



## **AMLO Guideline on Customer Due Diligence**

**For Banks**

**Supervision and Examination Division**

**The Anti-Money Laundering Office**

## Contents

Organizational Internal Policy.....	1
Arrangement for Customer Identification .....	7
Approval for Customer Acceptance.....	15
Money Laundering and Financing of Terrorism Risks Management .....	24
Customer Due Diligence (CDD) .....	40
Enhanced Customer Due Diligence (CDD) for High-Risk Customers.....	47
Simplified Customer Due Diligence (CDD) for Low-Risk Customers .....	54
Reporting of Suspicious Transactions .....	58
Transmission of Information Accompanying Wire Transfers .....	61
Record Keeping .....	66
Foreign Branches and Subsidiaries .....	67
Correspondent Banking Relationship and Reliance on Third Party.....	70
Summary of Guideline In Compliance with the Law on Anti-Money Laundering (AML) and the Law on Counter Terrorism Financing (CTF) .....	76

## **Organizational Internal Policy**

Relevant to Anti-money Laundering and Combating the Financing of Terrorism (AML/CFT)

Under the provisions of the Ministerial Regulation Re: Customer due diligence, 2013, in combination with the essentials in international standard on Anti-money Laundering and Combating the Financing of Terrorism (AML/CFT), the reporting entity is required to set out policy expressing the acceptance of measure on AML/CFT as the organization's main policy which is equally important as the main policy in the business operation.

The said policy consists of the main policy and secondary policy whereas the difference of both policies is as follows:

Main policy must be the policy issued by the top executive board of the organization having the authority to steer the direction of organizational administration of the reporting entity and is equally important as the policy set out for the success of the operation.

Secondary policy may be named otherwise other than the policy, for example, measure, organizational regulation, organizational notification, internal guideline which may be issued by the top executive board or the executive board having the authority to issue the said secondary policy. However, the secondary policy in this regard must be strictly enforceable within the organization and it will result in the breach of duty if the officers fail to comply therewith. Such policy will contain details and specific procedures for the performance of particular duty.

This section will describe the scope of the main policy and secondary policy to be set out by the reporting entity.

### **1. The main policy on AML/CFT**

It shall be the main policy as prescribed in the ministerial regulations, i.e. the reporting entity must have AML/CFT objectives as its main policy. In order to ensure that the reporting entity is able to achieve the objectives, the policy should contain the following matters:

(1) The reporting entity will support and is ready to comply with the law on anti-money laundering and the law on counter terrorism financing and strictly undertakes the customer due diligence process, including the transaction report and performance of other duties under the said laws in full;

(2) The reporting entity will set out the (secondary) policy or essentials in performing duties concerning customer acceptance which deals with arrangement for customer identification under the law on anti-money laundering;

(3) The reporting entity will have the (secondary) policy or measures laying down the rules for money laundering and financing of terrorism risk management;

Whereas the (secondary) policy or measures on risk management must consist of (1) management of internal organizational risks arising from products or services or service channels; (2) risk management for all customers; (3) risk management for auditing the suspicious transactions;

(4) The reporting entity will have to accomplish the (secondary) policy or program regarding recruitment of employees or staff by efficient process and assurance that the said recruitment system will render the employees or staff to understand the main policy and secondary policy, including arrangement of ongoing staff training programs relevant to compliance with the AMT/CFT measures in order to properly perform the duties;

(5) The reporting entity will conduct internal audit for the work related to compliance with the AML/CFT measures, as well as operation system under the main policy and the secondary policy in full, whereas the authority for such internal audit shall be independent without interference from any unit or the senior management;

(6) The reporting entity will have the process to revise and update the main policy and secondary policy consistent with the products, services or new service channels specifically in connection with the application of technology or electronic networks at all times.

For the establishing of the main policy, the reporting entity should consider the provisions in the Notification of AMLO, Re: Guideline for setting customer acceptance policy and money laundering risk management policy related to customers of financial institutions and professions under Section 16 (1) and (9), 2013, in addition to this guideline.

It is not necessary to have details in the main policy. Details and procedures will usually appear in the secondary policy which may be called otherwise, e.g., standard, measure, notification, guidance, manual, etc. of the organization.

**2. The secondary policy or details of performing duties relevant to acceptance of customers**

The customer acceptance policy forms an integral part of the operation under the main policy on AML/CFT. Using the term “policy” in this regard means the operation as stated in order to achieve the objective in such subject. In this case, the customer acceptance policy is deemed as the secondary policy under Clause 1 of the main policy and the term may be revised from “policy” to other term up to each reporting entity’s internal system:

The customer acceptance policy should take into account of:

(1) Procedure in arrangement for customer identification: Identifying type of information, documents or evidence to be presented by the customer to the reporting entity, types of questionnaire, method of filling in the information, and advice given to customers in various cases such as:

- The customer having previous business relationship with the reporting entity;
- The customer is disabled or paraplegic;
- The customer giving insufficient information;
- .....etc.

The reporting entity must have the principle not contrary to Notification of the Prime Minister Office, Re: Procedure in identification of customer of financial institutions and professions under Section 16, dated July 11, 2013. Therefore, the said notification should be strictly considered in combination with this guideline.

(2) Procedure in identification of customer: Outlining the method of information examination, initial assessment to consider requesting additional information, method of verification with name list as prescribed by the law and procedures in various cases, such as,

- In case it has been assessed that additional customer information must be requested owing to finding some risk factors;
- In case of finding that the customer refused to give information;
- In case of finding that the customer gave false information;
- In case of finding that the customer has information matching with the name list prescribed by the law;
- Method of rejecting customer;
- Method of requesting extension of time in approval of customer acceptance;
- .....etc.

The reporting entity may look at the details relevant to customer acceptance in Section 3: Approval of customer acceptance in this guideline.

(3) Customer acceptance procedure: Stating how to establish customer relationship and use of discretion in the following cases, such as,

- In case of finding that the customer has already passed the stage of identification but the information is insufficient for clearly determining the risks;
- In case of finding that the customer is the person subject to report suspicious transaction before or during the course of establishing a relationship;
- In case of finding that the customer has high risks, how many levels of executives must be requested for approval?
- In case of the customer refusing to give additional information for specifying his risks;
- .....etc.

### **3. (Secondary) policy or the measure laying down the rules for ML/FT risk management**

Guideline in setting the secondary policy and its enforcement is same to the secondary policy in Clause 2;

ML/FT risk management policy should consist of:

- Rules and risk factors to assess the risks of the products, services and all service channels through which the reporting entity provides its services or carries out the customer

relationship. (See this guideline in the part of risks management in combination with the setting of this policy);

- Rules and risk factors to assess risks of the customer;
- Guideline in using discretion in the analysis and risks assessment;
- Method of summarizing the assessment and request of approval to revise the risks;
- Process after approval of assessment results and recording of information.
- .....etc.

The reporting entity may look at details concerning the setting of steps and risk factors in the subject: risks management in this guideline.

#### **4. (Secondary) policy or program on recruitment and staff training**

Guideline in setting the secondary policy and its enforcement is same to the secondary policy in Clause 2;

##### **(1) Recruitment of staff**

The reporting entity must have steps and procedures for hiring employees in consistent with the main policy in Clause 1. Interview or testing or training prior to accepting as employees or any steps may also be conducted to ensure that the selected employees (to be responsible for the work under the policy in Clause 1) understand the duty under the AMLA and the CTF law and are able to comply with the policy, principle or measures and guidelines set out by the organization to support the compliance with the said laws.

##### **(2) Staff training**

The reporting entity must be certain that the employees are able to always properly perform duties under the AMLA and the CTF law. Therefore, there must be training program in place to increase knowledge and understanding in AML/CFT, including understanding of the policy, measures and guideline to support the compliance with the main policy in Clause 1. In this respect, the said training should be provided regularly, whereas the problems or obstructions in compliance with the policy, measures and guideline within the organization can be an issue in the training. In this regard, the reporting entity must be certain that the employees who joined the training understand the essentials of relevant laws and rules or procedures prescribed by the organization under the framework of the law.

