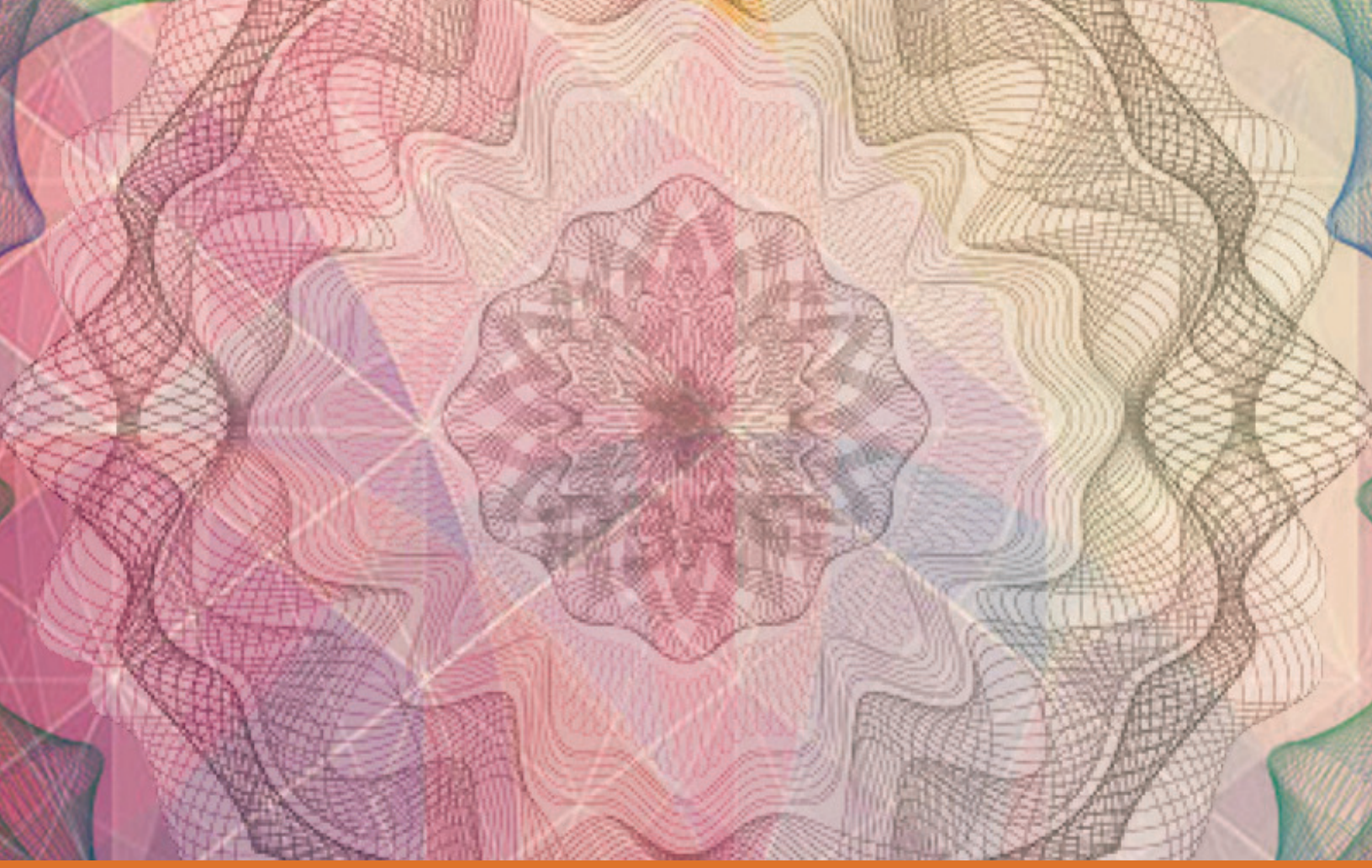


Royal Monetary Authority of Bhutan
Department of Financial Intelligence

Guide on Customer Due Diligence

Royal Monetary Authority of Bhutan
Department of Financial Intelligence

Guide on Customer Due Diligence

Whilst this publication has been prepared by the Royal Monetary Authority, it is not a legal document and should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions.

CONTENT

Content continued

Foreword

Money laundering and terrorism financing (ML/TF) continue to pose threat to the global economy and its security. Financial services institutions such as banks, non-banking financing companies, insurers, and capital market firms are generally the most favored channels through which illicit money is laundered across the globe. In order to address the vulnerabilities and threats faced by such financial institutions, financial firms are subjected to stringent anti-money laundering (AML) regulations to track the trail of illegally-sourced earnings.

Customer due diligence (CDD) is one of the best and the first defense a Reporting Entity can maintain to guard against the dangers of money laundering and other financial crimes. Also referred to as "knowing your customer," customer due diligence encompasses important aspects of an Anti-Money Laundering (AML) program, such as customer identification and Enhanced Due Diligence (EDD). Additionally, the need for customer due diligence is essential for suspicious activity reporting requirements because the data collected during the CDD process adds value to the reporting if the customer and the transaction conducted is found to be suspicious. These systems and processes will assist Reporting Entities in determining when transactions are potentially suspicious, and what action they need to take based on these determinations.

The Royal Monetary Authority (RMA) recognizes the challenges faced by Reporting Entities in meeting national and international AML/CFT requirements. Therefore, this guidebook has been drafted to establish better Customer Due Diligence procedures in Reporting Entities which will in turn assist in protecting the integrity and stability of the Bhutanese financial system and thus making it more difficult for those engaged in crime to legitimise proceeds from their criminal activities.

Dasho Penjore

Governor
Royal Monetary Authority of Bhutan

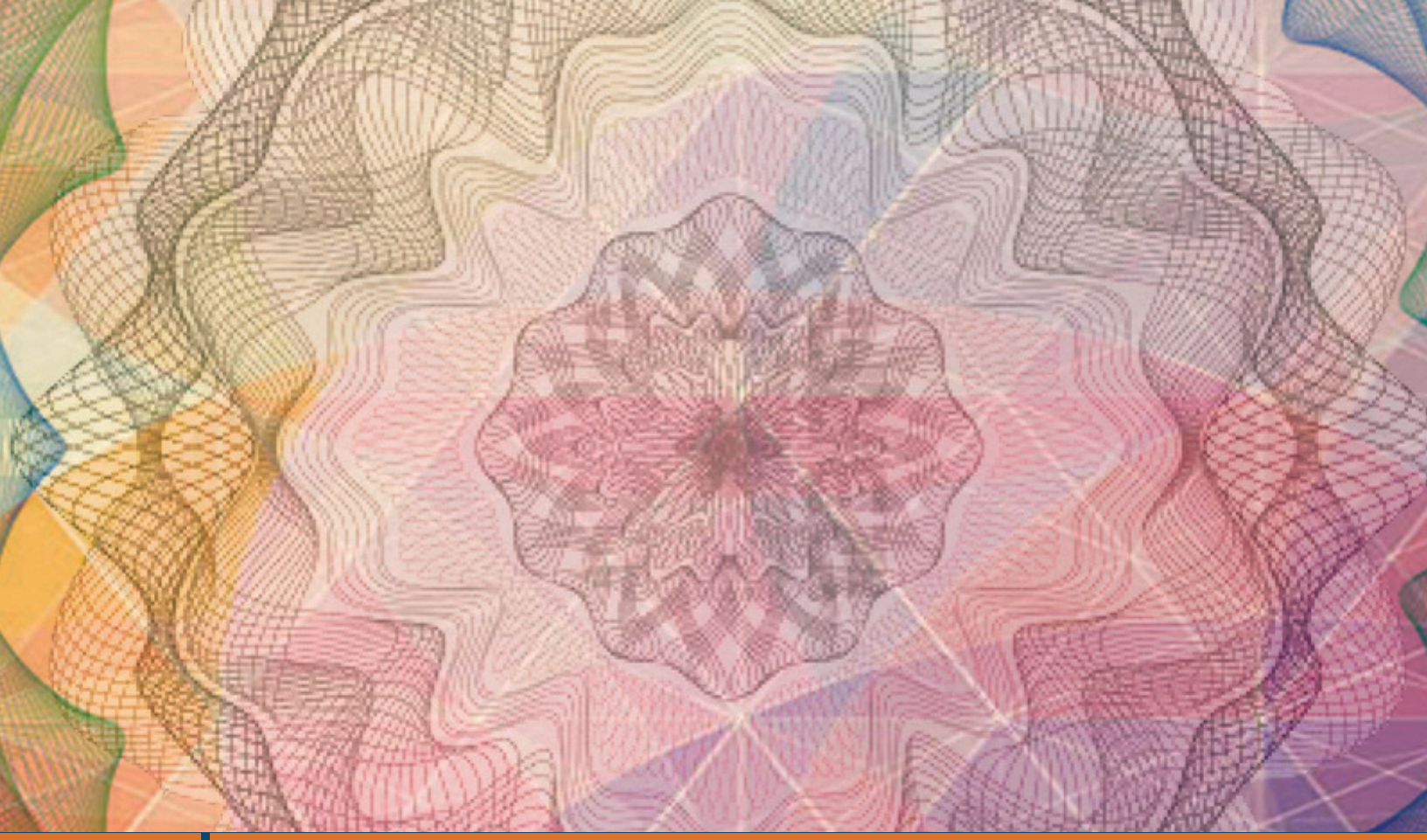
Acknowledgment

The Royal Monetary Authority (RMA) of Bhutan would like to acknowledge the Asian Development Bank (ADB) for their technical assistance towards the development of the Customer Due Diligence (CDD) Guidebook.

The RMA would specifically like to thank ADB's Office of Anticorruption and Integrity (OAI) for its much needed support and guidance in drafting the guidebook

Abbreviations and Acronyms

AML/CFT	anti–money laundering/countering financing of terrorism
CDD	Customer Due Diligence
ECDD	Enhanced Customer Due Diligence
FATF	Financial Action Task Force
DFI	Department of Financial Intelligence
FIU	Financial Intelligence Unit
KYC	Know Your Customer
ML/TF	money laundering/terrorism financing
NGO	nongovernment organization
Nu.	Bhutan ngultrum
PEP	politically exposed person
RMA	Royal Monetary Authority of Bhutan
STR	suspicious transaction report



Guide on Customer Due Diligence

01. Overview

1.1. Introduction

Countries around the world are placing increasing emphasis on ensuring that their financial institutions and other businesses engaged in significant financial transactions know with whom they are dealing as clients or customers. Adequate controls and procedures, particularly for those relationships that present a higher risk for money laundering and terrorist financing (ML/TF), are necessary to accomplish this. Without adequate due diligence, these businesses can become subject to several risks—reputational, operational, legal/compliance, and concentration, among others— that can result in significant financial costs.

The Royal Monetary Authority of Bhutan (RMA) and the Department of Financial Intelligence (DFI) are committed to fight money laundering, terrorist financing, and financing of weapons of mass destruction. To aid in this effort, the RMA and DFI are issuing this Guide to Reporting Entities in Bhutan. Through the advice in this Guide, the RMA and DFI aim to further promote and maintain the financial stability, soundness, and reputation of Reporting Entities and the finance sector in Bhutan.

Customer Due Diligence (CDD) is an important part of the "Know Your Customer" (KYC) process. KYC means knowing who a Reporting Entity's customers are and the relevant information about them and their business. By knowing its potential or existing customers, a Reporting Entity can make an informed decision on whether to accept a potential customer, and what must be done to monitor the customer relationship once it is established. CDD refers to the processes and procedures that enable the Reporting Entity to accomplish these goals. To put it another way, KYC refers to *what* must be done; CDD refers to *how* to do it.

1.2. Objectives of this Guide

This Guide is meant to assist Reporting Entities in (i) predicting, with a reasonably high degree of confidence, the types of transactions in which their customers are likely to engage; (ii) determining the degree of ML/TF risk associated with these transactions; and (iii) developing and implementing systems and processes to control these risks. These systems and processes will assist Reporting Entities in determining when transactions are potentially suspicious, and what action they need to take based on these determinations.

This Guide does not introduce new regulatory requirements; rather it aims to assist Reporting Entities comply with existing laws and regulations relating to money laundering, terrorist financing, and financing of weapons of mass destruction. The objective is to minimize the possibility of these entities and individuals becoming involved in these activities, thereby reducing the risks to their own reputations and to the finance sector.

1.3. Legal Bases

The main laws and regulations relating to money laundering and terrorist financing (where applicable as amended) are:

(1) The Anti–Money Laundering and Countering of Financing of Terrorism Act of Bhutan 2018 (AML/CFT Act).

(2) Financial Intelligence Unit (FIU) G1: Guidelines for Appointment of AML/CFT Compliance Officer (AMLCO).

(3) FIU G2: Suspicious Transaction Guidelines for Reporting Entities 2014.

(4) FIU G4: Guideline on Anti-Money Laundering and Combating the Financing of Terrorism for Capital Market Intermediaries 2014.

(5) FIU G5: Anti-Money Laundering and Combating the Financing of Terrorism guideline for Money Service Business 2014.

In accordance with the AML/CFT Act, all Reporting Entities:

(1) are required to apply customer due diligence to all customers in accordance with their anti– money laundering/countering financing of terrorism prevention program; and

(2) may apply simplified customer due diligence to low risk customers with the written approval of their supervisor.

Per Section 50 of the AML/CFT Act, Reporting Entities include:

(1) financial institutions, and

(2) designated nonfinancial businesses and professionals.

The AML/CFT Act defines a "financial institution" as "a bank, insurer, reinsurer, stock exchange or another entity licensed under Financial Services Act 2011 to the extent designated to a financial institution under regulations adopted by the Royal Monetary Authority in light of the licensee's scale of operation and the exposure of its customers to its insolvency". The AML/CFT Act lists several activities that financial institutions perform on behalf of customers:

(1) Acceptance of deposits and other repayable funds from the public, including private banking;

(2) Lending, including, but not limited to, consumer credit, mortgage credit, factoring (with or without recourse), and financing of commercial transactions, including forfeiting;

(3) Financial leasing other than with respect to arrangements relating to consumer products;

(4) Money or value transfer services;

(5) Issuing and managing means of payment, including, but not limited to, credit and debit cards, cheques, travelers' cheques, money orders and bankers' drafts, and electronic money;

(6) Issuing financial guarantees and commitments;

(7) Trading in

(a) money market instruments, including, but not limited to, cheques, bills, certificates of deposit and derivatives;

(b) foreign exchange;

(c) exchange, interest rate and index instruments;

(d) transferable securities; and

(e) commodity futures trading;

(8) Participation in securities issues and the provision of financial services related to such issues;

(9) Individual and collective portfolio management;

(10) Safekeeping and administration of cash or liquid securities on behalf of other persons;

(11) Otherwise investing, administering, or managing funds or money on behalf of other persons;

(12) Underwriting and placement of life insurance and other investment related insurance, including insurance intermediation by agents and brokers;

(13) Money and currency trading;

(14) Engaging in funds transfers as a business; or

(15) Carrying on such other activity, business, or operation as prescribed by rules and regulation.

