventative Measures Regulation, undertaken by the reporting entity will provide it with information and knowledge of the customer and will be crucial to enable the reporting entity to identify a suspicion transaction.

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 and does not satisfy the reasonable grounds element.

A large transaction may be considered suspicious where it does not fit with the customer's financial or transaction profile. Comparing the transaction to previous account records may prove helpful and demonstrate reasonable grounds. Furthermore, attaching this information to the STR will assist FINTRACA to understand reasonable 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 your 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 reasonable grounds element.

3.3 WHO MUST REPORT

If you are a reporting entity, as defined in Article 5 of the AML/PC Law, any transactions conducted (or attempted) using your services that are considered suspicious must be reported to FINTRACA.

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

3.4 WHAT TO REPORT

An STR submitted to FINTRACA must contain:

A. A valid statement of the grounds on which the reporting entity holds a suspicion
B. Mandatory details (as required in regulations)
C. Correct identifications
D. Other details or supporting documents
E. (additional information that will support FIU analysis) / Details asked by FinTRACA.

3.5 WHEN TO REPORT

Once a suspicion is formed, a reporting entity must as soon as practicable, but no later than three working days after forming a suspicion, report the transaction to the FIU.

In practice, where account monitoring processes identify a transaction, the three day requirement does not commence until a suspicion based on reasonable grounds is formed.

Reasonable grounds may not exist until a member of your staff has had time to consider the transaction in light of the surrounding circumstances or new information obtained. Once the requisite suspicion is formed, the three day 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/PC law, CFT Law and relevant regulations, including the requirement to submit additional STRs where appropriate.

3.6 HOW TO REPORT

Reporting entities must transmit reports via the software of FinTRACA provided to commercial banks and MSPs for the purpose of transmitting LCTR and STR. An exception to the requirement to report electronically exists where the urgency of the situation requires an STR to be made orally.

Circumstances in which suspicions transactions can be reported orally include:

A. Where a reporting entity thinks that a situation requires urgent action.
B. When a reporting entity has more than a reasonable suspicion, rather, knowledge or belief that the transaction is related to serious criminal offending.

Where a suspicious transaction has been reported orally, the reporting entity must, send an official email to FinTRACA regarding the matter after oral reporting immediately and as soon as practicable, but no later than 3 working days after making the oral report and official email, forward an electronic version of the report to FINTRACA.

To make an oral report, please contact Compliance department of FINTRACA on; (+93 20 25 12 689) within business hours.

4. RECORD KEEPING

As a reporting entity for purposes of Article 16 of the AML/PC law you must keep and maintain records of all transactions for 5 years, and STRs, for at least 10 years after the transaction. You may also be required to keep records for a longer period if requested to do so by any competent authority.

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

Records should also be kept in form and manner to facilitate the easy reconstruction of transactions.

5. MANAGEMENT AND STAFF TRAINING

Reporting entities 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. At a minimum, the institution's training program must provide training for all personnel whose duties require such knowledge. 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 relevant regulations and guidelines. In addition, reporting entities should ensure that staff is 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. Training will focus on employee consciousness and understanding of AML/CFT 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 as specified in AML/CFT responsibilities and preventative measures regulation 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;
- 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 supervisory, 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;
    - Developing and implementing of Internal policies, such as customer identification and verification procedures and CDD policies;
    - What the legal recordkeeping requirements are;
    - Suspicious transaction reporting requirements;
    - Currency transaction reporting requirements;
    - Duties and accountability of employees;
    - The details of the institution's AML/CFT program 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 methods for conducting trainings, 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.
- It is preferable to train in the workplace as it is more relevant and attendees can more easily access systems and forms to check their understanding.

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.

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 AML/CFT compliance officer may help to dismiss or support the suspicion.

A list of internationally established indicators is provided in Appendix A. This list is divided into (1) common and (2) industry specific indicators.