#### **5. (Secondary) policy on internal audit relevant to operation system**

Guideline in setting the secondary policy and its enforcement is same to the secondary policy in Clause 2

The reporting entity must set up a compliance unit to enable the organization to perform duties consistent with the AMLA/CFT rule and internal audit for the performance of duties of the said work section, including the operations of other work sections which must comply with the policy or

guideline or measures set out to implement the AML/CFT measure. The system will be functioned both by the staff and information technology.

The form of internal audit which should be stated in this secondary policy:

(1) The reporting entity should set up the internal work section or work unit to specifically perform this duty;

(2) The reporting entity may assign a third person to audit the internal performance under (1);

(3) The reporting entity must give independence in exercising audit power to the auditing work section or work unit in (1), including also the third person in (2), and be certain that there must not be interference in the audit or evaluation results by other work section and the executive board at every level;

(4) The internal audit under this policy includes the audit of operations of the headquarters, branches and affiliated companies, both domestic and international;

(5) The results from performing duties of the persons in Clauses (1) and (2) must be paid attention from the high level executive board and taken into consideration for further work improvements (in case of finding defects or problems in the operations).

In this regard, the secondary policy in this clause will make the reporting entity be certain that the set policy, measures, rules or various guidelines shall be properly performed and in case of finding defects or mistakes, it shall be the guideline for development and revision of such policy, measures, rules or guidelines in consistent with the secondary policy in the next clause.

## **6. (Secondary) policy or program to be carried out to achieve the target on development and revision of policy**

Guideline in setting the secondary policy and its enforcement is same to the secondary policy in Clause 2

The reporting entity must have the secondary policy in the revision of policies, measures, rules and guidelines consistent with the law, including internal policies in response to the newly issued international rules, specifically upon having the policy in launching products, services or using new transaction channels relevant to use of technology which may be vulnerable to money laundering risk. The reporting entity must examine whether or not the said policy is contrary to or obstructs the compliance with the applicable law at that time (newly amended) or obstructs the main policy in Clause 1, including the secondary policy, measures, rules or guidelines relevant to the policy in Clause 1.

The secondary policy in this matter should consist of:

- Setting specific period cycle for examining whether or not the policy, measures, rules or guidelines relevant to the main policy in Clause 1 are still strictly complied therewith and are there problems or obstructions thereto which may be found from the internal audit under the secondary policy in Clause 5 above;

- Executives or high level executive board shall participate in the process of reviewing and revising the policy, measures, rules or guidelines relevant to the main policy in Clause 1;

- Setting a process for examining the products, services or new transaction channels related to use of technology on money laundering risks, and potential risks in case of not being able to comply with the law, policy, measures, rules or guidelines relevant to the main policy in Clause 1;

- Setting a process for revision, development, or change in urgent cases (in case of taking actions upon encountering emergency) and being approved by high level executive or high level executive board;

- Setting a process for reporting the results of ML/FT risks management of the products, services or new transaction channels relevant to use of technology (See the Notification of AMLO, Re: Guideline for examining money laundering risks of new technology, products or services of financial institutions and professions under Section 16 (1) and (9) in combination with the setting of this process).

In this respect, the reporting entity may consider setting out other internal policies, measures, rules or guidelines to support the compliance with the main policy in Clause 1 in order to be consistent with the nature of business, structure, products, services and customers but they must not be contrary to the provisions of the relevant law.



## **Arrangement for Customer Identification**

Arrangement for customer identification is the first step when a customer wishes to establish relationship or the person making occasional transaction wishes to make the first transaction in the prescribed amount. The reporting entity must arrange for the customer to provide initial information under the Notification of Prime Minister Office, Re: Procedure of customer identification for financial institutions and professions under Section 16.

The reporting entity must arrange for its service users, both the customer and the person making occasional transaction, to properly identify themselves according to the products or services as follows:

### **1. Identification of customer wishing to establish face-to-face relationship**

The customer establishing relationship in this category means the customer who wishes to establish business relationship with the reporting entity through its employee, including the agent or third person by normal channel in the face-to-face manner, not by means of any technology or devices at the time of establishing such relationship. In this regard, the reporting entity must arrange for the customer to identify oneself as follows:

#### **(1.1) Natural person customer**

(1.1.1) Full name;

(1.1.2) Date of birth;

(1.1.3) ID number:

- In case of Thai national, meaning ID number in the ID card;

- In case of alien, meaning passport number in the passport book or ID number issued by the government or government agency of nationality to support any legal rights or ID number issued by the Thai government in the ID paper.

(1.1.4) Address:

- In case of Thai national, meaning address in the house registration book and in case of not living therein, stating also the present address;

- In case of alien, meaning address in the country of nationality and address in Thailand.

(1.1.5) Occupation and workplace;

(1.1.6) Contact information to enable the reporting entity to make contact with the customer, e.g., phone number, electronic address;

(1.1.7) Signature of the person establishing relationship.

**(1.2) Legal person customer or legal arrangement**

(1.2.1) Name of legal person or legal arrangement (as shown in accompanying papers);

(1.2.2) Taxpayer ID number (for legal person or legal arrangement required by the state to pay taxes);

(1.2.3) Reliable documents certifying status of legal person or legal arrangement):

- In case of Thai legal person, namely, affidavit of registration as issued by competent registrar, not more than six months;

- In case of legal person not registered in Thailand, namely, documents showing legal person status issued by government or state agency in the country being registered or permitting business operation or certified by reliable organization and such issuance or certification has been made not more than six months;

- Where official agency, government organization, state enterprise or other state agency is a legal person, namely, letter of intent to establish relationship and to make transaction and letter of appointment or power of attorney to establish relationship and to make transaction;

- In case of cooperative, foundation, association, club, temple, mosque, shrine and other legal person in similar manner, namely, registration documents, license to operate business or to show establishment from relevant state agency and letter of appointment or power of attorney to establish relationship and to make transaction and such issuance or certification has been made not more than six months;

- In case of legal arrangement, namely, accompanying documents showing the establishment of such legal arrangement and the said certification has been made not more than six months by the authorized person of such legal arrangement.

(1.2.4) Business type and objectives of the business operation;

(1.2.5) Common seal (if any);

(1.2.6) Place of establishment and phone numbers, including other contact information, e.g., electronic address;

(1.2.7) Full name of every authorized signatory on behalf of the legal person or the legal arrangement;

(1.2.8) Information of “the authorized signatory on behalf of the legal person being assigned to establish relationship and to make transaction with the reporting entity” and “the person being granted the last chain of authority to establish relationship and to make transaction with the reporting entity”, namely:

(1.2.8.1) Full name;

(1.2.8.2) Date of birth;

(1.2.8.3) ID number:

- In case of Thai national, meaning ID number in the ID card;

- In case of alien, meaning passport number in the passport book or ID number issued by the government or government agency of nationality to support any legal rights or ID number issued by the Thai government in the ID paper.

(1.2.8.4) Address:

- In case of Thai national, meaning address in the house registration book and in case of not living therein, stating also the present address;

- In case of alien, meaning address in the country of nationality and address in Thailand.

(1.2.9) Signatures of the authorized signatory and the attorney-in-fact under (1.2.8).

## **2. Identification of non face-to-face customer**

In principle, should the reporting entity want to add or create other channel for establishing non face-to-face business relationship with the customer, i.e. through technology or any devices, the reporting entity must consider the risks of using such service. It means that the reporting entity should select the channel of establishing non face-to-face relationship with the service type having low ML/FT risks (The procedure in consideration of the risks shall be in accordance with the guideline announced by the Secretary-General under the ministerial regulation).

However, the reporting entity may consider using the channel of establishing non face-to-face relationship with the service type having high risks but it must set out a measure requiring the customer to inform or submit full information of identification in the same manner as the establishment of face-to-face relationship by extending the period of approving the establishment of relationship until obtaining full information. The procedure for informing or submitting the information may be adopted thereafter prior to approval of making the first transaction.

At least the information for non face-to-face customer who uses service of low ML/FT risks shall be as follows:

### **(2.1) Natural person customer**

(2.1.1) Full name;

(2.1.2) ID number:

- In case of Thai national, meaning ID number in the ID card;

- In case of alien, meaning passport number in the passport book or ID number issued by the government or government agency of nationality to support any legal rights or ID number issued by the Thai government in the ID paper.