"Designated non-financial businesses or professions" include:

(1) Real estate agents;

(2) Dealers in precious metals;

(3) Dealers in precious stones;

(4) The professionals and accountants of the private and independent legal officers;

(5) Unit trust service providers;

(6) Trust and company service providers not otherwise covered by the AML/CFT Act which, as a business, prepare or carry out transactions on behalf of customers in relation to any of the following services to third parties:

(a) Acting as a formation, registration, or management agent of legal persons;

(b) Acting as, or arranging for another person to act as, a director or secretary of a company or a partner of a partnership, or to hold a similar position in relation to other legal persons;

(c) Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership, or any other legal person or arrangement;

(d) Acting as, or arranging for another person to act as, a trustee of an express trust or other similar arrangement;

(e) Acting as, or arranging for another person to act as, a nominee shareholder for another person;

(7) Other businesses and professions that may be prescribed by rules and regulations.

In accordance with Section 40 of the AML/CFT Act, the RMA supervises the following businesses and activities licensed or registered under the Act:

(1) Banks;

(2) Insurers or reinsurers;

(3) Securities brokers;

(4) Investment advisors;

(5) Investment fund operators;

(6) Securities depositories or registries;

(7) Foreign exchange dealers; and

(8) Money value transfer services.

Further, Section 44 of the Act empowers DFI to supervise a Reporting Entity for which no supervisor is identified.

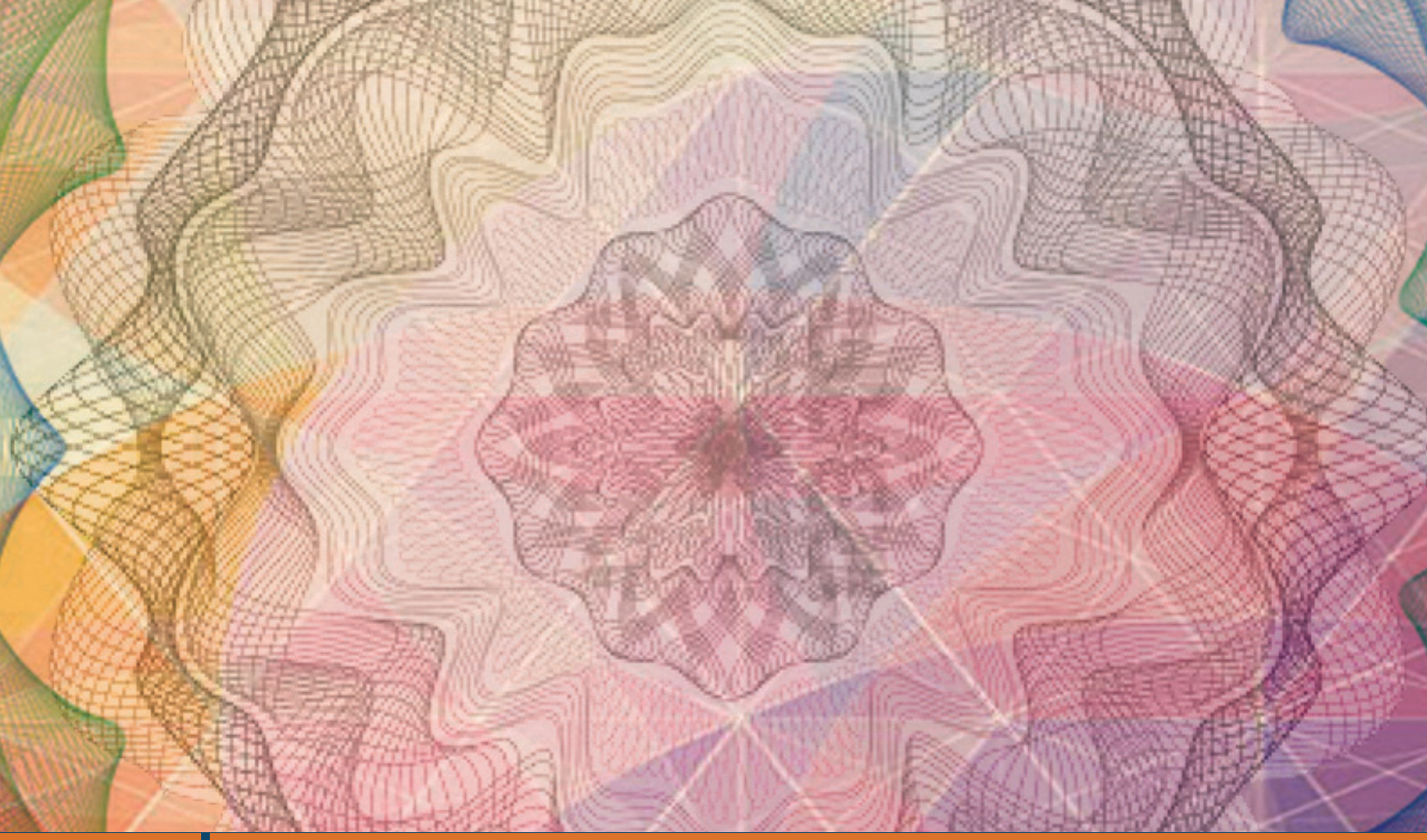
Per the Act, the RMA is authorized to issue guidelines to Reporting Entities that are subject to its supervision (Section 45). Thus, this Guide applies to the Reporting Entities referenced in the preceding paragraph.

1.4. Organization of this Guide

This Guide is divided into four parts:

- **Part I** is an overview of the objectives and purposes of the Guide.
- **Part II** contains general information that is common to all Reporting Entities. It includes information on customer identification and due diligence, risk identification, and general measures to control these risks.
- **Part III** focuses on the types of transactions and services that are most common to banks.
- **Part IV** pertains to nonbanks that are subject to the supervision of the RMA for AML/CFT purposes under the Act.

Some of the information in each part will, of course, be applicable to other parts. In addition, there is necessarily some overlap in the information covered in the respective parts. For example, banks typically engage in transfers of funds, but there are also licensed money transfer service firms that engage exclusively in this activity. Reporting Entities are therefore strongly encouraged to review all of the parts carefully and to consider what information in other parts may be applicable or useful for their own situation.



02. General Information Applicable to All Reporting Entities

2.1. The Risk-based Approach to Customer Due Diligence

The AML/CFT Act, as well as international standards, require that a risk-based approach be applied to CDD.

The risk-based approach (RBA) is the most efficient and appropriate means of managing and reducing the ML/TF risks faced by a business. It enables the business to concentrate its efforts where they are most needed. This means that the costs to the business and its customers will be balanced with the real levels of risk that the business faces, as determined by its board of directors and management. For example, if a business provides low-risk products to low-risk customers, its approach will be relatively simple; if it provides high-risk products to high-risk customers, a greater level of sophistication will be necessary.

The steps involved in applying the risk-based approach are

(1) identifying the business's ML/TF risks;

(2) assessing those risks;

(3) developing and implementing processes to manage and reduce those risks;

(4) monitoring and continuously improving those processes; and

(5) recording what has been done, and why.

Using this approach, an enterprise can determine for itself what are the main AML/CFT risks it is likely to face to assess each risk; decide how great each one of them is; and put in place policies, procedures, and processes to manage and reduce those risks.

Reporting Entities should do an enterprise-wide risk assessment which will form the basis of an RBA. An RBA enables the Reporting Entity to understand how and to what extent it is vulnerable to ML/TF. The policies, procedures, and processes that form the overall RBA should always be properly documented, maintained, and communicated to relevant personnel within the entity.

A Reporting Entity's risk assessment does not have to be complex, but it should reflect the type and size of its business. For smaller or less complex businesses (for example where the customers are relatively homogenous and/or where its products and services are quite limited), a simple risk assessment will likely be enough. Conversely, if an entity offers more sophisticated products and services, has numerous subsidiaries or branches operating in many jurisdictions, or maintains a more diverse customer base, a more detailed risk assessment will be necessary.

In identifying and assessing its ML/TF risks, a Reporting Entity should consider the following:

(1) the nature, scale, diversity, and complexity of its business;

(2) its target markets;

(3) the risk profile of its customers, particularly those that may be considered high risk;

(4) the jurisdictions where it operates, or where its customers reside or conduct business, including in particular jurisdictions known to have significant levels of corruption or organized crime, terrorist activity, and/or deficient AML/CFT regimes, based on reports of reputable international standard–setting bodies such as the Financial Action Task Force (FATF);

(5) its distribution channels, including whether it deals with customers directly or uses the services of third parties or agents to conduct the CDD process, and the extent to which it uses technology;

(6) findings of internal or external audits and government regulatory or supervisory bodies;

(7) the volume and size of its transactions relative to its typical activity and the profile of its customers.

Once the potential risks to the business have been established, it is likely not all its customers and services will pose the same level of risk. As such, a Reporting Entity will unlikely need to apply the same level of due diligence to all its customers equally. This Guide refers to three levels of due diligence: (i) standard, (ii) simplified, and (iii) enhanced. The level of identified risk will determine the level of due diligence required.

Closely held companies and other entities, such as trusts, are generally considered to carry higher risk than publicly owned companies. This is because they are subject to a lower level of external scrutiny than those quoted on organized stock exchanges. For such relationships, the identities of the beneficial owners and ultimate controlling persons need to be verified in addition to the identities of the actual corporate customers. Beneficial owners may also be executives or directors of such companies or the settlors of trusts (for more detailed information, see discussion below on beneficial ownership).

2.2. Customer Identification Program

Sound KYC policies and procedures are an important factor in protecting the financial integrity of Reporting Entities and the financial system. These policies and procedures go beyond the simple mechanics of account opening and document filing. They require Reporting Entities to formulate customer acceptance policies and tiered customer identification programs that involve closer scrutiny of higher risk accounts as well as proactive monitoring of the customer relationships for suspicious transactions or activities.

The KYC framework presented here will assist Reporting Entities in designing their own programs. An overriding aim of this Guide is to ensure that Reporting Entities obtain sufficient customer information. This will aid and/or detect suspicious transactions and/or activities and create effective "audit trails" that can be used in the event of any subsequent investigation or legal proceedings.

Each Reporting Entity is required to collect, verify, and keep records of customer identification information and conduct sanction screening against lists of known criminals/United Nations Security Council Resolutions.

This Guide provides clear standards on how to conduct CDD at each stage of a business relationship with a customer or client:

(1) when the relationship is established;

(2) when financial transactions with existing customers are performed;

(3) on an ongoing basis after the business relationship is established.

Customer acceptance policies and procedures should include provisions for obtaining a description of the types of customers likely to pose a higher-than-average risk. Factors such as the customer's background, country of origin, public or high-profile position (such as politically exposed person [PEP] status), linked accounts, business activities, and other risk indicators should be considered.

Where an account is managed by a trustee or other professional intermediary (such as a lawyer/law firm, chartered accountant, or other agent), information confirming the legal authority of that person should be ascertained.

At a minimum, due diligence and screening should confirm that beneficial owners and relevant entities are not in the sanction lists, PEP involvement, and other government database checks.

In determining what level of due diligence is appropriate (standard, simplified, or enhanced due diligence), a Reporting Entity should look for "red flags" relating to

(1) the customer's residence or location of the customer's business;

(2) the customer's occupation or nature of business;

(3) the purpose of the business transactions;

(4) the anticipated pattern of transaction activity, including monetary amounts, and frequency;

(5) the anticipated origin and methods of payments;

(6) basic founding documents of legal entity customers, such as articles of incorporation, partnership agreements, and business certificates;

(7) basic information about the customer's own customers;

(8) identification of beneficial owners of an account or entity customer;

(9) basic information about the customer's other significant personal and business relationships;

(10) approximate annual income or business revenue;

(11) AML policies and procedures in place;

(12) third-party documentation;

(13) the customer's reputation in the local market, through review of media and other publicly available sources.

2.3. What is Customer Due Diligence?

CDD entails (i) identifying a Reporting Entity's customers, and (ii) confirming that they are who they say they are.Simply put, Reporting Entities must satisfy themselves that they know with whom they are dealing and do so with the best available information.

CDD comprises the following elements:

(1) identifying the customer through documents, data, or other information obtained from trustworthy independent sources;

(2) identifying, where applicable, each beneficial owner of the relevant account(s) or legal entity customer, and employing risk-based measures to understand the true ownership and control structure of the customer;

(3) determining the purpose and anticipated nature of the business relationship;

(4) continuously monitoring the relationship, which should include ensuring that transactions are compatible with what the Reporting Entity knows about the customer's profile, business, and risk level, including, where necessary, the customer's source of funds and/or wealth, and ensuring that all relevant documents, data, and other information are kept current.

Reporting Entities should undertake a combination of steps and apply the appropriate level of CDD based on their assessment of the ML/TF risk that each customer presents. Three categories of CDD can be applied—simplified, standard, and enhanced.

2.4. When to Undertake Due Diligence

FATF standards call for due diligence to be applied

(1) when establishing a business relationship with a potential customer;

(2) when carrying out an "occasional transaction" as follows:

(a) above the applicable designated reporting threshold (in Bhutan, Nu. 500,000), including situations where the transaction is carried out in a single operation or in several operations that appear to be linked, or;

(b) involving a wire transfer in the circumstances referenced below;

(3) when there is reason to suspect a customer's involvement in ML/TF or other criminal activity;

(4) when there is reason to doubt the identification information the customer has provided; and

(5) when circumstances indicate that it is necessary in the case of existing customers; for example, if there is a significant change in their business activities or the geographic locations where they operate or have business relations.

In accordance with the AML/CFT Act, some level of due diligence is required for all customers, although the intensity may vary depending on the nature of the customer and the degree of ML/TF risk posed by the relationship.

2.5. Simplified Customer Due Diligence

Simplified due diligence is the lowest level of due diligence that can be completed on a customer. This is appropriate where there is little opportunity or risk of an entity's services or customer becoming involved in ML/TF.

For example, simplified CDD can be used for small-value accounts, such as savings accounts of no more than a certain threshold [tiered KYC] that do not involve international transfers of funds.

Where a Reporting Entity is satisfied that a customer, product, or service falls into the simplified due diligence category, then it is only required to identify the customer. This can be done by requiring the customer to submit certain basic information such as his or her name, citizenship identity card, address, and so forth, along with a passport-type picture. In the case of such small limited-use accounts, the information may be submitted electronically or in person at the office of the Reporting Entity or its agent. This information does not need to be verified through third party sources.