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/PC LAW

FINTRACA may 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. FINTRACA will ensure that all requests are made in good faith and are relevant to analyzing a STR.

FINTRACA shall also set out the time frame and form for the submission of the additional information requested.

8. OFFENCES & PENALTIES

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 24, 50 & 51 of the AML/PC Law.

8.1 OFFENCES

Refer to Article 4 of AML/PC law.

8.1.1 TIPPING OFF

It is an offence to provide an STR or information related to an STR to an unauthorized person. This is commonly referred to as tipping off.

Under Article 18 (5) of the AML/PC law, the following persons are prohibited from disclosing to a customer or any other person the fact that an STR has been made or any additional information has been submitted:

A. Reporting entities;
B. Their directors; and
C. Their employees.

This shall not preclude disclosures or communications between and among directors and employees of the financial institution or designated non-financial business and profession, in addition to lawyers for the purpose of obtaining legal advice in relation to the STR, competent authorities, and the law enforcement agencies.

A reporting entity commits an offence if the reporting entity fails to report a suspicious transaction within 3 days of forming a suspicion. A person who provides misleading information, communicates or discloses information or records required to be kept confidential pursuant to the AML/PC law to any person not authorized to receive such information or records by AML/PC Law commits an offence.

8.2 PENALTIES

Refer to Articles 24, 50 & 51 of AML/PC law.

9. PROTECTIONS

Under the AML/PC Law a number of protections exist for persons reporting suspicious transactions.

9.1 PROTECTION OF PERSON REPORTING A SUSPICIOUS TRANSACTION

Where a person reports a suspicious transaction or supplies any information in connection with a STR, they will not be held liable where the disclosure has been made in good faith.

This protection is offered to any reporting entities or their directors, officers or employees. This protection does not apply if the person reports or supplies the information in bad faith or misleading.

9.2 IMMUNITY FROM LIABILITY FOR DISCLOSURE OF INFORMATION

No criminal, civil, disciplinary or administrative proceedings for breach of banking or professional secrecy or contract or restriction on disclosure of information will also be instituted for reporting entities who submit an STR or any related information. This immunity only applies whenever the reporting is done in good faith.

10. FINTRACA GUIDANCE MATERIALS:

FINTRACA produces a range of material related to the AML/CFT environment. This material is available on its website at http://www.fintraca.gov.af.

11. AMMENDMENTS:

This guideline may be reviewed on a regular basis and appropriate changes made. The changes shall be initially approved by the Director General and shall be approved by DAB Governor.

FinTRACA can amend the annexes when required and is not subject to the approval of DAB Supreme Council.

APPENDIX A 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.
- Customer is accompanied and watched.
- 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.

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 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 consistently makes cash transactions that are significantly below the reporting threshold amount in an apparent attempt to avoid triggering the identification and reporting requirements.
- 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.
- 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.

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.

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.
- Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers.
- Activity far exceeds activity projected at the time of opening of the account.
- 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.
- Deposits or withdrawals of multiple monetary instruments, particularly if the instruments are sequentially numbered.
- Frequent deposits of bearer instruments (for example, checks, money orders or bearer bonds) in amounts just below the threshold amount.
- Unusually large cash deposits by a customer with personal or business links to an area associated with drug trafficking.
- Regular return of checks for insufficient funds.
- 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 Afghanistan

- Customer and other parties to the transaction have no apparent ties to Afghanistan.
- Transaction crosses many international lines.
- Use of a credit card issued by a foreign bank that does not operate in Afghanistan 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.
- Customer takes cash advance to deposit into savings or checking account.
- Large cash payments for outstanding credit card balances.

- Customer makes credit card overpayment and then requests a cash advance.
- 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.

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, 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.

- 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 (for example, deposits that include a mix of business, payroll, and social security checks).
- 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 purchases cashier's checks and money orders with large amounts of cash.
- 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.

Transactions for non-profit organizations (including registered charities)

- 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 Afghanistan.