(2.1.3) Address:

- In case of Thai national, meaning address in the house registration book and in case of not living therein, stating also the present address;

- In case of alien, meaning address in the country of nationality and address in Thailand.

(2.1.4) Contact information to enable the reporting entity to make contact with the customer, e.g., phone number, electronic address;

## **(2.2) Legal person customer or legal arrangement**

(2.2.1) Name of legal person or legal arrangement (as shown in accompanying papers);

(2.2.2) Taxpayer ID number (specific for legal person or legal arrangement required by the state to pay taxes) or in case of legal person not required to pay taxes, the documents establishing the legal person or the documents showing the permission of establishment shall be shown;

(2.2.3) Place of establishment and phone number, including other contact information such as electronic address;

(2.2.4) The information of “the authorized signatory on behalf of the legal person being assigned to establish relationship and to make transaction with the reporting entity” and “the person being granted the last chain of authority to establish relationship and to make transaction with the reporting entity”, namely:

(2.2.4.1) Full name;

(2.2.4.2) Date of birth;

(2.2.4.3) ID number:

- In case of Thai national, meaning ID number in the ID card;

- In case of alien, meaning passport number in the passport book or ID number issued by the government or government agency of nationality to support any legal rights or ID number issued by the Thai government in the ID paper.

(2.2.4.4) Address:

- In case of Thai national, meaning address in the house registration book and in case of not living therein, stating also the present address;

- In case of alien, meaning address in the country of nationality and address in Thailand.

## **3. Identification of the person making occasional transaction**

In case of the reporting entity giving service, whereas each transaction may not be related to or linked with the previous transaction, the reporting entity shall arrange for this group of persons using the service as “the persons making occasional transactions”. The reporting entity should consider providing such occasional service specifically for low risk transaction/service. (The procedure in consideration of the risks shall be in accordance with the guideline set forth by the Secretary-General under the ministerial regulation).

In the case where the reporting entity provides occasional service for high risk transaction or service, the reporting entity must set out measures in requesting additional information in order to be certain that such transaction is reasonable and not under ML/FT risks such as requesting trade documents capable of showing reasons or objectives of the transaction or requesting additional identification information, etc.

The reporting entity shall oblige the person making occasional transaction in monetary value or under the following conditions to identify oneself:

(1) Making transaction with cash or property at the value from seven hundred thousand baht or more;

(2) Making transaction of electronic fund transfer (both the electronic fund transfer conducted by financial institutions and electronic fund transfer under the Royal Decree governing electronic payment conducted by the professions under Section 16 (9)) and having electronic money transaction at the value from fifty thousand baht or more;

(3) Regardless of designated threshold if there is a suspicion in giving information on the transaction or to find suspicious or unusual conduct.

At least the information of identification for the person making occasional transaction in using the service or making transaction having low ML/FT risks shall include the following:

**(3.1) The person making occasional transaction who is a natural person:**

(3.1.1) Full name;

(3.1.2) Date of birth;

(3.1.3) ID number:

- In case of Thai national, meaning ID number in the ID card;

- In case of alien, meaning passport number in the passport book or ID number issued by the government or government agency of nationality to support any legal rights or ID number issued by the Thai government in the ID paper.

(3.1.4) Address:

- In case of Thai national, meaning address in the house registration book and in case of not living therein, stating also the present address;

- In case of alien, meaning address in the country of nationality and address in Thailand.

(3.1.5) Contact information to enable the reporting entity to make contact with the customer, e.g., phone number, electronic address;

**(3.2) The person making occasional transaction who is a legal person or legal arrangement**

(3.2.1) Name of legal person or legal arrangement (as shown in key documents);

(3.2.2) Taxpayer ID number (specific for legal person or legal arrangement required by the state to pay taxes) or in case of legal person not required to pay taxes, the documents establishing the legal person or the documents showing the permission of establishment shall be shown;

(3.2.3) Place of establishment and phone number, including other contact information such as electronic address;

(3.2.4) The information of “the authorized signatory on behalf of the legal person being assigned to establish relationship and to make transaction with the reporting entity” and “the person being granted the last chain of authority to establish relationship and to make transaction with the reporting entity”, namely:

(3.2.4.1) Full name;

(3.2.4.2) Date of birth;

(3.2.4.3) ID number:

- In case of Thai national, meaning ID number in the ID card;

- In case of alien, meaning passport number in the passport book or ID number issued by the government or government agency of nationality to support any legal rights or ID number issued by the Thai government in the ID paper.

(3.2.4.4) Address:

- In case of Thai national, meaning address in the house registration book and in case of not living therein, stating also the present address;

- In case of alien, meaning address in the country of nationality and address in Thailand.

#### **4. Identification of the person making non face-to-face, occasional transaction**

The reporting entity should not provide non face-to-face service for the person making occasional transaction owing to the high ML/FT risks unless the reporting entity shall have measure to reduce the risks in providing such service such as limitation of amount for each transaction and for each day, requesting additional information for examining objectives in making transaction and identity of the person making occasional transaction, as well as an audit system or refusal for occasional transaction which is unusual or suspicious, etc.

At least the identification information for the person making the face-to-face, occasional transaction in using the service or making transaction having low ML/FT risks is the information as follows (comparable to the identification for the customer in Clause 2: The customer not making face-to-face relationship):

##### **(4.1) Natural person customer**

(4.1.1) Full name;

(4.1.2) ID number:

- In case of Thai national, meaning ID number in the ID card;

- In case of alien, meaning passport number in the passport book or ID number issued by the government or government agency of nationality to support any legal rights or ID number issued by the Thai government in the ID paper.

(4.1.3) Address:

- In case of Thai national, meaning address in the house registration book and in case of not living therein, stating also the present address;

- In case of alien, meaning address in the country of nationality and address in Thailand.

(4.1.4) Contact information to enable the reporting entity to make contact with the customer, e.g., phone number, electronic address.

#### **(4.2) The legal person customer or legal arrangement**

(4.2.1) Name of legal person or legal arrangement (as shown in key documents);

(4.2.2) Taxpayer ID number (specific for legal person or legal arrangement required by the state to pay taxes) or in case of legal person not required to pay taxes, the documents establishing the legal person or the documents showing the permission of establishment shall be shown;

(4.2.3) Place of establishment and phone number, including other contact information such as electronic address;

(4.2.4) The information of “the authorized signatory on behalf of the legal person being assigned to establish relationship and to make transaction with the reporting entity” and “the person being granted the last chain of authority to establish relationship and to make transaction with the reporting entity”, namely:

(4.2.4.1) Full name;

(4.2.4.2) Date of birth;

(4.2.4.3) ID number:

- In case of Thai national, meaning address in the house registration book and in case of not living therein, stating also the present address;

- In case of alien, meaning passport number in the passport book or ID number issued by the government or government agency of nationality to support any legal rights or ID number issued by the Thai government in the ID paper.

(4.2.4.4) Address:

- In case of Thai national, meaning ID number in the ID card;

- In case of alien, meaning address in the country of nationality and address in Thailand.

## **5. Examination of information and identification documents**

The reporting entity must set steps in the examination of information and identification documents of the customer or the person making occasional transaction, whereas the examining personnel or employee must be authorized in using appropriate discretion. In this respect, the objectives of examination at this stage are:

(5.1) To learn that the customer or the person making occasional transaction is the person, legal person or legal arrangement legally existing in reality;

(5.2) To learn that the objectives in establishing relationship or making occasional transaction are consistent with the identification information of the customer or the person making occasional transaction;

(5.3) To learn that the obtained identification information is sufficient for carrying out risk management and customer due diligence (CDD) process under the Ministerial Regulation, Re: Customer due diligence, 2013.

Moreover, the use of appropriate discretion in this regard includes requesting additional documents, information or evidence from the customer or the person making occasional transaction and also the decision not to establish customer relationship or to accept making occasional transaction if not receiving complete information.



## **Approval for Customer Acceptance**

Steps in the approval for customer acceptance are the process continuing from the arrangement for customer identification. Approval for customer acceptance must take into account initial information required for identification and examination of the name list relating with ML/FT risk assessment.

Hereinafter, it is the process which the reporting entity must carry out immediately after arrangement for customer identification.