The AML/CFT Act 2018 requires approval of the Reporting Entity's supervisor in simplified due diligence. Reporting Entities that wish to apply simplified CDD to certain customers should therefore submit their proposed CDD policies and procedures to their supervisor, outlining the circumstances for simplified CDD.

While simplified CDD is sufficient when starting a low-risk relationship, the Reporting Entity should continuously monitor the account for any significant circumstances that may require heightened scrutiny in the future. If during the business relationship additional information indicates that the relationship may pose a greater risk than originally determined, the Reporting Entity should undertake increased due diligence.

2.6. Standard Due Diligence

Most customer relationships can be handled through standard due diligence. The following information comprises the elements of standard due diligence, which should be applied when a new business relationship is established or certain occasional transactions are to be conducted. Simplified due diligence can be used in circumstances described above. Enhanced due diligence, which entails heightened measures, should be applied in the circumstances described below.

2.6.1. Customer due diligence when establishing a business relationship

When a Reporting Entity establishes a new business relationship with a customer, it should determine the following:

(1) the purpose of the relationship;

(2) the intended nature of the relationship, such as where the customer's funds will come from, the general purpose of transactions, and so on.

The Reporting Entity may need to obtain the following type of information:

(1) details of the customer's business or employment;

(2) the expected sources and origin of the funds that the customer will be using during the relationship;

(3) copies of recent and current financial statements;

(4) details of the relationships between the customer (including signatories on any account) and any underlying beneficial owners;

(5) the expected level and type of activity that will occur during the relationship.

For the detailed list of the documents that the Reporting Entities can ask for, please refer to Appendix I.

Where a Reporting Entity determines that it cannot obtain information sufficient to enable it to know its customer and the risks posed by the business relationship, it should

(1) not open the account, start business relations or perform the requested transaction, or terminate the existing business relationship; and

(2) consider making a suspicious transaction report (STR) regarding the customer.

If a Reporting Entity suspects money laundering or terrorist financing but is concerned that the CDD process would tip off the customer, it need not pursue the process. Instead, it should file an STR. This decision should be thoroughly documented according to the Reporting Entity's policies and procedures (see discussion below).

2.6.2. Purpose and intended nature of business relationship

The nature and intended purpose of a new business relationship or occasional transaction are important factors in assessing the risks posed by the relationship or transaction. Unless it is obvious from the product involved, Reporting Entities should determine the following:

(1) the expected type, volume, and value of activity associated with the relationship;

(2) the expected geographic location or sphere of the customer's activity; and

(3) details of any existing relationships between the Reporting Entity and the customer.

For legal persons and arrangements, this information should include:

(1) a thorough understanding of the ownership and control structure of the entity, including characteristics of the group of which the entity is a member (such as the ultimate parent company, beneficial owners, etc.) where applicable;

(2) the nature of activities undertaken by the customer or group (considering the need to protect sensitive information such as trade secrets, etc.);

(3) the main geographic location(s) or sphere of the entity's activities and assets; and

(4) the name of the entity's regulator, if any.

It is a good business practice to obtain the list of all directors of the entity. This will be helpful in determining whether any of these persons, or the customer's controlling persons or beneficial owners, might be PEPs or other high-risk persons.

Reporting Entities should also closely monitor transactions undertaken during the business relationship to confirm that they are consistent with the client's profile and the Reporting Entity's assessment of the risks associated with the relationship.

2.6.3. Source of funds & wealth

Part of CDD when entering a new relationship or carrying out an occasional transaction entails determining a customer's source of funds. For higher risk customers, Reporting Entities should also consider inquiring about the source of wealth. This should be done, for example, for all foreign PEPs, higher risk domestic PEPs, and when unusual activity occurs. This could include, for example, situations where the product or service requested does not match the customer's profile or is otherwise inconsistent with known facts about the relationship.

An inquiry regarding the source of funds refers to determining where the money is coming from to finance the relationship or carry out the requested transaction. This does not necessarily mean that the Reporting Entity must scrutinize every payment going through a customer's account, but it must ensure that it has effective ongoing monitoring provisions so that it can recognize potentially unusual activity.

A customer's source of funds will often be a bank account maintained by the customer. Where this is not the case, such as when funds are provided by a third party, the Reporting Entity may take an RBA and determine whether to inquire about the relationship between the provider of the funds and the customer, including beneficial ownership factors. Reporting Entities should consider verifying the identity of the ultimate underlying owner or provider of the funds. When deemed necessary, the Reporting Entity should document the steps it took to determine the source of funds and, if applicable, the beneficial owner. This information should be retained on file.

Source of wealth differs from *source of funds*. *Source of funds* refers to the origin of the specific funds or assets that will be used for a transaction (for example, deposit, investment, payment for insurance premium, or remittance) or to establish a business relationship. *Source of wealth*, a broader concept, refers to the origin of the entire body of the customer's (or potential customer's) wealth (i.e. total assets), even if those assets will not necessarily be the same assets used for one of these purposes. In short, source of wealth refers to the origin of a customer's total financial standing.

2.6.4. Identification of beneficial owners

One of the most critical aspects of customer identification is knowing the beneficial owner of an account or of a legal entity that seeks to become a customer of an institution. The AML Act requires Reporting Entities to identify and maintain records of such beneficial owners (Section 68).

Section 187(5) of the AML/CFT Act defines a beneficial owner as

(1) a natural person who ultimately owns or controls the rights to or benefits from a property, including the person on whose behalf a transaction is conducted; or

(2) a person who exercises ultimate effective control over a legal person or a legal arrangement.

Per the AML/CFT Act, a natural person is deemed to ultimately own or control rights to or benefit from property within the meaning of the above definition when that person

(1) owns or controls, directly or indirectly, whether through trusts or bearer share holdings for any legal entity 25% or more of the shares or voting rights of the entity; or

(2) otherwise exercises control over the management of the entity.

Beneficial ownership is not always obvious. For this reason, it is good business practice for a Reporting Entity to require each account holder to complete and sign a "beneficial owner declaration form" as presented in the Appendix for each account. A similar form (or a different part of the same form) can also be used to obtain information about the beneficial ownership of legal entity customers, particularly those that are owned through multiple layers of entities.

2.6.5. Legal entities or arrangements: direct/indirect ownership

Ownership of a legal entity, such as a company, may be either direct or indirect, i.e., through one or more controlled entities, such as subsidiaries. It includes ownership that is exercised alone or jointly ("acting in concert") with one or more other persons.

In determining "effective" control of a legal entity customer, the Reporting Entity should take steps to identify any person or persons:

(1) who can elect a majority of the board of directors, supervisory board, or any equivalent body, of a legal entity; or

(2) who can exert a "dominant influence" over the financial, economic, or management policies of the entity regardless of the amount, if any, of share ownership or voting rights in that entity.

In determining "dominant influence" (point 2 above), the institution should take particular note of any situation in which a majority of the members of the board of directors, supervisory board, or any equivalent body, of a legal entity are accustomed or are obliged to act in accordance with a given person's directions, instructions, or wishes in conducting the affairs of the entity. Such an obligation may be formal or informal, written or unwritten.

In some cases, it may not be possible based on the above criteria to identify a natural person who ultimately owns or exerts control over a legal entity. In such cases, Reporting Entities may deem one or more senior management officials (such as the chief executive officer) to be the beneficial owner(s) of the entity. This, however, should be done after the Reporting Entity is satisfied that it has exhausted all other means of identification, and that there is no reason to suspect "hidden" or concealed beneficial ownership. The Reporting Entity should keep records of the actions taken to identify the beneficial ownership.

2.6.6. Ownership or control structure: legal entities

Reporting Entities need to ensure that they clearly understand the ownership and control structure of any legal entity customer with multiple layers of ownership. This means, among other things, that any intermediate layers of the company's ownership structure should be fully identified. The Reporting Entity, through its internal procedures, should determine the manner in which this is accomplished. A very effective way to gather this information is to obtain a declaration from a knowledgeable person, such as a senior official, director, or majority shareholder, and an ownership chart clearly showing the intermediate layers with the respective ownership amounts. The amount and degree of detail of the information can be determined on a case-by-case basis depending on the perceived degree of

risk, but in all cases should include certain basic information. The name of each company in the group, its jurisdiction of incorporation, and the amount of ownership (direct and indirect) held by other persons, should all be included. If the Reporting Entity believes the ownership structure to be needlessly complex, it should inquire about the rationale for the structure. The goal should always be to trace the chain of ownership and actual effective control "all the way to the top," i.e., to the individuals who are the ultimate beneficial owners of the direct customer, and to verify the identity of those individuals.

A Reporting Entity does not necessarily need to verify the details of intermediate entities in an ownership chain, unless the structure arouses suspicion. However, Reporting Entities should be aware that extremely complicated ownership structures (for example, numerous layers, cross-ownership, companies and controlling shareholders located in different jurisdictions, trusts, and so forth) without an obvious business purpose are often tools for illegitimate activities and should prompt further inquiry. In some cases, ownership is purposely set up in a confusing manner to hide the actual beneficial owners and their illicit business activities. In these cases, further steps may be necessary to ensure that the Reporting Entity is satisfied on the identity of the beneficial owners and that their business activities are legitimate.

2.6.7. Effective control of property

In the case of property, Reporting Entities should take steps to identify any person who can decide on the ownership, use, and/or disposition of such property.

Per Section 187(9) of the AML/CFT Act, property, or an interest in property, may be subject to the effective control of a person whether that person has

(1) a legal or equitable estate or interest in the property; or

(2) a right, power, or privilege in connection with the property.

In determining this, the AML/CFT Act notes that Reporting Entities should consider

(1) shareholdings in, debentures over, or directorships of any company that has an interest (whether direct or indirect) in the property;

(2) a trust that has a relationship to the property; and

(3) a family, domestic, and business relationship between persons having an interest in the property, or in companies or trusts of the kind referred to above, and other persons.

2.7. Enhanced Customer Due Diligence

In higher risk situations, additional CDD measures beyond standard measures, or Enhanced Customer Due Diligence (ECDD), are necessary.

The extent of these additional measures, including what additional information will be sought and any heightened monitoring regarding any particular customer, will depend on the degree of ML/TF risk the customer might pose to the Reporting Entity. ECDD can take many forms, including

(1) obtaining more detailed information, including additional evidence of identity for verification;

(2) obtaining and updating additional information about the customer and beneficial owner (e.g. volume of assets and other information from public databases);

(3) inquiring further about the customer's source of funds or wealth;

(4) obtaining additional information about the intended level and nature of the business relationship;

(5) inquiring further about the reasons for intended or performed transactions; and

(6) in certain situations, obtaining the permission of senior management before establishing or continuing the relationship.

International standards (such as the FATF standards) and the AML/CFT Regulation note several circumstances when ECDD should be applied:

(1) where the client or beneficial owner is a PEP;

(2) where a prospective customer is acting, or appears to be acting, as an agent for a principal, particularly for a nonresident principal, or is reluctant to disclose information about the principal;

(3) where there is a reasonable suspicion of ML/TF[1];

(4) in trusts and fiduciary relationships;

(5) cash-intensive businesses or customers (particularly nonresident customers) purchasing large volumes of high value goods such as cars, jewelry, real estate;

(6) clients from jurisdictions

  (a) that are subject to financial sanctions, embargoes, or similar measures by the United Nations or other public international organizations;

  (b) that have been identified by credible sources[2] as

    (i) having deficient AML/CFT regimes;

    (ii) having significant amounts of corruption or other criminal activity, including illegal drug production, distribution, or trafficking; money laundering; or human trafficking;

    (iii) providing financing or supporting terrorism or terrorist activities, or having terrorist organizations operating within their territory;

    (iv) being tax havens; or

    (v) experiencing significant civil unrest.

(7) in non-face-to-face business relationships or transactions;

(8) correspondent banking relationships;

(9) transactions or customer relationships involving new technologies; and

(10) money value or transfer services, including wire transfers.

2.8. When to Apply Customer Due Diligence for Occasional Transactions

CDD is necessary for occasional transactions where the value is Nu.500,000 or more, even if these are not carried out within the context of an ongoing business relationship. This applies to both single and linked transactions.

Related or linked transactions are individual transactions of less than Nu500,000 that have been purposely broken down into these separate, smaller transactions to avoid triggering CDD checks or reporting to the DFI. Reporting entities must have systems in place to detect potentially linked transactions.

If a Reporting Entity identifies transactions that appear to be linked, the next step is to determine whether they have been purposely split ("structured") to avoid detection. Some red flag items to consider are

1 Reporting entities are not expected to investigate or confirm either the actual money laundering activity or the underlying crime in determining whether to apply Enhanced Customer Due Diligence (ECDD) or, ultimately, whether to file a Suspicious Transaction Report (STR). A reasonable suspicion is all that is necessary.

2 Credible sources include the Financial Action Task Force (FATF), FATF-style regional bodies such as the Asia Pacific Group on Money Laundering and the Egmont Group, national authorities such as the Office of Foreign Assets Control of the US Department of Treasury, or other reliable third parties such as regulatory authorities, international standard–setting bodies such as the International Organization of Securities Commissions, the Basel Committee, the International Association of Insurance Supervisors, or securities or commodities exchanges.

(1) whether the same customer or group of customers have carried out all or most of the transactions within a short period;

(2) circumstances suggest that several customers were acting on behalf of the same person when carrying out the transactions;

(3) where several customers have sent money transfers to the same person.

In certain circumstances, CDD is also appropriate even for occasional transactions amounting to less than Nu.500,000. This is the case, for example, when the nature of a transaction raises the suspicion that there is a higher risk of money laundering.

2.9. Ongoing Due Diligence

Reporting Entities can only control and mitigate their risk if they have an ongoing knowledge of their customers' business and account activities. Through this knowledge, they can identify transactions that are not typical of the regular pattern of a customer's activity. Conversely, without this knowledge, they are likely to miss suspicious transactions that they are required to report to the DFI Ongoing monitoring techniques may include

(1) reviewing transactions for consistency with the Reporting Entities' knowledge of the customer, their business and risk profile, including where necessary the source of funds and the source of wealth; and

(2) periodically reviewing existing CDD documentation to ensure that it is current and still relevant, especially for higher risk customer relationships.

For all accounts, Reporting Entities should have systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing benchmarks for classes or categories of transactions, and paying closer attention to transactions that exceed these benchmarks. Certain types of transactions should alert Reporting Entities to the possibility that the customer is conducting unusual or suspicious activities. Reporting Entities may consider the economic background and purpose of any transaction or business relationship which

(1) appears unusual;

(2) is inconsistent with the expected pattern of the client's activity or business model relative to the generally observed volume of transactions;

(3) does not have any apparent economic or business purpose; or

(4) creates doubt about the legality of such transactions, especially regarding complex and large transactions or involving higher risk customers.