- The organization's directors are outside Afghanistan, 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.
- 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 conducts transactions to or from, high-risk jurisdictions.

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.
- Customer instructs the bank/financial institution to transfer funds abroad and to expect an equal incoming 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 Afghanistan 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 is known for highly secretive banking and corporate law practices.

SUSPICIOUS INDICATORS RELATED TO LENDING

- 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.
- Frequent and/or unscheduled cash deposits to loan accounts.
- Frequent deposits of winning gambling checks followed by immediate withdrawal or transfer of funds.
- Use of internet banking to frequently access Afghanistan based accounts internationally.
- Children's accounts being used for the benefit of parents/guardians.
  Use of jurisdictions with weak AML/CFT framework

2 Industry Specific Indicators

- The following industry specific
- indicators may give rise to
- reasonable grounds for suspicion.
- Registered banks and non-bank
- deposit takers –
- Customer makes frequent or large payments to online payment services.
- Customer runs large positive credit card balances.
- Customer visits the safety deposit box area immediately before making cash deposits.
- Customer requests to have credit/debit cards sent to locations other than his or her address.
- Customer frequently transfers funds to unknown third parties.
- Unknown third parties frequently transfer funds into Customer's account
- Accounts are used to receive or disburse large sums but show virtually no normal business-
- Customer frequently exchanges currencies.
- Customer has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.
- Customer requests movement of funds that are uneconomical.
- High volume of wire transfers are made or received through the account.
- Immediately after transferred funds have cleared, the Customer moves the funds to another account or to another individual or entity.
- International funds transfers from an Customer's account to several offshore accounts held in the same name.
- Large foreign exchange transactions.
- Use of counterfeit currency.

related activities, such as the payment of payrolls, invoices, etc.

- Accounts have a large volume of deposits in bank drafts, cashier's cheques, money orders or electronic funds transfers, which are inconsistent with the Customer's business.
- Accounts have deposits in combinations of cash and monetary instruments not normally associated with the 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 check deposited.
- Customer pays in cash or deposits cash to cover bank drafts, money transfer or other negotiable instruments.
- Customer purchases cashier's check and money orders with large amounts of cash.
- 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 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.
- 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.
- 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.
- 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.
- A large number of incoming and outgoing wire transfers take place for which there appears to be no logical business or other economic purpose.

REGISTERED BANKS AND NON-BANK DEPOSIT TAKERS - NON-PROFIT SECTOR TRANSACTIONS

- 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 Afghanistan.
- 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.

MONEY SERVICE BUSINESSES (INCLUDING CURRENCY EXCHANGE AND MONEY REMITTANCE) AND OTHER BUSINESS INVOLVED IN ELECTRONIC FUNDS TRANSFER

- 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.

2.1.1 LIFE INSURANCE

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

2.1.2 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.
- Funds deposited into stockbroker's account followed immediately by request for repayment.
- Limited or no securities transactions recorded before settlement requested.

2.1.3 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.

2.1.4 TRUST AND COMPANY SERVICE PROVIDES

- 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.

2.1.5 ACCOUNTANTS, LAWYERS & REAL ESTATE AGENTS (GATEKEEPER SERVICES)

- Use of an agent or intermediary without obvious reason.
- Customer uses professional business or trust account, particularly, where large cash deposits are made.
- Funds are received from a foreign jurisdiction, particularly, where there is no connection between the jurisdiction and the Customer.
- Overseas instruction from a Customer for no economic reason.
- Customer is not concerned about the level of fees.
- Customer has a fast-growing real estate portfolio
- Purchaser is a company with complicated beneficial ownership.
- Purchase amount is unusual compared to the appraised value or the previous purchase amount.
- Customer appears to have access to cash substantially above their means.
- Customer uses a virtual office.

APPENDIX B TYPOLOGIES

Based on the Asia Pacific Group on Money Laundering and terrorist financing methods, techniques and schemes and instruments[1].

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.

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

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

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.