### **1. Assessing needs for additional information from customer**

Under the provisions of the ministerial regulation, the reporting entity is required to have identification of customer's or occasional customer's identity after the stage of arrangement for customer identification.

However, even though a customer or either one of the persons making transaction is not required to identify oneself, but, should the reporting entity be suspicious that it may be connected to ML/FT or reasonable to consider that the arrangement for identification should be carried out, the reporting entity must carry out this step:

#### **(1.1) Prescribing factors in the assessment**

The reporting entity should set up steps for conducting initial assessment whether or not it is necessary to obtain or request additional information or evidence from the customer for identification of the customer in order to be consistent with ML/FT risks, whereas the reporting entity should identify the factors or considerations in assessing needs for initial information (either one or more together, depending on the structure and discretion of the reporting entity) as follows:

- (a) The factors relevant to financial product, types of service, channels to use service;
- (b) The factors relevant to the complexity of business structure of the customer or of the person making occasional transaction;
- (c) The factors relevant to the area or country connected with the use of service;
- (d) The factors relevant to the source of funds or income of the customer;
- (e) The factors relevant to the value of service using.

#### **(1.2) Use of discretion in the assessment**

The reporting entity must set standards in using discretion to analyze ML/FT risks of each customer requesting establishment of relationship in order to assess the needs for additional information. In order to set the said standards, the reporting entity must refer to the factors in Clause 1.1 as the principle for determining the use of discretion.

Example

From the identification information and the request for establishing first-time relationship, it is found that factors relevant to the customer are:

Factor (a): The customer requests cross-border debt payment service through debiting from account or securities trading through agent company abroad which is considered to be the service not in the low-risk group;

Factor (c): The customer requests monetary and value transfer service or securities trading in the country having high risks of money laundering;

Factor (e): The customer requests the first transaction in high amount.

From the considerations, it is found that despite the customer is lacking Factor (b) which means that the customer possesses no complexity as it is the company having only three shareholders, and lacking Factor (d) which means that the customer states the source of funds from no-risks business operation and is able to show the source. However, upon consideration of the three factors related to the customer above, the reporting entity has set the standards that for the pattern in this manner, the officer should use the discretion “to request additional information because it is possible for the customer to become a customer having risks at high level”, etc.

Therefore, the reporting entity must initially identify customer’s risk levels and if it is found that the customer has information and facts identical to one or more than one risk factors, how will the reporting entity set the standards for use of discretion by the officer performing the duty. In this regard, the scope of use of discretion should be clearly stated.

Example 1

If it is found that the customer matches with risk Factor (b) or part of risk Factor (b) included, the officer must use the discretion in requesting additional information and documents from the customer, namely:

- The documents showing shareholding or legal person customer’s benefits<sup>i</sup>;
- The information identifying ultimate beneficial owner who is a natural person and information or facts showing that such person is connected with the legal person customer;
- The information related to the top executive<sup>ii</sup> of the legal person customer;
- ..... , etc.

Example 2

If it is found that the customer matches with risk factor (c) or part of risk factor (c), the officer must use the discretion in requesting additional information and documents from the customer, namely:

- The information showing clear objectives in making the transaction, e.g., the purpose of money transfer to risk area;
- The information showing the obligation or relation with the recipient in the risk country, e.g., the business agreement co-signed with the party being legal person in the risk country;

- Requesting the customer to advise the maximum amount expected for each transaction in order to consider the consistency with the business agreement or the objectives as informed;
- Verifying recipient party's information against the list of persons at risks of ML/FT e.g., examining the company name and name of the person signing the agreement with the said database as far as the information is available for examination;
- ....., etc.

Therefore, in order for the reporting entity to fully comply with the rules in Clause 1, the reporting entity must set the risk management standard for the product, service and service channel operated by one's own organization in parallel with the setting of risk management standards for the customer or the person making occasional transaction in the first place before adopting all standards to apply with the analysis factors in order to assess the needs for additional information from the customer.

Apart from considering risks for the product, service and service channel, the reporting entity may make use of the information on some of the low or high risk factors in case of being able to learn of such risks from the identification information (for the low or high risk factors, see the provisions of the chapter on ML/FT risk management and guideline prescribed by the Secretary-General, Re: Guideline on prescribing factors to consider the customer having low-risk level). For example, at the stage of identification, the customer identified himself as a politician in the position of minister, whereas the provisions prescribe that the person having domestic political status has high risks, therefore, the officer must assess at this stage that additional information must be sought (as the person is not in the low-risk group) whether or not the objectives or the product, service category and service channel have low risks, etc.

Therefore, in the guideline of using discretion in this matter, the reporting entity must identify certain factors that can be assumed by its officer during the course of customer identification without having to use discretion e.g., when the customer identified itself as an official agency or a public company listed on the stock exchange, the officer may assume that risks are low without having to request additional identification information unless ..... (the service of very high value of money is requested and being the investment or cross-border transaction, the officer should consider requesting information relevant to the source of investment or other businesses operated by the customer outside its main business to support the risk management at the stage of classifying risk level) etc.

## **2. Examination with name list information prescribed by the law**

Under the provisions of the ministerial regulation on customer due diligence, 2013, prescribing "the customer due diligence including the relevant person in establishing relationship or the person making occasional transaction, as may be the case, with the list of person, group of

persons, legal person or entity designated under the resolutions of the UN Security Council as terrorists or the person under court order to be the person designated under the CTF law” as an important step prior to the approval to accept customer or make transactions for occasional customer.

### **2.1 Name list information used for verification under the law**

Under the proper process, upon the reporting entity having already arranged for customer identification, appraising requirement for additional information from the customer, the last stage prior to accepting the customer is the verification of name list as stated in the paragraph above. The name list information to be verified with the customer is namely:

The information of designated person under the CTF law, in this regard, consists of two parts, namely:

- The information of person related to terrorism and terrorist financing who is the designated person by court order;
- The information of person related to terrorism and terrorist financing under the resolutions of the UN Security Council being verified by AMLO and approved by the Minister, including information from other country as verified by AMLO and approved by the Minister.

### **2.2 Target group subject to examination against the name list information prescribed by the law**

From the stage of customer identification to the stage of assessing needs for additional information, the reporting entity may have received two types of customer’s information or the person making occasional transaction, namely:

(2.2.1) The information obtained from customer identification and no additional information from the assessment in Clause 1:

In this case, the reporting entity must examine the persons as follows:

- The natural person customer requesting the establishment of relationship or the natural person requesting to make occasional transaction;
- The person authorized by the natural person customer requesting the establishment of relationship or the natural person requesting to make occasional transaction (if any);
- The legal person customer requesting the establishment of relationship or the legal person requesting to make occasional transaction;
- The person or legal person of significance<sup>iii</sup> within the organization of the legal person customer herein refers to every authorized director, including the ultimate authorized person establishing relationship with the reporting entity (if any) and the authorized director requesting to make occasional transaction, including the ultimate authorized person requesting to make occasional transaction (if any);

(2.2.2) The information received from the customer at the stage of identification and additional information from the assessment in Clause 1:

In this case, the reporting entity must examine the persons as follows:

- The natural person customer requesting the establishment of relationship or the natural person requesting to make occasional transaction;
- The person authorized by the natural person customer requesting the establishment of relationship or the natural person requesting to make occasional transaction (if any);
- The legal person customer requesting the establishment of relationship or the legal person requesting to make occasional transaction;
- The person or legal person of significance within the organization of the legal person customer herein means every authorized director, including the ultimate authorized person establishing relationship with the reporting entity (if any) and the authorized director requesting to make occasional transaction, including the ultimate authorized person requesting to make transaction (if any);
- The ultimate beneficial owner of the natural person customer (in case of having to examine under Clause 1 (1.2) and finding it relevant);
- The ultimate beneficial owner of the legal person customer (in case of having to examine under Clause 1 (1.2));
- The high-level executive (in case of having to examine under Clause 1 (1.2));
- The shareholder having the significance of the legal person customer who may not be the ultimate beneficial owner, but has key role in receiving benefits from the legal person customer in the amount also considered to be close to that of the ultimate beneficial owner (in case of prescribing internal policy for examination under Clause 1 (1.2) and finding it relevant);
- The legal person and the natural person signing the business contract as the party of significance<sup>iv</sup> of the legal person customer (in case of prescribing internal policy for examination under Clause 1 (1.2) and finding it relevant);
- The legal person or the natural person considered by the officer and decided to conduct examination owing to having significant connection with the customer (in case of prescribing internal policy for examination under Clause 1 (1.2) and finding it relevant).