Higher risk accounts should undergo intensified monitoring. Examples of techniques to accomplish this include setting key benchmarks or indicators for such accounts, and observing certain facts about the customer's background, such as the country of origin and source of funds, and the kinds of transactions undertaken.

Reporting Entities need to be especially vigilant when engaging in business relationships with PEPs and other high profile individuals, and with persons and companies that are clearly related to or associated with these persons. Because not all PEPs are identified initially, and ordinary customers sometimes become PEPs after the business relationship is established, Reporting Entities should periodically review the information and activities of at least the more important customers.

2.10. Requirements for Multiple Signatories or Directors

In some cases, there may be more than one signatory on a client account or more than one person authorized to act for the client. Reporting Entities should determine which signatories will likely sign off on transactions or are deemed to be acting on behalf of the customer. They should also consider the level of signing authority and determine whether the signatory's authority is considered significant. As noted above, in both standard CDD and ECDD situations, it is a good

practice to obtain the list of all directors. This information will help the Reporting Entity determine whether any PEPs or other higher risk persons are associated with the customer, and who is authorized to act on the customer's behalf.

2.11. Identification Requirements for Multiple Third Parties

A legal entity customer may allow one or more third parties to have limited control over some of his or her affairs, such as a signing authority on a bank account. Reporting Entities need to be aware of and understand the rationale for such an arrangement and be comfortable with it from an AML/CFT risk management standpoint. The authority, rationale, and Reporting Entity's review should be documented. If the arrangement involves many potential third parties, such as staff members of a legal entity, the Reporting Entity should obtain a list of the names and accompanying signatures of all such persons and fully identify and verify those persons who are expected to exercise such authority.

2.12. Changing Circumstances of Customers

Reporting Entities should keep current information about their customers. This allows them to

(1) amend their risk assessments of particular customers if their circumstances change; and

(2) update their CDD information, including carrying out ECDD if necessary.

Changes of circumstance refer to

(1) a significant change in the volume or type of the customer's business activity; and

(2) a significant change in the ownership or control structure of the business.

2.13. Where Customer Due Diligence Cannot Be Carried Out

In situations where Reporting Entities cannot obtain satisfactory evidence of the identity of a customer through their CDD measures, they must

(1) not carry out the transaction for the customer (in the case of a requested one-off transaction);

(2) not establish a business relationship (in the case of potential new business);

(3) discontinue the business relationship (existing business), report the matter to the Compliance Officer (who may decide, depending on the circumstances, that the filing of an STR is necessary).

2.14. Persons Who Should Not Be Dealt with as Customers

Reporting Entities must have policies and procedures to ensure that business relationships are not established or continued, or transactions are not carried out

(1) where the Reporting Entity has not obtained satisfactory evidence of customer's identity;

(2) with shell banks;

(3) with anonymous accounts; and

(4) for persons identified by the Security Council of the United Nations (UN) or other credible sources as terrorist entities or terrorists. Links to the UN list, FATF list, and European Union terrorist list are available on DFI's website.

2.15. Politically Exposed Persons

2.15.1. Overview

The AML/CFT Regulation defines two variations of PEPs:

> Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example, heads of state or of government; senior politicians; senior government, judicial, or military officials; senior executives of state-owned corporations; and important political party officials.
>
> Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, and important political party officials.
>
> Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management—i.e., directors, deputy directors, and members of the board or equivalent functions.
>
> The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Reporting Entities should apply ECDD procedures when opening and/or maintaining accounts for PEPs. Specifically, they should:

(1) Ensure that their risk management systems will enable them to determine whether a potential or existing customer (including any beneficial owner) is a PEP.

(2) Have procedures requiring senior management approval to establish or continue business relationships with PEPs.

(3) Determine the source of wealth and the source of funds of PEP clients.

(4) Conduct enhanced ongoing monitoring of their relationships with PEPs. This should include, at a minimum, greater oversight of the PEP's account to identify changes in patterns of behavior or business activity.

In accordance with international AML/CFT (e.g., FATF) standards, the above requirements regarding PEPs also apply to their family members and close associates.

2.15.2. Family members

Family members include individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership.

2.15.3. Close associates

Close associates of PEPs are individuals closely connected to a PEP, either through social or professional relationships. Examples include:

(1) prominent members of the same political party, civil organization, labor or employee union as the PEP;

(2) business partners or associates of the PEP, especially those who

(a) share beneficial ownership of legal entities with the PEP, or

(b) are otherwise connected (such as through joint membership on a company board);

(3) known sexual or romantic partners of the PEP outside of the PEP's family unit.

2.15.4. Once a PEP, always a PEP

The RMA generally expects Reporting Entities to apply the "once a PEP, always a PEP" principle. This means that an individual who has been identified as a PEP should continue to be treated as such even after he or she is no longer in that prominent public function. However, an RBA is acceptable if certain safeguards are in place, as outlined below.

If a Reporting Entity chooses not to adopt this approach for a customer, it should ensure that there is a clear and well-documented reason the individual should not continue to be treated as a PEP. That rationale should include considerations such as

(1) the nature and duration of the person's public role;

(2) the amount of time that has elapsed since he or she was in that role;

(3) the level of (informal) influence that the individual could still exercise; and

(4) whether the person's previous and current functions are in any way connected (for example, formally through appointment of the PEP's successor, or informally such as the former PEP continuing to deal with, or being consulted on, the same or similar matters).

2.16. Third Party Reliance

A Reporting Entity may rely on third parties to conduct CDD or to introduce business. However, the ultimate responsibility and accountability of CDD measures remain with the Reporting Entity relying on the third party.

Certain conditions apply to such third-party relationships:

(1) The relationship must be governed by an arrangement clearly specifying the rights, obligations, and expectations of all parties.

(2) The Reporting Entity must be satisfied with the third party's CDD process, record-keeping provisions, and ability to provide the CDD information and copies of the relevant documentation immediately upon request.

(3) The third party must be properly regulated and supervised by competent authorities.

(4) Reporting Entities must obtain written confirmation from the third party that it has conducted CDD on the customer or beneficial owner in line with the AML/CFT Act and any relevant regulations. However, ultimate responsibility still rests with the Reporting Entity and the CDD obligations are still applicable to the Reporting Entity. Specifically, the Reporting Entity must perform its own analysis and review of the information, including independent verification, where appropriate.

(5) Reporting Entities may not rely on third parties located in higher risk countries that have been identified by credible sources as having deficient AML/CFT regimes or ongoing or substantial ML/TF risks.

Such third party reliance is distinct from outsourcing/agency arrangements, in which the outsourced entity undertakes CDD on behalf of the delegating Reporting Entity. In the latter case, the outsourced entity operates in accordance with the Reporting Entity's procedures, and is subject to the delegating Reporting Entity's control of the effective implementation of those procedures. In a third-party reliance scenario described above, the third party will usually have an existing business relationship with the customer, which is independent from the relationship or potential relationship with the Reporting Entity.

2.17. Non–Face–to–Face Clients

In some situations, a customer may not be physically present when conducting transactions. This occurs especially in connection with electronically provided services. All provisions regarding face-to-face clients set out in this Guide apply to non-face-to-face clients. Reporting Entities also must put in place CDD policies to address specific issues posed

by non-face-to-face business relationships or transactions. For example, banks may reduce their risks by requiring a customer to remit his first payment through an account maintained at another bank that has performed CDD on the customer.

Reporting Entities must apply equally effective customer identification and ongoing monitoring procedures of non-face-to-face customers as to traditional relationships where the customer is available for personal contact. Where a customer is not physically present for identification purposes, the Reporting Entity usually cannot determine that the identity documentation pertains to the customer it is dealing with. As a result, the risks are increased, and Reporting Entities need to take sufficient measures to deal with such risks.

In these circumstances, it is a good practice to perform at least one of the following measures:

(1) further verifying the customer's identity through documents, data, or information referred to in this Guide but not previously relied upon;

(2) taking additional steps to verify the information provided by the customer, such as requesting additional documents to complement those required for face-to-face customers;

(3) requiring the initial payment into the customer's account to come from an account maintained in the customer's name at a reputable financial institution licensed and operating in a jurisdiction with a suitable AML/CFT regime, and that is effectively supervised for compliance with AML/CFT requirements by competent authorities in that jurisdiction;

(4) obtaining copies of documents that have been certified by a suitable certifier;

(5) making independent contact with the customer; or

(6) obtaining a third-party introduction by a reliable introducer.

Use of a suitable independent certifier can help reduce the risk that the documentation provided might not correspond to the customer whose identity is being verified.

Examples of such suitable certifiers may include

(1) a lawyer or notary practicing in Bhutan;

(2) a professional accountant or auditor practicing in Bhutan;

(3) a trust company carrying on trust business in Bhutan;

(4) a financial institution licensed to do business in Bhutan; or

(5) a lawyer, notary, auditor, professional accountant, trust company, or financial institution that carries out business in a foreign jurisdiction and that

  (a) is registered, licensed, or otherwise regulated in accordance with legal requirements in that jurisdiction;

  (b) has an AML/CFT regime that is at least as stringent as the regime in Bhutan; and

  (c) is effectively supervised for compliance with AML/CFT requirements by a competent authority in that jurisdiction

(6) a member of the judiciary in a foreign jurisdiction that has AML/CFT legal requirements at least as stringent as those imposed in Bhutan; and

(7) an official of an embassy, consulate, or high commission of the country issuing the document(s) being relied upon for identity verification.

For the certification to be effective, the certifier would need to have seen the original document(s). The Reporting Entity should therefore require the certifier to sign and date a copy of the relevant document (with his/her name clearly printed in capitals underneath) and clearly indicate his/her position or capacity on the document. The certifier should also state that the document is a true copy of the original, and should clearly indicate his/her contact details: name, address, e-mail address, telephone number, and any other relevant information.

The identification document may be sent via electronic mail provided that the Reporting Entity receives a certified copy within a specified and reasonable time (for example, no later than 10 business days following the receipt of the electronic version). The copy of the identification document, including any photograph where applicable, should be clearly legible.

Reporting Entities must be aware that they remain responsible for any failure to carry out required CDD procedures, and therefore must exercise care when considering accepting copies of identification documents provided by certifiers. This is particularly true in cases where such documents originate from a country identified by credible sources as having deficient AML/CFT regimes or otherwise constituting a high risk, or from unregulated entities in any jurisdiction.

If a Reporting Entity is uncertain about the authenticity of certified documents or that the documents belong to the customer, it should undertake additional steps to mitigate its ML/TF risk. If it is not satisfied as to these matters, it should decline to establish the relationship or to carry out the requested transaction.

2.18. Timing of Verification

The process of verifying the identity of a customer and/or beneficial owner generally should take place before or during the initial establishment of a business relationship (or in the case of occasional customers, carrying out a transaction for the customer). A Reporting Entity may complete verification after the establishment of the business relationship, provided that

(1) the verification is completed as soon as reasonably practicable;

(2) it is deemed essential, in accordance with the Reporting Entity's AML/CFT policies and procedures, and will not interrupt the normal conduct of business; and

(3) the Reporting Entity's AML/CFT policies and procedures include conditions for such delayed verification to ensure that its ML/TF risks are effectively managed, including provisions for termination of the relationship if the verification is not completed within the prescribed period.

2.19. Bearer Shares

Bearer shares are securities that are owned by whoever holds the actual stock certificate. Neither ownership of the stock nor any transfers of ownership are recorded by the issuing company. Delivery of the physical instrument is the only thing needed to transfer ownership of the stock. Bearer shares therefore lack the regulation and control mechanisms that are associated with common shares because ownership is never recorded. Because of this anonymity, there is a higher risk that bearer shares could be used to facilitate money laundering, terrorist financing, or other criminal or fraudulent activities. International standards therefore require that institutions dealing with companies that issue bearer shares take appropriate steps to ensure that those bearer shares are not misused for such criminal purposes.

The Bhutan Companies Act prohibits domestic companies from issuing bearer shares. However, some foreign jurisdictions do permit companies to issue such shares, and Bhutan's financial institutions may possibly encounter such firms as customers. Reporting Entities dealing with companies that issue such shares need to be particularly diligent, as it is often difficult to identify the beneficial owner(s). Reporting Entities' AML/CFT procedures should include provisions for establishing the identities of the holders and beneficial owners of bearer shares, and for ensuring that the Reporting Entity is notified of any changes of holders or beneficial owners.

The following are examples of suspicious situations that are particularly applicable to bearer shares:

(1) deposits of many bearer securities which are redeemed or sold on the open market shortly thereafter;

(2) cashing of bearer securities without first depositing them into an account;

(3) frequent deposits of bearer securities into an account;

(4) the title on the bearer securities, if any, does not match the name on the account;

(5) changing explanations as to the acquisition of the bearer securities, or an explanation that does not make sense;

(6) frequent deposits of bearer securities in amounts just below the threshold reporting requirement; and

(7) the stock certificate does not have a restrictive legend, but the history of the security and/or the volume of shares being traded suggest that such a legend would be expected.

A Reporting Entity dealing with bearer share entities must conduct ECDD on these companies and their existing shareholders and/or beneficial owners at the time of establishing the relationship. Specifically, the Reporting Entity must

(1) conduct ongoing monitoring of these companies during the relationship by updating the list of shareholders and/or beneficial owners within 30 days after every transfer of ownership;

(2) apply ECDD to any new shareholders and/or beneficial owners;

(3) obtain a declaration before account opening, and annually thereafter, from each beneficial owner holding more than a certain percentage of the customer company's share capital (which should be no more than 10%);

(4) require the customer to notify the Reporting Entity without delay of any changes in the ownership of the shares.

Reporting Entities should also consider taking one or more of the following measures:

(1) requesting that the client company immobilize any issued and outstanding bearer shares, such as by placing the share certificates with a third-party custodian such as a trustee. The arrangement should enable the Reporting Entity to:

(a) confirm at any time that the shares are indeed held by the custodian; and

(b) be informed without delay of any change of ownership of the shares;

(2) requesting that the client company amend its constitutive documents[3] to remove the authority to issue bearer shares and/or restrict the issuance of new shares; or

(3) requesting that the client company cancel any issued and outstanding bearer shares and replace them with registered shares.

Reporting Entities should ensure that the measures taken are documented. Reporting Entities should seek independent confirmation when bearer shares have been deposited with a third party custodian. Such evidence could include, for example, confirmation from the registered agent that the custodian holds the bearer shares, the identity of the custodian, and the name and address of any person who has the rights associated with the shares. The Reporting Entity should also confirm the identity of the custodian of the bearer shares as part of its ongoing periodic review.

2.20. Record Keeping

Section 67 of the AML/CFT Act requires Reporting Entities to

(1) maintain all books and records with respect to its customers and transactions in accordance with Section 68 of the Act; and

(2) ensure that such records and the underlying information are available on a timely basis to DFI and its supervisor as and when they are required to be disclosed under the Act.

Per Section 68 of the AML/CFT Act, such books and records include the following:

(1) Records obtained through customer due diligence measures, including account files, business correspondence, and copies of all documents evidencing the identities of customers and beneficial owners,

3 Constitutional documents of the entity are the documents that define the existence of the entity and regulate the structure and control of the entity and its members.

and records and results of any analysis undertaken in accordance with the Act. Such books and records must be maintained for not less than 10 years after the business relationship has ended.

(2) Domestic and international records of transactions that are sufficient to permit reconstruction of each individual transaction for both account holders and non–account holders. Such records must be maintained for not less than 10 years from the date of the transaction.

(3) Records of any findings resulting from customer risk analysis and related transaction information undertaken in accordance with internal policies, procedures, and rules and regulations. Such records must be maintained for at least 5 years from the date of the transaction.

(4) Copies of suspicious transaction reports or other reports made to DFI including any accompanying documentation. Such records must be maintained for at least 10 years from the date the report was made.

(5) Copies of records relating to risk assessments undertaken under the Act, which shall be maintained for at least 10 years from the date the assessment was completed.

When these records are part of an ongoing investigation or legal proceeding in court, they should be retained beyond the 5-year retention period until the relevant law enforcement authority notifies the Reporting Entity that the records are no longer required.

Reporting Entities are required to ensure that all CDD information and transaction records are readily available to domestic competent authorities upon appropriate authority.

2.21. Anti–Money Laundering/Countering Financing of Terrorism Program

Sections 54 and 55 of the AML Act requires each Reporting Entity to adopt an AML/CFT prevention program. The program should be approved in writing by the Reporting Entity's board of directors. If the Reporting Entity does not have a board, the program should be approved by its sole proprietor, general partner, managing director, or other person who effectively directs the affairs of the Reporting Entity on a day-to-day basis. Each Reporting Entity must make its AML program available to DFI or the RMA upon request. The program must be commensurate with the size and complexity of the Reporting Entity's business, and the ML/TF threats identified in the Reporting Entity's risk assessment. The program must include

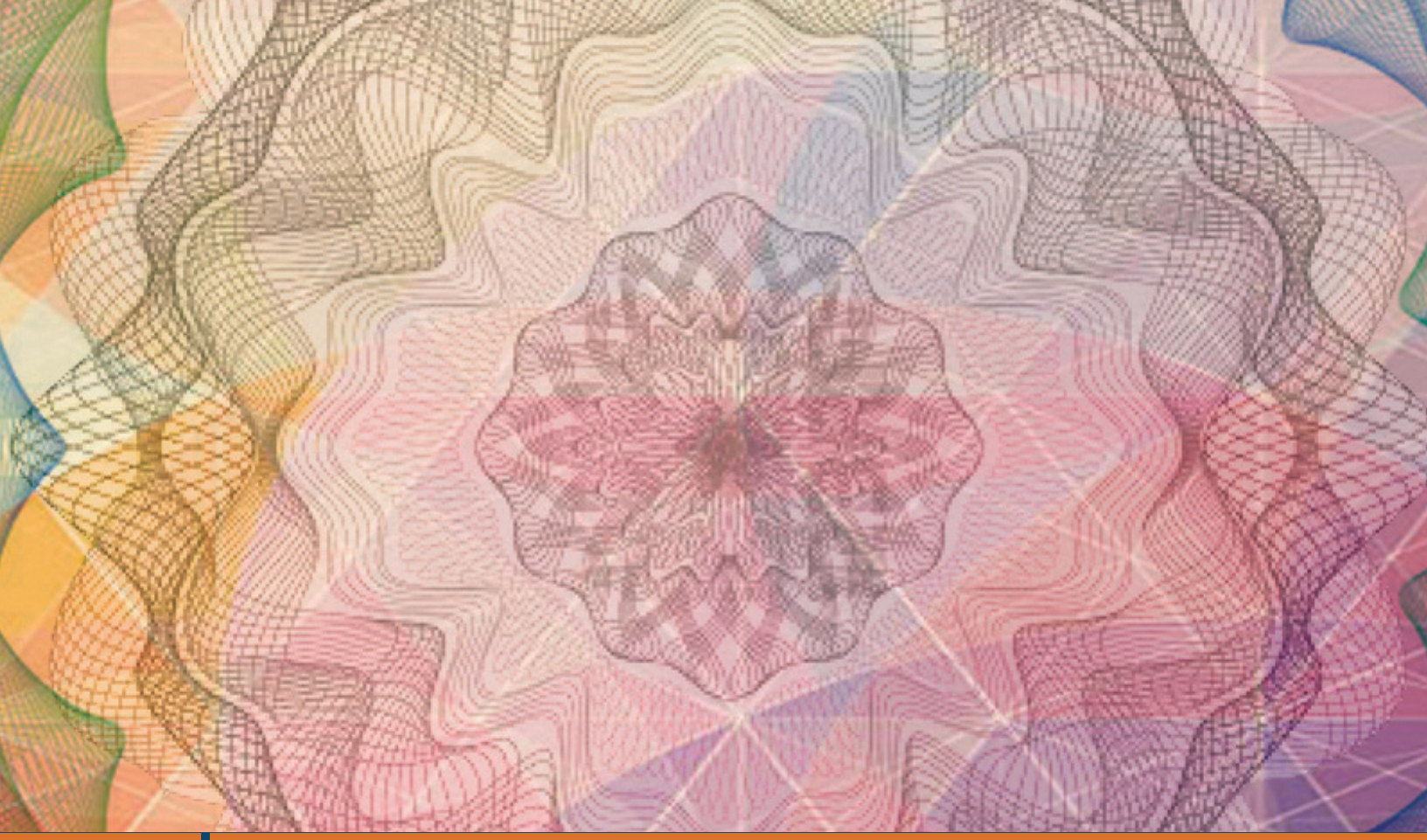
(1) internal policies, procedures, and control to fulfill the obligations imposed under the AML/CFT Act;

(2) adequate screening procedures to ensure that only appropriately qualified persons are employed;

(3) periodic training for directors, officers, and employees to maintain awareness of the Act; regulations, rules, guidelines, and internal policies and procedures relating to ML/TF and to provide guidance on the identification of suspicious transactions, behavior, and the procedures to be followed to deal with those;

(4) ongoing reviews of products and delivery systems to prevent and detect the misuse of technological developments, including those related to electronic storage and transfer of funds or value; and

(5) independent audit arrangements to review and verify compliance with the AML/CFT Act and the effectiveness of measures undertaken to implement the requirements of the Act.



03. Banks

This Part sets out money laundering/terrorist financing risks that banks, in particular, need to be aware of, and take steps to mitigate.

3.1. Lending Activities

Lending activities comprise a major component of a bank's business. These can take many forms: real estate (mortgage) lending, trade finance, cash-secured lending, credit card financing, consumer, commercial, and agricultural lending. Any of these activities can potentially involve some ML/TF risk; some involve greater risk than others.

Lending activities can include multiple parties in addition to the actual borrower. These may include guarantors, signatories, principals, or loan participants. Where multiple parties are involved, certain aspects of the lending process can increase a Reporting Entity's ML/TF risks. Some examples are:

(1) Using certificates of deposits as collateral - A criminal may buy a certificate of deposit and then use it as collateral for a loan. Illicit funds can be used to purchase the certificate of deposit itself, or in the usage of the loan proceeds.

(2) Sudden/unexpected payment on loans - A criminal may suddenly pay down or pay off a large loan, without any indication of refinancing or other reasonable explanation.

(3) Reluctance to provide information about the purpose of the loan, or providing an ambiguous explanation - A customer applying for a loan without disclosing the purpose may be attempting

to disguise the true nature of the loan. Banks should document the purpose of all loans of any significant amount. This is simply a good business practice. Banks should be reasonably sure that their customer can pay their loans back; one way to do this is to know what the customer plans to do with the loan proceeds. It also helps guard against money laundering.

(4) Inconsistent or inappropriate use of loan proceeds - In some cases, a criminal may use loan proceeds or disbursements for purposes other than what he or she told the bank these would be used for. Sometimes loan proceeds are not disbursed all at once; disbursements may be gradual over time. This is especially common in construction lending. The property developer will complete some aspect of a project, then request a disbursement of part of the loan proceeds to cover the costs he has just incurred. Again, it is a good business practice for a bank to know the purpose of each disbursement of loan proceeds, not just the general purpose of the loan when was made.

(5) Overnight loans - These loans create high balances in accounts (e.g., "parking" loan proceeds in a deposit account.)

(6) Loan payments by third parties - Loans repaid by a third party may indicate that the loan collateral really belongs to the third party, who may be attempting to disguise the ownership of illegally obtained money.

(7) Loan proceeds used to purchase property in the name of a third party, or collateral pledged by a third party- Using loan proceeds to purchase property in the name of a third party such as a trustee or shell corporation and pledging it as collateral may suggest that the borrower may be acting as an agent for the third party, who may be attempting to disguise the ownership of illegally obtained money.

(8) Mortgage financing with an unusually short term - Real estate loans are generally longer-term loans simply because of the substantial amounts involved and the fact that borrowers need time to pay them off. Financing a large mortgage on an unusually short term raises suspicions because most ordinary borrowers do not have the financial capacity to repay such loans quickly.

(9) "Structured" down payments or escrow money transactions - Criminals often attempt to disguise the source of illicit funds and avoid reporting requirements by "structuring" down payments or escrow money transactions, i.e., by breaking down the total amount of the down payment into smaller amounts.

(10) Attempts to sever the paper trail - Criminals often attempt to sever or obscure any paper trail connecting a loan with the collateral for that loan to hide the true purpose of the loan.

(11) Wire transfers of loan proceeds - A customer may direct loan proceeds to be wired to a third party for no apparent legitimate reason, or for reasons that do not appear to make commercial or business sense.

(12) Disbursement of loan proceeds by multiple bank checks - Criminals often request disbursement of loan proceeds via multiple bank checks, each below the reporting threshold. The criminal can then negotiate these checks elsewhere for currency. This enables the customer to avoid the currency reporting requirement, and even severing of the paper trail.

(13) Loans to companies outside Bhutan - Unusual loans to customers located in offshore zones, particularly "secrecy havens," are generally considered higher-risk lending activities because it is often difficult to obtain reliable information about those kinds of companies.

(14) Financial inconsistency - A customer lends money to a company whose financial situation, based on submitted financial information such as financial statements, etc., differs significantly from that of companies engaged in similar businesses.

Of course, the above transactions or activities do not always mean that the customer is involved in money laundering or other nefarious activities. However, Reporting Entities need to be aware of the potential for such activities and take steps to assess and mitigate their risks.

3.2. Real Estate Lending

Real estate lending can carry particular money laundering risks, particularly when it involves "high-end" properties. When banks provide financing for the purchase of real property, they can be involved in money laundering schemes if they do not have policies and procedures designed to recognize such schemes. Some of the more common means that criminals use to launder illicit funds through the real estate market include the following:

(1) Early payment of a mortgage - Applying for a mortgage to buy the property, then paying off the mortgage in full after a short time. Taking out a mortgage to purchase property is typical; paying it off soon after obtaining it is not. This is a major red flag for a money laundering activity.

(2) Undervaluation - Recording the property value on a contract of sale that is less than the actual market price. The difference between the contract price of the property and its true worth is paid secretly by the purchaser to the vendor using illicit funds.

(3) Successive selling ("flipping") - The same property is bought and sold many times within a relatively short period; the objective is usually to confuse the audit trail.

(4) "Parking" the property - Buying a property and keeping it for some time, then selling it with a higher value that the market does not support.

(5) Oversees ownership through shell companies - Establishing "shell" companies, especially in a weakly regulated and highly corrupt country, and then using this shell company to own the subject property. This is the method most commonly used by corrupt PEPs, tycoons, and organized crime figures to launder illicit funds.

3.3. Cash-Intensive Businesses[4]

Most cash-intensive businesses are legitimate enterprises. However, some aspects of these businesses may be susceptible to ML/TF. Some examples are (i) convenience stores, (ii) restaurants, (iii) retail stores, and (iv) liquor stores.

Criminals may use these kinds of enterprises to disguise their illicit proceeds. For example, a criminal may own a small convenience store and use it to launder profits obtained through illegal drug transactions or human trafficking. To an outside observer, the owner's currency deposits into the store's bank account might appear quite innocuous because the store is a cash-generating enterprise. However, the volume of currency in a convenience store that is being used as a conduit for money laundering will almost always be considerably higher compared to similar stores in the same vicinity. The nature of these businesses, combined with the difficulty in detecting unusual activity, may require Reporting Entities to treat them as higher risk customers.

When establishing and maintaining relationships with cash-intensive businesses, banks should:

(1) Establish policies, procedures, and processes to identify customer relationships that should be considered higher risk.

(2) Assess AML risks.

(3) Complete CDD (or if necessary, ECDD) during account opening and periodically during the relationship.

(4) Conduct effective monitoring of such relationships to identify unusual or suspicious activities.

At the time of account opening, the bank should have an understanding of:

(1) the customer's business;

(2) the customer's anticipated use of the account;

(3) the expected volume of transactions, products, and services to be undertaken; and

(4) any geographic locations where the customer conducts business.

4 Federal Financial Institutions Examination Council (FFIEC), *Bank Secrecy Act/Anti–Money Laundering Examination Manual* (2014), www.ffiec.gov (accessed May 7, 2018)

When conducting a risk assessment of cash-intensive businesses, banks should concentrate on those accounts that are most likely to pose the greatest risk of ML/TF. Risk factors may include:

(1) the customer's purpose in setting up the account;

(2) the number, frequency, and type of currency transactions undertaken;

(3) the customer's history with the bank (e.g., length of relationship, currency transaction filings, and STR filings);

(4) the customer's main business activity, products, and services;

(5) the structure of the business (sole proprietorship, partnership, etc.);

(6) geographic locations and jurisdictions where the business operates; and

(7) the degree of cooperation that the customer has shown in providing information to the bank.

For customers considered higher risk, bank management may consider implementing supplemental monitoring practices, which could include periodic on-site visits, interviews with the business's management, or closer reviews of transactional activities.

3.4. Purchase and Sale of Monetary Instruments

Banks deal in various monetary instruments such as cashier's checks, traveler's checks, and money orders. Banks can be attractive vehicles for criminals seeking to launder funds because they provide and process these instruments through their deposit products. This occurs particularly at the placement and layering stages. For example, a criminal might purchase cashier's checks in small amounts, and then place them into deposit accounts in amounts less than Nu.500,000 to avoid having to provide proper identification or triggering the reporting requirement.