Remark: The reporting entity may set this examination stage as prescribed by the law as the stage subject to immediately action after receiving the customer identification information and thereafter should there be additional identification information of the person connected to the customer, such additional information of the person or legal person shall be verified with the name list prescribed by the law before granting customer acceptance.

### 3. Prescribing measure or other relevant rules

In order for the stage of customer acceptance in accordance with the principle under the ministerial regulation on customer due diligence, 2013, and AML/CTF international standard, it is necessary for the reporting entity to set forth policy, guideline or internal rules as follows:

#### 3.1 Guideline for examination of identification information

The reporting entity must set stages and procedures of using discretion for relevant officers to assure that the said identification is fully completed.

##### Example

Stage 1: The officer must examine the filling up of information of the customer to confirm that it is complete as prescribed by the law;

Stage 2: The reporting entity may rely on reliable information technology system as the tool for customer verification;

Stage 3: In case of no reliable verification under Stage 2, the reporting entity must establish other procedures instead, for example, setting out additional procedures for the officer to request original evidence if the copy of documents submitted by the customer have not been certified or unclear;

Stage 4: In case of suspicion during the course of verification in Stage 2 or Stage 3, the reporting entity may set out procedures for the officer to extend the period of receiving the identification documents and inform the customer to bring other reliable documents for reference, e.g., public utilities bills having the name of customer and present address, etc.

Stage 5: Establishing principle for the relevant officer to be able to refuse the request for establishment of customer relationship at the stage of identification should there be suspicious reason which may be risks of money laundering or financing of terrorism and report to the superior to determine whether a suspicious transaction report should be filed with the AMLO.

....., etc.

#### 3.2 Use of discretion in customer identification

The reporting entity should use the principle and assessment factors under Clause 1 (Re: Assessing needs for additional information from customer) as the basis for issuing rules for the officer to perform duty and use proper discretion in requesting additional information, e.g., organization structure of customer, name list information of executives or top management board, etc. It is also necessary to set forth procedures in using discretion or process of finding additional customer information, in particular, the stage of finding information relating to ultimate beneficial owner of the customer (for example, see Clause 1, Re: Assessing needs for additional information from customer).

### 3.3 Rules in accepting information of the ultimate beneficial owner of the customer

The reporting entity must set out the procedures for its officers for the verification of “the ultimate beneficial owner of the customer” by stating how the said beneficiary can be found from what information, facts, original evidence or any reference and stating the next stage in case the first procedure fails. In this regard, such procedures should follow the ministerial regulation on customer due diligence, 2013, and relevant guideline prescribed by the Secretary-General.

The reporting entity may set out the procedures other than the principle under the law and international standard but must be certain that the procedures are useful in finding the true information, for example, should Procedure 1, Procedure 2 and Procedure 3 fail to find the results, the reporting entity may set out other alternative, e.g., requesting the customer to give information of “the ultimate beneficial owner of the customer” as well as facts as information showing how such natural person who is “the ultimate beneficial owner of the customer” is related to the customer, etc.

Apart from this, the reporting entity must identify types of information necessary for the verification against the name list prescribed by the law in the next stage. For example, when the officer obtained information concerning “the ultimate beneficial owner of the customer”, the customer must give the information connected with the said beneficial owner, i.e. full name and ID number. In case of not being able to give ID number information owing to the obstruction on the source of information, the customer must find other circumstantial information of such beneficial owner, e.g., nationality, other legal person in which the beneficial owner holds shares as supporting information for verification against the name list as prescribed by the law in the next stage.

The reporting entity must give freedom to the officer’s use of discretion and should ensure that such officer truly understands the principle and practice and strictly performs duties under such principle. It is utmost necessary for the reporting entity to set out requirements for its officer to refuse establishing customer relationship if there is a suspicion of ML/FT risks, and to report to his/her superior for considering whether a suspicious transaction report should be filed with the AMLO.

#### Example

Procedures in seeking information of “the ultimate beneficial owner” of legal person customer<sup>1</sup>:

Procedure 1: Examination from benefits obtained from shareholding from.....% or more<sup>2</sup> as appeared in the evidence or reference documents. In case of not finding such information,

---

<sup>1</sup> In case of the beneficial owner of the natural person customer, it may be initially assumed for the setting of the method to find information that the natural person customer will establish relationship or transaction for one’s own benefits (the beneficiary is the customer itself), however thereafter the reporting entity finds that, under reasonable belief, the customer may carry out relationship for other person, for example, money transfer in account to other person at every deposit or full amount transfer or almost full amount or authorization for third person to act on one’s behalf indefinitely (not acting on one’s behalf from time to time), the facts may be recorded or it may be assumed that there may be other ultimate beneficiary included.

<sup>2</sup> The reporting entity should determine the shareholding proportion by considering majority shareholding proportion which may appear in the law relevant to supervision of business or by considering from general guideline used in the same business group as the reporting entity.

more information shall be requested from the customer until finding “the ultimate beneficial owner”. Should it be unable to make examination by this procedure owing to serious obstacles, Procedure 2 shall be considered.

Procedure 2: Examination from information or facts concerning the ultimate effective control over the customer organization, whereas the information may be sought from other reliable sources of information. Should it be unable to make examination by this procedure owing to lacking sources of information or not finding information, Procedure 3 shall be considered.

Procedure 3: Consideration shall be made by assuming that the natural person having the authority to set out the policy or to manage the customer organization may be “the ultimate beneficial owner” of the customer. Should there be a doubt that the results from consideration under this procedure may be contrary to the facts, Procedure 4 shall be considered as finality.

Procedure 4: Requiring the customer to state the information as to the identity of “the ultimate beneficial owner” of the customer and showing the facts, documents or evidence showing connection between the legal person customer and the said beneficiary.

The reporting entity must identify the information of “the ultimate beneficial owner” required from the customer as follows (see the relevant guideline announced by the Secretary-General):

- (a) Full name information;
- (b) ID number information as issued by the state;
- (c) Address information.

In case the customer is unable to give information in (b) or (c) or both, the customer must give other circumstantial information useful for the examination, such as, nationality, other occupations or position held by the ultimate beneficial owner in other legal person, etc.

Should every procedure has been performed but still failing to find “the ultimate beneficial owner” of the customer or the customer is unable to give at least the information under (a) and other circumstantial information, and with regard to customer’s risks found in the initial assessment, the reporting entity must eventually refuse the customer’s request to establish relationship.

### **3.4 Procedures in approval for customer acceptance**

The reporting entity must set out procedures for the approval of customer’s request to establish relationship by having to classify types of relationship and assign the officer with authority to give approval consistent with the business relationship or group of customers in order to be certain that prior to the approval to establish business relationship with the customer, the reporting entity has also carefully verified the customer information consistent with the initial assessment level in order to request additional customer information as well as ML/FT risks at the approval stage.

#### Example

The reporting entity must set up steps for approving business relationship consistent with the risks of the product, service category or service channel as follows:



Category 1: For credit with a low limit, saving account in the amount not exceeding ..... baht in the category of ..... , the officer in the position at the level of ..... has authority to approve the establishment of relationship in case of the initial assessment finding that it is not required to request additional information from the customer (as the customer does not have risk factors).

Category 2: For international trade, international money transfer in the category of ..... , the officer in the position at the level of ..... has authority to approve the establishment of relationship in case of the initial assessment finding that it is not required to request additional information from the customer (as the customer does not have risk factors).

Category 3: For the establishment of all types of relationship which requires additional customer information owing to having risk factors, the officer in the position of ..... shall prepare the report and results of approval for submission to ..... (position) for verification and confirmation of the said approval at the higher hierarchy.

Category 4: For the establishment of all types of relationship found at the stage of ML/FT risk management that the customer is not included in the group of low-risk customers, the officer in the position of ..... shall prepare the report and results of approval for submission to ..... (position) for verification and confirmation of the said approval at the higher hierarchy.