Banks involved in sale of monetary instruments therefore need to have effective policies, procedures, and processes in place to mitigate these risks. These should include:

(1) criteria for acceptable and unacceptable transactions with such instruments (for example, transactions for noncustomers, instruments with blank payee information, instruments lacking signatures, procedures for detecting structured transactions, or multiple sequentially numbered instruments for the same payee);

(2) procedures for review of unusual or suspicious activity involving such instruments, including procedures to escalate concerns internally to management; and

(3) criteria for closing accounts, or refusing to do business with noncustomers who have consistently or egregiously been involved in suspicious activities.

3.5. Nongovernment Organizations and Charities

Nongovernment organizations (NGOs) are private noncommercial organizations that conduct activities with the goal of serving the public good. These organizations may provide basic social services, work to alleviate suffering, assist the poor, bring citizens' concerns to the attention of public authorities, encourage civic participation, promote environmental protection, or undertake community development. An NGO can be any nonprofit organization that is independent from government.

NGOs comprise large regional, national, or international charities as well as community-based self-help groups. They may include research institutes, religious institutions, professional associations, and lobbying organizations. NGOs typically depend on charitable donations and voluntary service, in whole or in part, to support their activities.

NGOs are susceptible to abuse by money launderers and terrorists because the in-flow and out-flow of funds can be quite complex. To assess and control the risks posed by NGO customers, banks need to conduct adequate due diligence on the organization.

In addition to required Customer Identification Program information, Reporting Entities should focus on

(1) the NGO's stated purpose and objectives;
(2) geographic areas where the NGO maintains its headquarters and/or conducts its activities;
(3) the NGO's organizational structure;
(4) the composition of the NGO's donor and volunteer base;
(5) the sources of funding and criteria for disbursements (including basic beneficiary information);
(6) record-keeping requirements;
(7) the NGO's affiliation with other NGOs, governments, or groups;
(8) the NGO's internal controls and audits.

Higher-risk NGO accounts should be subject to more stringent documentation, verification, and transaction monitoring procedures. Such higher-risk accounts generally include those operating or providing services internationally, conducting unusual or suspicious activities, or lacking proper documentation. Examples of ECDD for these accounts may include

(1) examining the background of the principals,
(2) obtaining and reviewing financial statements and audit reports,
(3) verifying the sources and uses of funds,
(4) examining the backgrounds of large contributors or grantors of the NGO, and
(5) conducting reference checks on the organization.

3.6. Correspondent Banking

Correspondent banking entails providing banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). The correspondent bank acts as an intermediary or agent for the respondent bank, executing or processing payments or other transactions for customers of the respondent bank. These customers may be individuals, companies, or other financial institutions. Beneficiaries of the transactions may be customers of the correspondent bank, the respondent bank itself, or in many cases customers of other banks.

The correspondent bank usually does not have any direct relationship with the actual parties to a transaction. It therefore cannot verify their identities or conduct CDD about them. Correspondent banks also do not normally have detailed information about the nature of the purpose of the underlying transactions, particularly when these transactions involve processing electronic payments (e.g. wire transfers) or clearing checks.

Because of these factors, correspondent banking is considered high-risk from an ML/TF perspective. To effectively handle the risks inherent in these relationships, banks providing correspondent services need to exercise special care. Without such diligence, they find themselves holding and/or transmitting money linked to corruption, fraud, or other criminal activity through the accounts of the respondent banks or being used by shell banks. This is especially true for cross-border correspondent relationships. Banks providing these services should:

(1) thoroughly understand the respondent bank's business and determine from publicly available sources the reputation of the respondent bank and the quality of supervision in its home country, including whether it has been subject to an ML/TF investigation or enforcement action;
(2) assess the respondent bank's AML/CFT controls, considering the AML/CFT regime of the country or jurisdiction where the respondent bank operates;
(3) obtain senior management approval before entering into new correspondent banking relationships; and
(4) clearly understand the respective AML/CFT responsibilities of each institution.

"Payable-through" accounts, in which the respondent bank's customers transact business on their own behalf through direct use of the correspondent bank's accounts, require caution. Correspondent banks should confirm that the respondent bank

(1) has performed any necessary CDD relative to its customers that will have direct access to the accounts of the correspondent bank; and

(2) can provide relevant CDD information to the correspondent bank upon request.

A bank should not establish a correspondent banking relationship with a proposed respondent bank unless it is satisfied that the proposed respondent bank

(1) has procedures like those required by the AML/CFT Act for verifying the identities of customers who will be allowed to use such "payable-through" accounts, and continuously monitoring those customer relationships; and

(2) will provide the correspondent bank with any documents, data, or information that it may request regarding those customers.

A major concern in the AML/CFT area involves "shell banks", banks licensed or incorporated in a jurisdiction where they are not physically present, and are not affiliated with any regulated or supervised financial group. The AML/CFT Act 2018 require banks to:

(1) take necessary measures to ensure that it is not exposed to the threat of ML/FT through the accounts of their respondent bank clients;

(2) not enter into correspondent banking relationships with shell banks; and

(3) satisfy themselves that their respondent bank clients do not permit their accounts to be used by shell banks.

Information about the reputation of a proposed respondent bank, including the quality of bank regulation and supervision in its home country, can often be obtained through publicly available sources, such as the bank's website and annual reports.

Banks considering to provide correspondent services should examine publications of regulatory authorities and reputable international bodies, such as the FATF, to evaluate the degree of risk posed by the jurisdiction where the potential correspondent banking client is based, the jurisdiction where its ultimate parent (if any) is headquartered, and jurisdictions where they conduct business.

Banks need to exercise caution when maintaining correspondent relationships with respondent banks licensed or operating in jurisdictions known to have substandard AML/CFT regimes. ECDD in such cases should include obtaining details of the beneficial ownership of such banks and more extensive information about their AML/CFT policies and procedures. Correspondent banks should also apply enhanced procedures for ongoing monitoring of any activities conducted through such correspondent accounts, such as developing procedures for review of transaction reports by the compliance officer and close monitoring of suspicious fund transfers.

It is a good business practice for a representative of the Reporting Entity to visit the correspondent banking client at its premises, either before or within a reasonable time after establishing a relationship with a correspondent banking client. Such visits can (i) confirm the information provided to the correspondent bank by the respondent bank, and (ii) generally support the CDD process. These visits may also be conducted at the time of periodic reviews, if deemed necessary.

The quality of the banking supervision and regulation regime of the jurisdiction where the potential respondent bank is licensed or has its principal place of business should be seriously considered in determining whether to establish a correspondent banking relationship. The rationale for this is simple: the higher the quality of a country's financial supervisory regime, the less likely it is to have ML/TF problems.

For this purpose, the bank should obtain, if possible, the most recent Basel Core Principles assessment of the respondent bank's home country performed by a third-party evaluator such as the World Bank and/or the International Monetary Fund (IMF). Such assessments can sometimes be found at the World Bank or IMF websites. This should not be limited to just consistency with the Basel capital standards but a full assessment of compliance with the Core Principles. The bank should not establish the relationship if, in its judgment, the assessment shows significant weaknesses or deficiencies, particularly regarding AML/CFT.

If such a third-party assessment is not available or if the respondent bank's home country supervisory authority has not made any assessment publicly available, a self-assessment can be used. These assessments can sometimes be found at central bank or financial supervisory authority websites. However, the bank will need to review such self-assessments with a certain "healthy skepticism" as the supervisory authority may present an overly optimistic view of its capabilities.

If no such assessment can be found or is considered unreliable, the bank should use its best efforts to conduct its own "mini-assessment" of the home country's supervisory regime based on publicly available sources. The banking law and regulations should definitely be considered, focusing particularly on compliance with AML/CFT principles. Good sources of information for these purposes include World Bank and IMF country reports, which are often undertaken in connection with financial sector assessment programs (FSAPs) and can usually be found at these organizations' websites. While not full Core Principles assessments, such FSAP reports typically contain useful information about the quality of financial supervision in the subject country.

Banks should ensure the information about their correspondent banking clients remains current and relevant. Periodic reviews should include information about significant events, such as significant changes in the risk profile of the respondent bank or a sudden and/or significant change in transaction activity (by value or volume in the respondent bank account).

If a respondent bank does not provide the required CDD information or where its AML/CFT controls are determined to be inadequate or ineffective during a review, the correspondent bank should take all reasonable measures to rectify the situation by mitigating its own ML/TF risk. These may include performing additional due diligence measures or adjusting its risk assessment. If the issues are not resolved to the satisfaction of the correspondent bank within a reasonable time, it should seriously consider terminating the correspondent relationship.

Banks entering into correspondent relationships must clearly agree with the respondent bank as to which institution will perform the required measures.

3.7. Trade Finance

3.7.1. Overview

Banks participate in international trade financing in several ways. They may provide pre-export financing; assist in the collection process; confirm and issue letters of credit, discount drafts, and acceptances; and perform fee-based services such as providing credit and country information about purchasers.

Trade finance normally entails providing short-term financing for the import or export of goods. These operations can involve payment if documentary requirements are met (for example, in the case of letters of credit) or in the event of default on a commercial transaction by the original obligor (such as via guarantees or standby letters of credit). In both cases, the bank's services minimize payment risk to the importer or exporter.

Trade financing arrangements tend to be short-term and self-liquidating, but medium-term (1 to 5 years) or long-term (more than 5 years) arrangements may also be used to facilitate import or export of capital goods, such as machinery and equipment.

Trade finance activity requires multiparty involvement on both sides of a transaction. Exporters and importers are often involved in other relationships beyond their basic business relationship with each other. The exporter will have dealings with its suppliers, and the importer will engage in transactions with its customers. Both the exporter and importer are also likely to have other banking relationships. Many other intermediary institutions, both financial and

nonfinancial, may provide channels or services to facilitate the underlying documents and payment flows associated with international transactions. Participants in trade finance transaction include the following:[5]

- Applicant - The buyer or party who requests their bank to issue a letter of credit. Typically, a buyer or importer of goods or services
- Issuing bank - The bank that issues the letter of credit at the request of the applicant and advises it to the beneficiary, either directly or through an advising bank. The applicant is the issuing bank's customer.
- Confirming bank - The bank that acts at the request of the issuing bank to add its commitment to honor draws made by the beneficiary, provided the terms and conditions of the letter of credit are met. Typically located in the home country of the beneficiary.
- Advising bank – A correspondent bank or a noncustomer bank of the issuing bank that advises the credit at the request of an issuing bank. The issuing bank will send the original credit to the advising bank, which in turn will forward it to the beneficiary. The advising bank will authenticate the credit and advise it to the beneficiary. There can be multiple advising banks involved in a letter of credit transaction. The advising bank might also be a confirming bank, typically located in the home country of the beneficiary.
- Beneficiary - The seller or party to whom the letter of credit is addressed. Typically, this is the exporter or seller of the goods or services.
- Negotiation - The process of a nominated bank buying drafts that are drawn from a different bank. The purchase by the nominated bank of drafts (drawn on a bank other than the nominated bank) or documents under a complying presentation, by advancing or agreeing to advance funds to the beneficiary on or before the banking day on which reimbursement is due to the nominated bank.
- Nominated bank - A bank with which a credit is available (which can be any bank in the case of a credit).
- Accepting bank - A bank that accepts a draft, if the draft is considered under the terms of the credit. Drafts are drawn on an accepting bank which dates and signs the instrument.
- Discounting bank - A bank that discounts a draft for a beneficiary after that draft has been accepted by an accepting bank. The discounting bank and the accepting bank are often the same bank.
- Reimbursing bank - A bank authorized by an issuing bank to reimburse a paying bank that submits a claim according to the terms of a letter of credit.
- Paying bank - A bank paying a beneficiary according to the terms of a letter of credit.

3.7.2. Potential money laundering risks in international trade

There are two main reasons the international trade system is vulnerable to ML/TF:

(1) Multiple party involvement on both sides of a transaction makes the due diligence process more challenging.

(2) Trade finance tends to be more document-based than other banking services. This increases its susceptibility to documentary fraud. In addition to money laundering and terrorist financing, this can result in the circumvention of sanctions or other restrictions (such as export prohibitions, licensing requirements, or controls).

The most obvious risks involve particularly dangerous goods, such as weapons or nuclear equipment, and banks need to be alert of transactions involving these goods. But they also need to be aware of transactions involving other less conspicuous goods.

5 Wolfsberg Group, International Chamber of Commerce, and Bankers Association for Finance and Trade, *Trade Finance Principles 2017* (2017), https://iccwbo.org; FFIEC (2014).

In general, criminals can attempt to misuse the international trade system in three main ways:

(1) moving illicit money through the financial system;

(2) physically moving currency (for example, through cash couriers); and

(3) physically moving goods.

The following are more specific examples of some of the many ways by which money laundering can take place in the international trade process:[6]

(1) Exclusive relationships - A high-volume exporter might deal and trade with only one importer, often by trading goods in different categories, typically with high values. From an ML/TF standpoint, both the importer and exporter are considered suspicious and should be subjects of ECDD.

(2) Over- and under-invoicing - Criminals will often move money out of a country by buying high-end merchandise with their illicit funds, then exporting the goods to a collaborating partner in another country, who will then sell these at their actual value in the open market. To create the appearance of legitimacy, the criminals might use a financial institution, such as a bank, for trade financing, which often entails letters of credit and other documents. This is a very old technique but criminals still use it. The key factor is falsification of the price of the goods or services to transfer additional value between the cooperating importer and exporter.

    To illustrate, imagine that a criminal in Bhutan wants to launder profits from illegal narcotics sales. He finds an agreeable partner in India, purchases 10 genuine high-end watches in Bhutan in cash for their actual market price of US$10,000 each, then exports them to his collaborator in India for US$3,000 each. The Indian collaborator then sells each watch at its actual market price to legitimize these funds, reimburses the Bhutan criminal, and might take a small cut for his services.

(3) Multiple invoicing for the same goods - Detection of this can be difficult because there are several legitimate explanations for such situations. For example, payment terms may be amended, previous payment instructions may be corrected, or late fees may be charged. In addition, the exporter or importer does not need to misrepresent the price of the goods or services on the commercial invoice.

(4) Over- and under-shipments - A criminal can misrepresent the quantity of merchandise being shipped or services being provided. In extreme cases, the criminal might not ship any goods at all (a "phantom shipment"). In such cases, the exporter will simply agree with a willing importer to ensure that any documents involved in this transaction are routinely processed through the banking system. Banks may unknowingly be involved in financing these misrepresented or phantom shipments.