Special condition: In case there is ground for refusing the request for establishment of relationship of the customer, the officer having position and duty to endorse must prepare the summary report explaining the cause of refusal for submission to ..... (position) for consideration and issuance of the order "Refusal of request for establishing customer relationship" at the final stage also together with "the consideration of making a suspicious transaction report" to AMLO.

....., etc.

Despite the reporting entity having already set out the customer acceptance policy consisting of the stage, rules, procedures or examination guideline, it is also duty bound to manage the risks of money laundering and financing of terrorism of the customer along with the approval to accept customer. It means that upon endorsing customer acceptance, the risks of money laundering and financing of terrorism of the said customer must be classified, which shall be in accordance with the policy or measure or rules in the ML/FT risk management as prepared by the reporting entity under the scope of the ministerial regulation on customer due diligence, other relevant regulations and this guideline.

## **Money Laundering and Financing of Terrorism Risks Management**

The reporting entity must set out the policy or standard for money laundering (ML) and financing of terrorism (FT) risk management which addresses risk management within the organization, products, financial services and service channels. The risk management aims to assess the extent of ML risks associated with each product, financial service and delivery channel and to perform customer risk analysis at the stage of customer identification, approval for customer acceptance as well as the stage of carrying out relationship with the customer.

Apart from setting out policy or standard of risk management within the organization, the reporting entity is also obliged to set out policy or standard for customer risk management taking into account the results of risk management within the organization together with other factors as prescribed by the law or as the reporting entity deems fit within the scope of law.

The process of customer risk management must be completely carried out by the reporting entity at the same time with the approval for establishment of relationship or when making occasional transaction. After the establishment of relationship, the reporting entity is responsible for continuously carrying out management of risks until the termination of relationship.

### **1. Money laundering and financing of terrorism risk management within the organization**

The reporting entity must set out standards for management of risks associated with its products, services and delivery channels. This said standard considers the result of risk assessment relating to every product, service and delivery channel. In this respect, the said risk management will be used as a condition in the assessment process to request additional information of the customer at the customer identification stage, and to determine whether the customer is subjected to closer scrutiny.

The risk management standard may be set out either in the form of main policy of the organization or secondary policy under the AML/CFT policy or in the form of other internal regulations but it must be certain that this risk management standard is the essential stage not to be neglected by the organization and staff members and it must be strictly carried out.

#### **1.1 Risk management of products, services and delivery channels relating to the use of equipment or technology**

The reporting entity must have policy, measure or rules in place for management of risks of all products, services and delivery channels relating to the use of equipment and technology.

As the products, services or delivery channels of the reporting entity are related to providing financial and investment services to customers, therefore, the chance for these to be abused by the customers or criminals as the channels or tools in laundering money may occur. Particularly, the use

of electronic equipment or technology that provides fast and easy services is more vulnerable to misuse than those carried out face-to-face with the service staff.

The risk management has the objectives for the reporting entity to examine the extent to which its products, services or delivery channels relating to the use of electronic equipment or technology have the risks of money laundering; what products, services or delivery channels that can be abused by the customers for money laundering purpose; and how to mitigate such risks either by employing technology or personnel to minimize the risks as much as possible; and if money laundering occurs, damages can be kept to the lowest level. The procedure in mitigating risks also depends on the form and nature of the use of such technology or equipment.

#### Example

(1) If the service is the deposit or withdrawal of cash through the channel of information technology in receiving/transmitting data, the reporting entity may limit the amount of money and number of transactions made by the customer on each day and conduct more enhanced scrutiny on the transactions made through such equipment or technology than the transactions made through the normal channel at the office or branch office, etc.

(2) In the case of electronic cards by which customers withdraw cash or buy goods and services within limited chains of shops, the reporting entity may limit the amount of money that suits with daily living of such group of customers. If cards can be used for cash withdrawal and making electronic monetary value transfer, the reporting entity should prescribe the amount of cash withdrawal of each transaction on each day by the customers and conduct enhanced and quick scrutiny on such cash withdrawal or money transfer.

### **1.2 Assessment of product or service risks**

The results obtained from the risk assessment relating to the products and services are one of many factors used to sort out group of customers at the customer identification stage and customer acceptance stage, hence, to consider whether simplified customer due diligence (simplified CDD) can be performed. Apart from that, it is also a factor used in customer risk management.

The reporting entity must have standard for management of ML/FT risks for its own business operation by determining which of the financial products and services have higher or lower ML/FT risks. The criteria for risk management are contained in the guideline regarding criteria or factors for determining low-risk customers as prescribed by the Secretary-General.

However, the results of assessment of the products and service risks do not indicate that the reporting entity which provides high-risk products or services is a high-risk reporting entity. Rather, the assessment signals the reporting entity to undertake proper risk-based approach, to mitigate or reduce the risks to the minimum and then to assess whether additional customer information must be acquired as well as to appraise the risk level of each customer.

In principle, the reporting entity must follow the guideline regarding criteria or factors for determining low-risk customers as prescribed by the Secretary-General. However, in the case that the reporting entity has enhanced measures for risk management and effectively controls the risks associated with such products or services, the products or services previously assessed as high risks may be reassessed to a lower risk level.

#### Example

The reporting entity may set out the guideline for management of product or service risks according to the following simple processes:

**Stage 1:** Listing all products and services provided to customers relating to finance, investment or commerce wherein the customers have asset or financial flows in or through the system;

**Stage 2:** Sorting out the product groups and financial services having low risks from all the products and services, including classification of various risk levels for the remaining products and financial services;

**Stage 3:** Assessing risks and undertaking management to reduce risks of the products and financial services not in the low-risk groups;

**Stage 4:** Regularly examining the risk mitigation system and revising the risk management of the products and financial services, specifically upon launching new products or financial services.

**Special stage:** In the analysis and assessment of risks of the products and financial services relating to the use of new technology, the reporting entity is required to prepare reports and inform AMLO (under the provisions and guideline prescribed by the Secretary-General in the ministerial regulation, Re: Guideline to examine the risks on money laundering of the new technology, products or services of the financial institutions and professions under Section 16 (1) and (9).

#### **Identifying factors in risk assessment**

In assessing risks relating to products and services, the reporting entity must follow the guideline regarding criteria or factors for determining low-risk customers as prescribed by the Secretary-General with due regard to specific factors relating to products and services, namely:

(1) The transfer, negotiable financial products or the right to use services, including benefits from transferable or negotiable services This category of services expose the reporting entity to money laundering and financing of terrorism as the customer carries out the transfer or negotiation itself or because the stage of negotiation or transfer is easily executed and quickly completed;

(2) Cash conversion: The products or the right to use services that is convertible to cash in the last chain of payments whereas the reporting entity makes payment directly to the customer, specifically, the negotiable instrument which can be cashed at any banks, or the business related to foreign currency payment or reference number or document stating simple information that

can be cashed at any establishments (except when the it is ascertained that the recipient information will be verified in compliance with the ministerial regulations);

(3) Unlimited amount of money or unlimited number of times in using services/ products or right to use services with unlimited amount of payment should have risks of becoming the channel of money circulation in large amount and should it also have unlimited number of times in using services, it will cause even more risks. Therefore, the products without conditions in limiting the purchase or the financial services without limiting number of using services shall have more risks;

(4) Cross-border use: The products or the right to use services that may be used abroad will have higher risks of cross-border money laundering. In the case that the products or the right to use services can be used abroad and payable to the receiver (i.e. not made through any account at financial institution obliged to perform customer due diligence) shall have even higher risks;

(5) Debt burden: Lending services that thus cause debt burden on the customers usually have low risks of money laundering. However, the use of credit cards which has certain credit limit and will not charge interest if customer pays on due may be a channel for money laundering as the person can purchase goods and services without having to pay in cash. The use of credit cards will have higher risks if the service provider does not set a threshold, or allow a very high credit limit. From all reasons, this type of products or services has lower risks in money laundering than other types described above;

(6) Type of products or services: Some products or services have low risks in money laundering if the objectives of the products or services and benefits obtained from such products and services are for the remedy or compensation of damages or for savings necessary for only some group of persons, namely:

- Casualty insurance;
- Life assurance paid only when the insured died;
- Group insurance having objectives for benefits of employees or for remedy of damages;
- Funds set up under the law with the objectives for savings or for providing assistance to the elderly or underprivileged persons and having limit in buying share units or in obtaining the right in using services;
- Financial products for the persons-in-need as supported by the state and with limited amount of money for each customer.

It is necessary for the reporting entity to apply the said principles for setting up policy/guidance/rules, and management of risks related to the financial products and services. This will also be used in assessing the request for additional customer's information and also in the stage of classifying the risks level of the customers.

### **1.3 Risk assessment of service delivery channels:**

The service delivery channel means the procedure used by the reporting entity to bring the products or services to the customer, including the channel of services from the commencement of establishing relationship to the making of transaction. The service delivery channel may be divided into:

Channel 1: The service delivery channel through employees of the reporting entity whether at the branch offices or by appointment to provide off-the-site services;

Channel 2: The service delivery channel through agents/brokers: In this case, the reporting entity must bear responsible for the agents/brokers' conducts (within the scope of agreed services). It is also deemed as face-to-face services in the same manner as that of Channel 1;

Channel 3: The service delivery channel through electronic media or communication by other means which is not a face-to-face service, such as, opening account to trade securities through internet, purchase order of unit trust by phone, withdrawal of money from ATM, use of monetary value transfer service through internet, etc.

Generally, the service delivery channel type 3 usually has more risks than others, whereas the reporting entity may prescribe strict measures that the customer must contact the employee for confirmation prior to opening first transaction service to mitigate risks from non-face-to-face transaction. In the case that there is no provision for the customer to meet the employee for confirmation of business relationship, it is still considered to be the delivery channel having more risks except when the reporting entity has efficient procedures for customer identification and verification of identity and is certain of the least chance for the customer to use fake name, pseudonym or to use one's own name on behalf of other person without notifying the reporting entity.

The reporting entity should consider the risks relating to the selection to use the service delivery channel in combination with the risk factors relating to the products and services, including also the risk factors of the customer itself in order to use discretion in making the most accurate risk assessment.

## **2. Money laundering and financing of terrorism risk management for the customer**

The reporting entity is duty bound to prescribe the policy/measures or rules for money laundering (ML) and financing of terrorism (FT) risk management and apply to every customer. The risk management in this regard is the classification of risks appropriate for each customer taking into consideration the factors prescribed in principle by the law, in combination with other factors which may be added by the reporting entity under internal policy of the organization in order to conduct enhanced examination commensurate with the risks level of customers.

The risk management process for customers must be carried out at all times until the termination of business relationship, whereas the risk management for customers will be carried out for the first time and should be completed at the time the reporting entity approves the establishment

of relationship, followed by regular monitoring. For the risk management in the next stage, apart from depending on the standard prescribed by the reporting entity, it also depends on the circumstance of the relationships, making of transactions, and business movements carried out by the customer. If the customer has unusual behaviors or suspicious transactions, leading the reporting entity to assume that there is a high chance of committing predicate offense or money laundering, the reporting entity must undertake risk management by immediately re-assessing such customer risks based on the most up-to-date information.

## **2.1 Principle for determining risk factors in customer risk assessment**

In setting out the measures for ML/FT risk management, the reporting entity must determine risk factors for all categories of customers (i.e. natural person customers and legal persons or legal arrangements. If the customers are grouped by service category, risk factors for assessing customers by service category must also be defined). The reporting entity must have a clear solution in the case of conflicting risk factors on single customer, for example, a customer's information and nature match low risks factors and high risk factors at the same time.

### **2.1.1 Identifying the definitive factors for assessing customer risks**

In the case that the customer has certain information, the reporting entity must refuse to establish relationship, to carry out occasional transaction or to start freezing the assets without having to use any discretions to mitigate the risks, namely:

“Factors relating to the name lists related to terrorism and financing of terrorism as prescribed by the law”

In the case where the reporting entity finds that the customer is the designated person related to terrorism or financing of terrorism as follows:

- The person designated under the CTF law: there are two categories of designation, namely:

Part 1: Information of the person related to terrorism and financing of terrorism and designated by court order;

Part 2: Information of the person related to terrorism and financing of terrorism under the resolutions of the Security Council of the United Nations whose name is verified by AMLO and approved by the Minister, including information from foreign sources as verified by AMLO and approved by the Minister.

### **2.1.2 Identifying the high-risk factors for assessing customer risks**

In identifying customer risks, the reporting entity must consider the following key factors: If the customer has one or a combination of risk factors, the said customer thus poses high-

risks of money laundering and financing of terrorism. However, it may be necessary to take various factors into account before determining risks.

#### **2.1.2.1 Involvement with serious offenses**

In the case that the reporting entity finds that the customer is related to the commission of serious offenses, specifically the predicate offenses under the AMLA (except for relating to financing of terrorism under the CTF law), including having involved in the commission of offenses, or having been adjudged or punished owing to the offenses.

In this case, the reporting entity may refuse to accept the customer (i.e. by not establishing business relationship) or terminate the business relationship should it be found that the customer poses high ML risks or may have committed predicate offenses.

#### **2.1.2.2 Information on asset seizure or restraint and the forfeiture order**

In the case that the reporting entity finds that the customer is the person whose assets have been seized or frozen by AMLO or forfeited by court order (under the AMLA), the reporting entity must classify the said customer as high-risk level customer since the person may possess property connected with money laundering.

In the case that the reporting entity finds that the customer's assets are under seizure or restraint (under the CTF law), the reporting entity is obliged to take actions in accordance with the CTF law against such customer, namely, freezing the transactions of payment, transfer, disposal, returning to the customer or third party and reporting to AMLO under the prescribed rules and procedure (the CTF law) without delay.

#### **2.1.2.3 Politically exposed person**

In the case that the reporting entity finds that the customer is a politically exposed person whether at domestic, foreign or international organization level, the reporting entity must identify the said customer as high-risk customer. According to international standard, the politically exposed person is most exposed to corruption and bribery<sup>3</sup>. Thus the politically exposed person must always be identified as high-risk customer and also subject to enhanced due diligence process regardless of risk levels of the products or services being used.

The term 'politically exposed person' under the provisions of the ministerial regulation as well as the international standard is broad but there are some specific characters as follows:

---

<sup>3</sup> And in order to be consistent with the U.N. Convention on Anti-Corruption (UNCAC, 2003)



(1) A domestic and foreign politically exposed person should cover the person assuming position in the state agency or state organization, national level politician, interested person in important national affairs, such as:

- The public official in central and provincial administration holding highest level of state agency at ministerial, bureau, department level, including military and police official at highest rank or highest commanding position or closely related to interests in the organization at the level of department, regional or central organization of every service, high-level public prosecutor and high-level judicial official;

- The person assuming political position or political appointee at national level, for example, member of the government, political advisor, member of important state council and independent commissions established by the constitution;

- The high-level executive or executive committee of public organization, state enterprise or organization operating commercial business in which the state has interests;

- The closely-related person (spouse, child, parents) or the person related by means of business (being or previously being business partner or possessing property on one's behalf, etc.) shall also be deemed to be in the same group as the person having political status;

- The person formerly assuming the above position and already leaving the said position not exceeding one year and/or finding that one still having important role in politics or in national administrative affairs.

In this regard, the consideration may be made to include the religious leader or social leader having important role in setting the direction or faith of large number of followers in the society (may depend on the culture in such country or in such situation).

(2) In the case of a politically exposed person having prominent functions in international organization

Consideration should be made to the high-level executive or executive committee or the person in the position with the opportunity to be connected to interests of international organization.

In this regard, the international organization which should be considered is the organization consolidated by national-level representatives from many countries and having huge finance irrespective of its establishment objectives.

#### **2.1.2.4 High-risk professions**

The types of high-risk professions are defined in the guideline prescribed by the Secretary-General. The list of professions will be in accordance with each national risk assessment. Therefore, the types of risk professions may be changed when such professions have AML/CFT measures in place and been supervised adequately and efficiently. Therefore, the reporting entity has the duty to check the list of high-risk professions upon receiving notification from AMLO.