(5) Falsely described goods or services - This involves misrepresenting the quality or type of merchandise or services described on an invoice. For example, a criminal might ship cheap merchandise but create an invoice that describes much more expensive items or, in extreme cases, different merchandise altogether. As a result, what is shipped bears little or no resemblance to what is shown on the shipping and customs documents. This technique is not limited to transactions in goods. It can also be used to create the impression that a criminal is charging fees for services (financial advice, consulting services, or market research) when no such services were provided. Because the fair market value of these kinds of services is difficult to determine with precision, this can present valuation challenges.

(6) Exceeding expected activity - In this case, a bank might have a profile of an exporter, with information on the monetary amounts and volume of goods exported monthly to certain jurisdictions. Actual transactions that exceed these expected amounts should be considered unusual and, depending on the circumstances, potentially suspicious. For example, suppose an enterprise that specializes in home furniture consistently exports goods valued at about US$50,000 to locations in East Asia each month. If the same business suddenly begins to export luxury automobiles (an entirely new line of business) valued at US$500,000 each month to places in the Middle East that have been identified as terrorist enclaves, this should be considered highly suspicious and requires further investigation.

6 FATF, *Trade-Based Money Laundering* (2006), www.fatf-gafi.org (accessed May 7, 2018); ACAMS, How Can Trade Finance Anti-Money Laundering Monitoring Be Improved? (2014), https://www.acamstoday.org (accessed May 7, 2018).

(7) "Cash for trash" - A criminal may use the proceeds of an illegal activity to pay a large sum of money for merchandise that is virtually worthless and eventually simply abandoned or discarded. The goods are purchased from the importer's "partner in crime" (the exporter), who then reimburses the importer.

(8) False documents - A criminal may fraudulently alter trade documents, such as invoices, to disguise an illegal operation. The specific means of doing this may vary. Common techniques include inaccurate or double invoicing, shipping only some of the merchandise described in the documents (short shipping), and shipping "phony" merchandise. The illegal proceeds used in transactions of this sort can thus appear to be "sanitized" and subsequently are introduced into the regular stream of legitimate commerce.

To complicate the scheme further, the applicant's true identity or ownership may be disguised through certain corporate forms, such as shell companies or offshore front companies. This creates a lack of transparency and effectively hides the identity of the actual purchaser, thus increasing the ML/TF risks.

3.7.3. Risk mitigation

Banks involved in the international trade process need to undertake varying degrees of CDD depending on their role in the transaction.

Issuing banks, for example, should conduct effective CDD before issuing a letter of credit. They should collect pertinent information about the applicants and the beneficiaries, such as their identities, the type of business they conduct, and sources of funding. The banks may need to undertake more extensive background checks or investigations, particularly for customer relationships that will entail transactions with counterparties located in higher-risk jurisdictions.

In addition, these banks should have a solid understanding of trade finance documentation. The bank's policies, procedures, and processes should require a thorough review of all applicable documentation (such as customs declarations, trade documents, and invoices) to ensure that they can monitor unusual and suspicious activity, and file STRs when necessary.

The monitoring process should particularly note the following:

(1) imports or exports of merchandise that do not match the customer's normal business patterns (see the example above regarding exceeding expected activity);

(2) customers importing merchandise from, or sending merchandise to, higher-risk jurisdictions;

(3) customers shipping merchandise through higher-risk jurisdictions, including transit through countries identified as having deficient AML/CFT regimes;

(4) transactions involving higher-risk or restricted goods or activities (for example, hardware to be used by foreign governments for military or law enforcement purposes, weapons and related ammunition, chemical mixtures, nuclear materials, precious stones or metals, or other natural resources such as metals, ore, or crude oil);

(5) goods or services that are obviously over- or underpriced;

(6) obvious misrepresentation of quantity or type of merchandise involved in a transaction;

(7) unusually complex transaction structures that appear to be designed to obscure the true nature of the transaction;

(8) payment proceeds that are directed to unrelated third parties with no reasonable commercial or business explanation;

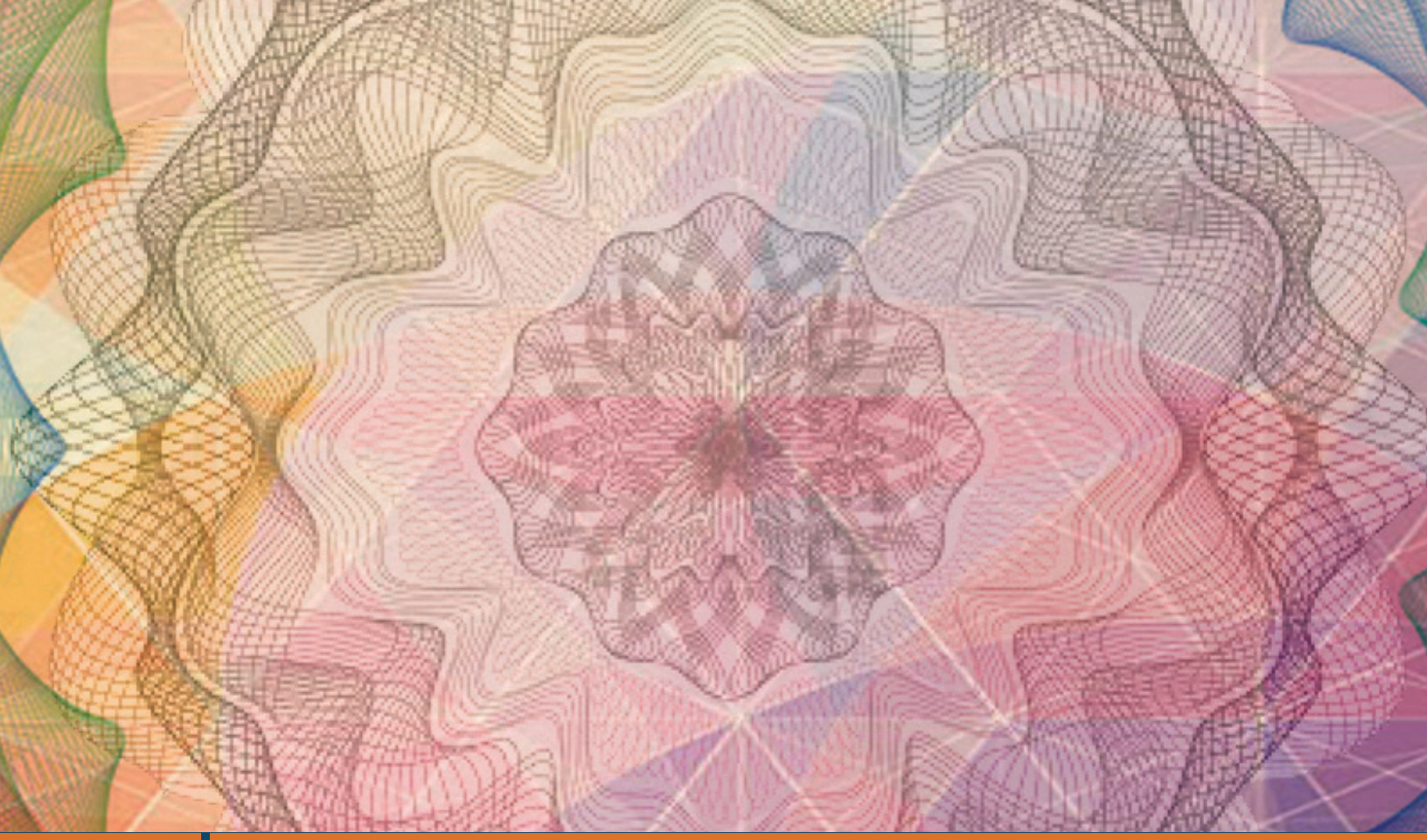
(9) shipment locations or descriptions of merchandise that are inconsistent with the letter of credit;

(10) significant changes in the terms of letters of credit or changes to the beneficiary or location of payment without any reasonable commercial or business explanation. Any changes in the names of parties also should prompt additional review.

When possible, a bank's review should focus not only on compliance with the terms of the letter of credit but also on any red flags or unusual circumstances that could arouse suspicion of criminal or fraudulent activity. Reliable documentation is a key element in this process. It is therefore a good business practice to compare the submitted documents to official government import and export forms.

It is not necessary for banks to investigate the underlying transaction in detail, unless the circumstances are clearly unusual. The "red flag" examples noted above, particularly for an issuing bank, can be included as part of the bank's routine CDD process. Banks with rigorous CDD processes may find that this is sufficient for CDD purposes and that they need to focus less on individual transactions due to their comprehensive knowledge of their customer's activities. Banks taking other roles in the letter of credit process should complete CDD that reflects their role in each transaction.

Where the bank determines that an STR should be filed, it does not necessarily need to discontinue processing the transaction or insist that it be stopped, unless directed to do so by the department. However, the department should be notified.



04. Nonbank Institutions

4.1. Money Transfer and Currency Exchange Businesses

4.1.1. Overview

Per the AML/CFT Act, financial institutions are considered "Reporting Entities" and are thus subject to the Act. These include, among others, the following business enterprises:

(1) money or value transfer services,

(2) trading in foreign exchange,

(3) money and currency trading, and

(4) engaging in funds transfer as a business.

Any enterprise that transfers money as part of its normal operations is in the "remittance" business. Banks typically provide these services. Remittance services may also be conducted by certain nonbank institutions. Independent remittance dealers, however, specialize in these services, providing them to customers directly through their own systems and processes. These kinds of transfers are normally conducted through the business's bank accounts rather than through the provider's own system.

While many of the points that apply to banks will also be applicable to the remittance business, independent remittance dealers face additional challenges. This is mainly because of the nature of the business, which often

entails carrying out one-off transactions with occasional customers, where the customer relationships are not ongoing. Thus, it is thus not possible for a remittance firm to conduct ongoing monitoring of the customer relationship in the same sense that a bank can with its customers, who often maintain deposit or current account relationships with the banks. Typically, remittance providers are only aware of the name of the customer, the beneficiary (sender or receiver), and the destination or origin of the funds being sent or received. An additional problem for currency exchange services is that once the money has been exchanged, it is difficult to trace its origin.[7]

A major component of CDD is unusual customer behavior. Several indicators raise concerns about possible ML/TF activities. While these indicators are also applicable to banks, they are especially pertinent to remittance business.

4.1.2. Unusual customer behavior–sending transactions:

(1) Structuring a transaction by breaking up the total sum to be sent into smaller amounts in an apparent attempt to avoid the Nu.500,000 reporting threshold;

(2) A transaction that is unnecessarily complex for no apparent business or lawful reason;

(3) The volume or monetary value of transactions that is not in accord - with the customer's financial standing or occupation, or with the customer's normal course of business;

(4) Offering a bribe, or a tip where a tip is not customary, or willingness to pay fees that are unusual or higher than normal to have a transaction carried out;

(5) A customer has vague knowledge of the purpose of the remittance or the amount of money involved;

(6) Unusual inquiries, threats or attempts to convince the firm's employees not to report a transaction when such reporting is required;

(7) Sending money internationally and then receiving, or expecting to receive, an equal incoming transfer or vice versa;

(8) Sending money to illegal online gambling sites (often indicated by e-mail addresses containing gambling references) or to jurisdictions that have many internet gambling sites;

(9) Sending money to higher-risk jurisdictions or locations;

(10) Requesting a transaction, but canceling the request after becoming aware that ECDD procedures or reporting to the DFI would be necessary;

(11) Indicators of potential consumer fraud:

  (a) transferring money to claim lottery or prize winnings or to someone the customer has met only online;

  (b) transferring money as credit card payment or loan fee or in connection with an employment offer or a mystery shopping opportunity;

(12) The sender appears to have no family or business relationship with the receiver and has no reasonable explanation for the transfer.

4.1.3. Unusual customer behavior–receiving

(1) Transaction documents that do not indicate required information about the originator or beneficiary;

(2) Additional customer or transactional information is requested from the sending firm, but is not received;

(3) A large number of transfers received at the same time, or over a certain period (for example, during illicit drug production seasons), or which do not seem to match the recipient's typical past pattern.

7 FATF and Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)(n.d.), https://www.coe.int (accessed May 7, 2018).

4.2. Insurance Companies

4.2.1. Potential money laundering through insurance companies

Insurers offer highly flexible investment-type products that allow potential clients to dispose of large amounts of money with relative ease and then recover that money whenever they choose to do so, even if it means taking a relatively small loss.

Potential client behavior or transactions that may indicate possible criminal activity include:

(1) "Single premium" policies - These policies, which enable criminals to dispose of substantial amounts of money all at once, are generally considered to entail the greatest potential money laundering risk;

(2) Annuity policies - The money launderer pays the premium(s) by using criminally derived funds, and then starts receiving income that appears to be legitimate;

(3) Purchasing a high regular premium savings policy (or a series of small regular premiums to avoid attracting attention);

(4) Requesting a refund of premiums during the "cooling off" period, or deliberately overpaying premiums. This helps the criminal to disguise the illicit source of the funds because he will be receiving money from a legitimate source (the insurer). It is important in these circumstances that insurers reimburse clients by directly paying into their bank accounts;

(5) Surrenders/redemptions/withdrawals:

  (a) The criminal surrenders his policy and gets a refund of his money. Because of the substantial amount of illicit money, the criminal is willing to take a small loss (the surrender penalty);

  (b) Alternatively, the criminal may gradually surrender part of a policy to dispose of the investment in "phases" so as not to attract attention;

  (c) In either case, the perpetrator receives a check from an insurer that can be used again to buy further investments (the layering/integration phases). Anyone will unlikely question the source of funds at that point because by that time, the perpetrator will be paying with funds from an insurer.

(6) "Top-ups" - The criminal pays a small initial premium (to avoid attracting attention) and then makes further payments ("top-ups"), which might be relatively large, or a series of small top-ups. This scheme will almost always work if the insurer does not repeat the CDD measures (including establishing the source of funds) at the time of the top-up.

(7) Policy loans - The criminal purchases a policy involving a single premium and subsequently takes out a loan secured by the policy. The amount of the policy loan is a percentage of the policy's surrender value. If, as is often the case, the client does not repay the loan, any loan amounts that are still outstanding are simply deducted from any future claim (which may occur at the time of death or maturity);

(8) Transferring ownership/designating beneficiary - This technique involves collusion between a purchaser of an insurance policy and a criminal. After purchasing the policy with illicit funds and designating the beneficiary, the client transfers ownership of the policy, or changes the beneficiary to a (supposedly) unconnected third party (the criminal who is seeking to launder the illicit funds). A diligent insurer will undertake CDD on the new beneficiary or owner of the policy.

(9) Using single premium policies as collateral for bank loans - This is like the policy loan described above. The difference is that in this case, the loan is obtained from a bank rather than directly from the insurance company. Shortly after receiving the loan, the criminal will surrender the policy and use the proceeds to repay the bank.

4.2.2. Customer Due Diligence for beneficiaries of life insurance policies

CDD should be undertaken not only on the customer and the beneficial owner but also on the beneficiary as soon as this person is identified or designated. CDD measures should include[8]

(1) the name of the person, in the case of a specifically named person (natural or legal) or legal arrangement;

(2) information about the beneficiary—if he or she is designated by certain characteristics, class, or in some other manner—that will enable the reporting entity to identify the beneficiary at the time of payout.

In both the above cases, verification should take place at the time of payout. Reporting entities should consider the beneficiary of a life insurance policy to be one of the relevant risk factors in determining whether ECDD measures should be undertaken.

If an insurer determines that a legal person or legal arrangement beneficiary presents a higher risk, it should conduct ECDD, which should include identifying and verifying the identity of the beneficial owner of the beneficiary, at the time of payout.

4.3. Securities Professionals

Under the AML/CFT Act, the RMA supervises securities brokers, investment advisors, investment fund operators, and securities depositories/registries.

The majority of securities are related to legitimate publicly traded or closely held companies and pose limited financial crime risk. However, in addition to understanding and controlling the risk from clients and third parties, securities professionals should also pay close attention to the risk posed by securities that are poorly regulated or may have been created for illicit purposes.

4.3.1. Securities brokers

Under Section 285 of the Financial Services Act 2011, a person in the business of effecting transactions in securities for the account of others or in the business of dealing in securities for his own account (but not simply an investor) is considered a securities broker.

Some examples of potentially high-risk products, services, and delivery channels involved in the securities brokerage business include

(1) non-face-to-face transactions or accounts that are opened online, especially when these differ from the broker's normal business practices. The greater client anonymity involved in these transactions and accounts can pose a higher risk;

(2) high-value transactions, particularly when third-party involvement is suspected;

(3) offering the capability for electronic transfer of securities. The ease of transfer, the potential lack of transparency, and the ability to transfer across borders all combine to create a higher money laundering risk.

4.3.2. Investment advisors[9]

Investment advisors provide advisory services to a variety of customers. These clients may include individuals, institutions, pension plans, companies, trusts, foundations, mutual funds, private funds, and other pooled investment vehicles. They assist their clients in managing their investment portfolios, financial planning, and consulting on pension-

8 FATF, *Risk-Based Approach - Guidance for the Life Insurance Sector* (2009), www.fatf-gafi.org (accessed May 7, 2018).

9 US Department of the Treasury, Financial Crimes Enforcement Network (FINCEN), Anti–Money Laundering Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers (Proposed Rule, September 1, 2015) (2015), https://www.fincen.gov (accessed May 7, 2018).

related questions. Investment advisors often work closely with their clients in formulating clients' investment decisions and strategies, and designing the most effective means of implementing them. These advisors may be large or small enterprises and may be organized as corporations, limited liability companies, partnerships, or sole proprietorships.

Money launderers often consider investment advisors to be a low-risk means of gaining access to the financial system. Financial institutions such as banks and brokers have certain CDD obligations under the AML/CFT Act when executing orders to purchase or sell client securities, or when directing custodial banks to transfer assets. But these brokers or banks do not always have sufficient information about the underlying clients to assess suspicious activity or money laundering risk. For example, when an investment advisor places an order with a broker to execute a trade on behalf of the advisor's client, the broker may not know who the advisor's client is. Similarly, when a custodial bank holds assets for a private fund managed by an advisor, the custodial bank usually will not know the identities of the underlying investors in the fund. Such knowledge gaps could enable money launderers to evade detection by operating through investment advisors rather than directly through securities brokers or banks.

Investment advisors often have considerable insights about their clients' transmission of funds through the financial system. If a client is involved in unlawful activities and the client's funds represent the fruits of those activities or are being used to carry them out, an investment advisor's AML/CFT program and STR reporting can be extremely valuable tools.

Wealth management typically involves providing financial services to high net worth clients in a managed relationship. The value and complexity of products offered to these clients, together with the international character of the business, make wealth management services particularly attractive to criminals seeking to launder illicit funds.

4.3.3. Securities depositories

A securities depository is a business where securities certificates are stored until they are ready to be transferred later to their holder or to a third party.

A securities depository or custodian performs various services, such as securities safekeeping, processing and executing securities settlement instructions, settling trades cleared by a central counterparty and the related management of margins, processing payment obligations stemming from clearing and settlement, funds distribution, and related asset services. These services may be performed for a customer's own account and/or for the account of the customer's clients, who may be individuals, legal entities, or even other financial institutions, and may represent a broad range of beneficial owners.

4.4. Money Laundering Risks in the Securities Sector

Securities-related money laundering schemes typically involve a series of transactions that are not consistent with the investor's profile. Often the investor appears to be unconcerned with getting a good return on his or her investment.

The following provides more specific information about some activities of which securities professionals need to be particularly aware.

4.4.1. Client Due Diligence/Know Your Client

(1) The client is willing to pay higher fees to keep some of his or her information secret.

(2) The client acts through intermediaries, such as money managers or advisers, and lawyers or accountants, to avoid having his or her identity disclosed.

(3) The client (whether a natural person or legal entity) fails or is reluctant to provide sufficient information about their business activities, existing or previous financial relationships, the expected activity for the account being established, the entity's managers, directors, controlling shareholders, or beneficial owners, business location, or jurisdictions in which it or its own customers conduct business.

(4) The client insists on undertaking investments that are inconsistent with his or her profile, even after the firm's professional staff recommends investments that are better suited to the client's situation.

(5) The client cannot provide information about the source of funds to be used for a transaction or to establish a business relationship; refuses to provide such information; or provides information that turns out to be false, misleading, or substantially incorrect.

(6) The client is reluctant to meet the firm's staff members face-to-face, appears secretive or evasive or nervous during discussions with the firm's staff, or becomes defensive about furnishing information required for the firm's CDD procedures.

(7) The client is a PEP.

4.4.2. Location

(1) The person or entity is in a jurisdiction that has been identified by credible sources as a bank secrecy haven, tax shelter, or high-risk geographic location.

(2) A client who is not a local resident or is outside of the securities firm's normal customer area.

(3) A client opens or maintains multiple accounts in many different jurisdictions.

(4) A foreign-based client uses domestic accounts to trade on foreign securities exchanges through foreign affiliates, each with different AML/CFT controls and identification practices.

4.4.3. Client profile

(1) The client has a history of changing financial advisors or using multiple securities firms or banks for identical or similar services.

(2) The client does not use the account for its intended purpose, changes transaction patterns suddenly in a manner that is inconsistent with their normal activities (for example, making extremely complex transactions or depositing securities in amounts that do not fit the customer's past patterns or profile).

(3) A legal entity customer has no apparent business activity, sales, revenues, or products, creating the suspicion that it may be a shell company being used for securities purposes.

(4) The client is an individual who has a known history of predicate offenses, such as insider trading, market manipulation, or securities fraud.

(5) The value of the securities deposited into the client's account is inconsistent with the client's profile.

(6) The client appears to be unusually concerned with the firm's compliance with RMA/DFI reporting requirements or the firm's AML/CFT policies and procedures.

(7) The firm is aware or becomes aware from a reliable source (which might include media or other publicly available sources) that a client is suspected of being involved in illegal activity.

4.4.4. Patterns

(1) The client's address is connected to multiple but apparently unrelated accounts.

(2) A client's trading patterns suggest that he or she may have inside information (for example, purchasing or selling a large volume of a particular security shortly before a public announcement that affects the security's price, having friends or family who are major shareholders, or working for the company issuing the security).

(3) The client receives many incoming remittances from unrelated third parties when their profile does not suggest a legitimate business reason for receiving such third-party payments.

(4) The client sends many payments to third parties shortly before or after receiving multiple third-party payments.

4.4.5. Transactions

(1) Securities or funds transfers between apparently unrelated parties, especially when the name or account number of the beneficiary or remitter has not been supplied.

(2) Physical securities titles do not match the name on the customer's account.

(3) Transfers of funds to financial institutions or banks other than those that have been previously identified, particularly when they are located outside Bhutan.

(4) A securities account used for sending or receiving payments or wire transfers, even though little or no actual securities activity is associated with the account.

(5) A client cashes bearer securities without first depositing them, or withdraws funds that have been in an account for only a very short time.

(6) A client deposits bearer securities and requests that the shares be placed in multiple but apparently unrelated accounts, or that they be sold, or their ownership otherwise transferred shortly thereafter.

(7) A client buys securities at a high price and then sells those to a third party at a considerable loss. This may suggest transferring value from one party to another or manipulating the market.

(8) "Pump and dump" schemes - artificially inflating the price of inexpensive securities through false and misleading positive statements, with the purpose of selling the securities at a higher price.

(9) A dormant account suddenly becomes active without a plausible explanation (for example, substantial cash deposits that are quickly wired out).

(10) Transactions that suggest that a client may be acting on behalf of an undisclosed third party, or transactions involving an unknown counterparty;

(11) A client purchases an investment product but seems unconcerned with investment performance or objectives, or about higher-than-normal transaction costs.

(12) A client provides an explanation about the acquisition of physical securities that does not make sense, or the explanation changes, particularly when depositing a large number of physical securities.

(13) A client with a significant history with a securities firm suddenly liquidates all his or her securities portfolio with no apparent concern about fees or penalties in order to remove assets from Bhutan.

Bibliography

ACAMS, How Can Trade Finance Anti-Money Laundering Monitoring be Improved? (2014), https://www.acamstoday.org (accessed May 7, 2018).

Federal Financial Institutions Examination Council (FFIEC), Bank Secrecy Act/Anti-Money Laundering Examination Manual (2014), www.ffiec.gov (accessed May 7, 2018).

Financial Action Task Force (FATF), FATF Recommendation 2012 (2012), www.fatf-gafi.org (accessed May 7, 2018).

Financial Action Task Force (FATF), Risk-Based Approach - Guidance for the Life Insurance Sector (2009), www.fatf-gafi.org (accessed May 7, 2018).

Financial Action Task Force (FATF), Trade-Based Money Laundering (2006), www.fatf-gafi.org (accessed May 7, 2018).

Financial Action Task Force (FATF) and Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) (n.d.), https://www.coe.int (accessed May 7, 2018).

Royal Monetary Authority of Bhutan, The Anti–Money Laundering and Countering of Financing of Terrorism Act of Bhutan 2018, www.rma.org.bt (accessed May 7, 2018).

US Department of the Treasury, Financial Crimes Enforcement Network (FINCEN), Anti–Money Laundering Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers (Proposed Rule, September 1, 2015) (2015), https://www.fincen.gov (accessed May 7, 2018).

Wolfsberg Group, International Chamber of Commerce, and Bankers Association for Finance and Trade, Trade Finance Principles 2017, https://iccwbo.org (accessed May 7, 2018).

Appendix

BENEFICIAL OWNER DECLARATION FORM

To: [Name of Designated Institution Official]

Dear Sir/Madam:

DECLARATION OF BENEFICIAL OWNERSHIP

Details of Company

License No.:

Company Name:

Country of Incorporation:

*Please tick whichever applicable:

☐ I/We declare that the beneficial owners, as described more fully on Page 2 of this form (i.e., individual(s) who ultimately own(s) or effectively control(s) the company (regardless of shareholding), and the percentage shares held by each such beneficial owner of the Company are as follows:

Details of Beneficial Ownership

Name:

CID /:

Passport No.:

Date of Birth:

Nationality:

% shares:

☐ I/We declare the Company is ultimately owned by the following entity:

Name:

Registration Number:

Date of Incorporation:

Country of Incorporation % shares:

I/we undertake to keep [name of institution] informed should there be any change to such beneficial ownership in the future.

_____

Signature above printed name

_____

Date

(To be signed by all beneficial owners OR 2 directors OR 1 director and 1 corporate secretary)

The AML/CFT Act defines a beneficial owner as

(1) a natural person who ultimately owns or controls the rights to or benefits from property, including the person on whose behalf a transaction is conducted; or

(2) a person who exercises ultimate effective control over a legal person or a legal arrangement.

Per the AML/CFT Act, a natural person is deemed to ultimately own or control rights to or benefit from property within the meaning of the above definition when that person

(1) owns or controls, directly or indirectly, whether through trusts or bearer shareholdings for any legal entity 25% or more of the shares or voting rights of the entity; or

(2) otherwise exercises control over the management of the entity.

(3) A natural person is considered to exercise "effective control" of a legal entity customer if that person canelect a majority of the board of directors, supervisory board, or any equivalent body, of a legal entity; or

(4) exert a "dominant influence" over the financial, economic, or management policies of the entity, regardless of the amount, if any, of share ownership or voting rights in that entity. This is the case, for example, if a majority of the members of the entity's board of directors, supervisory board, or any equivalent body are used to or obliged to act in accordance with that person's directions, instructions, or wishes in conducting the affairs of the entity. Such an obligation may be formal or informal, written or unwritten.

If no such natural person fits the above description, the beneficial owner is the [chief executive officer] or other person or persons performing similar functions, who effectively directs the business of the entity on a day-to-day basis.

Property, or an interest in property, may be subject to the effective control of a person within the meaning of the AML/CFT Act whether the person has

(1) a legal or equitable estate or interest in the property; or

(2) a right, power, or privilege in connection with the property.

Regard may be had to

(1) shareholdings in, debentures over, or directorships of any company that has a direct or indirect interest in the property;

(2) a trust that has a relationship to the property; and

(3) family, domestic, and business relationships between any person having an interest in the property, or in companies or trusts described above.

Guide on Customer Due Diligence

Royal Monetary Authority of Bhutan Financial Intelligence Department

This Guide is a response, among others, of Bhutan's Royal Monetary Authority and the Financial Intelligence Department to fight widespread money laundering and terrorist financing activities worldwide. Curbing such illegal activities requires proactive and adequate due diligence by financial institutions to know with whom they are dealing with as clients. This Guide provides clear standards and processes on how to conduct due diligence at each stage of a business relationship with a client. It helps financial institutions determine when transactions are potentially suspicious, and what action is needed to avert such transactions. Ultimately, it aims to further promote and maintain the financial stability, soundness, and reputation of the finance sector in Bhutan, and help fight these illegal activities.

About the **Royal Monetary Authority of Bhutan**

The primary objective of the Authority is to formulate and implement monetary policy with a view to achieving and maintaining price stability. The RMA conducts monetary policy in the context of peg arrangement with Indian Rupee. The one-to-one exchange rate peg arrangement has served as a nominal anchor for achieving and maintaining price stability. The RMA's monetary policy operation is pursued through (i) cash reserve ratio and interest rate policy to influence credit and monetary aggregates (ii) implementation of micro and macro prudential regulations and (ii) prudent management of international reserves to support the peg.

Royal Monetary Authority of Bhutan
Post box no. 154, Chhophel Lam
Thimphu, Bhutan
www.rma.org.bt/index.jsp