This factor is not deemed definitive. Should the customer have other information that helps lessen the risks, such customer risks can be lowered accordingly.

#### **2.1.2.5 Area and country risks**

High-risk area and country is defined in the guideline prescribed by the Secretary-General based on the official assessment of the Financial Action Task Force (FATF). In the case where risk areas are located in the country, AMLO will designate the area in accordance with the grave situation relating to predicate offenses and terrorism or financing of terrorism in the period during which such cause still occurs or is carried on. Therefore, the information of the area and country having risks may be changed in accordance with the announcements of the international organization and AMLO as may be the case. Therefore, the reporting entity has the duty to check the list of area and country of risks upon receiving notification from AMLO.

This factor is not deemed definitive. Should the customer have other information that helps lessen the risks, such customer risks can be lowered accordingly.

#### **2.1.2.6 Risks under other situations**

In the case of special circumstance causing the risks on money laundering or financing of terrorism or the risks from the commission of any predicate offense or having information useful for examination of customer whom the reporting entity should consider as essential factor in the due diligence process under the ministerial regulation, AMLO will notify the said information in accordance with the procedure prescribed by AMLO, such as, the analysis of suspicious transaction report submitted by each reporting entity to AMLO, etc.

It is essential that the reporting entity takes this factor into consideration when determining customer risks.

#### **2.1.2.7 Intended purposes and use of products or services**

Apart from numerous factors above, the reporting entity should also consider using the risk factors on the products, services and service channels which are in the process of internal risk management together with the risk factors in this part. This will be helpful for determining in case of the customer having several common factors.

### **2.1.3 Identifying low-risk factors for assessing customer risks**

Identifying low-risk customer will help reduce the burden of risk management for the reporting entity from the first stage of establishing relationship. Factors for considering low risks may be divided into two groups as follows:

Group 1: Low-risk customer group prescribed by AMLO

Group 2: Low-risk customer group determined by the reporting entity under the provision of the law

The difference of these two low-risk groups is, namely, in the case of establishment of relationship with low-risk customer as prescribed by AMLO, the reporting entity can examine customer's identity from identification information without having to request additional in-depth information of the customer (except when finding the conduct of high-risk transactions or having the pattern of unusual transactions). However, In the case of the customer in Group 2, the reporting entity is duty bound to carry out initial risk assessment in order to request additional information and is duty bound to use the discretion whether or not is it necessary to request additional information.

Apart from this, the reporting entity must set out criteria for adjusting the customer risks from low to higher risk level upon finding additional information from carrying out the relationships as detailed below.

#### **2.1.3.1 Factors or characters of low risk customers as prescribed by AMLO**

AMLO will prescribe characters of low-risk customers in accordance with enhanced supervision, low risks owing to structure of the customer and international standard guidance. The prescribed information will assist the reporting entity to omit the use of discretion in customer identification (except when finding the conduct of high-risk transactions or pattern of unusual transactions) and classify the risk levels under normal process since the information in this part has been initially assumed by the law to be the information having low ML/FT risks. However, the reporting entity may conduct examination of customer identity and risk management as it is not prohibited by law. The notification of this customer group's information has the objectives to reduce the reporting entity's burden in carrying out the process of customer due diligence, not to issue the regulation or prohibition.

According to the results of analysis and ML/FT risk assessment, the strength in supervision, efficiency of internal audit system, the probability in involving with money laundering or the commission of predicate offenses, it is found that the customers in the group as follows have low ML/FT risks.

(1) Being the government, central administrative service, provincial administrative service, local administrative service, state enterprises, public organizations or other state agencies;

(2) Chai Pattana Foundation, SUPPORT Foundation under patronage of H.M. the Queen and Saijaithai Foundation;

(3) Being the financial institutions as follows:

(3.1) Bank of Thailand, commercial banks and banks established by special law;

(3.2) Finance companies, credit foncier companies and asset management companies;

(3.3) Legal persons operating futures trade business;

(3.4) Legal persons operating futures agricultural commodities trading business;

(3.5) Securities companies;

(3.6) Asset management companies;

(3.7) Casualty insurance and life assurance companies.

(4) Being mutual funds, provident funds, private funds established under the rules of Office of Securities and Exchange Commission;

(5) Being public companies listed on the Stock Exchange of Thailand (which are subjected to disclose information under the rules and regulation of Office of Securities and Exchange Commission);

(6) In the case of foreign customers, the reporting entity may define the customers having the characters under (1), (3), (4) and (5) who hold other nationalities or are located abroad as low risk customers if there are credible measures or processes in the examination that the said customers (i.e. customers who are governments or representatives of any one country) have been evaluated by the Financial Action Task Force (FATF) or other bodies authorized by the FATF that their AML/CFT evaluation met international standard or complied with the FATF recommendations (i.e. not countries included in the watch list) or being under the supervision of the governments or reliable AML/CFT supervisory agencies of the said countries. In this respect, the reporting entity must regularly conduct the examination of reliability of the said group of customers in order to be certain that the customers should still be classified as low-risk.

Apart from the group of customers, AMLO also prescribes certain products or services as low-risk products and services, namely:

(1) Casualty insurance;

(2) Group life assurance and life assurance paid only when the insured died;

(3) Group insurance having the objectives for benefits of the employee or for remedy of damages;

(4) Fund having the objectives of savings for the elderly and underprivileged persons with a limit in purchasing or obtaining the right in using the services;

(5) Financial products for poor people as supported by the state and having a limit for each customer.

In order to prescribe the customers using the products and services above as low risk customers under this item, it must be certain that the said customers have not carried out transactions with other products or services not also in the group of products and services having high risks included and not having incorporated the characters or factors relating to high risks.

### **2.1.3.2 Guideline for the reporting entity in determining low risk factors**

Apart from the low-risk factors notified by AMLO in line with the national risk assessment, the reporting entity may consider identifying the low-risk factors for the customers by itself but it must not be contrary to the guidelines as follows:

(1) The customer has no other factors indicating toward risks at high level (see Clause 2.1.2: Identifying the high-risk factors for assessing customer risks);

(2) The customer's financial transactions in terms value and frequencies are low;

(3) The customer uses only low-risk financial services or products (see Clause 1.1: Risk management of products, services and delivery channels relating to the use of equipment or technology, and Clause 1.2: Assessment of product or service risks);

(4) The customer has no unusual conducts or never acts in any way that led to suspicious transaction reporting.

The reporting entity must have an adjustment to customer risk level should the customer no longer come under the conditions to consider for low risks.

## **2.2 Use of discretion in customer risk assessment**

Just like the use of discretion for staff officers in the assessment prior to requesting additional identity information upon customer identification, the reporting entity must clearly set a guideline for its staff in using discretion at the stage of customer risk classification as this will have long-term effects on the customer whether enhanced monitoring on customer transactions or ongoing relationship is required.

In classifying customer risks, risk factors should be determined in discretion, while the use of power should be flexible by allowing the responsible personnel to use discretion in analyzing all aspects of information of the customer who has several relevant factors, both low risks and high risks, before making final conclusion about that customer's risks.

### Example

The reporting entity must have internal measures/guidance/rules in place for ML/FT risk management for its officers who have the duty relating to the assessment of risks level of the customer which must be completely carried out at the time of customer acceptance.

Stage 1: Examination of customer identification: Upon obtaining customer's identification information and assessing customer risks for requesting additional information, the responsible officers must be certain that the customer's identity has been completely checked, specifically the

legal persons or legal arrangements which are subject to more scrutiny than natural person customers (in the this stage, the customers must have already passed the process of examination on risks related to products, services and channels of delivery of services).

Stage 2: In the first case: risk assessment for the customer not required to provide additional information

If, in the stage prior to customer identification, additional information is not required due to having initial risks at low level, i.e. the customer is an entity listed in low-risk group as prescribed by the Secretary-General or the customer is classified under the factors determined in the measures/guidance/rules issued by the reporting entity, The responsible officers may consider the customer to have low-risk level except when finding the customer having factors relating to high risks. An example of this is when a natural person customer did not disclose in the identification information that he/she is a politically exposed person, but it was found during examination of questionnaire or information form that the customer has ticked in the box “Have submitted asset and liability accounts to the state agency owing to having connection with the person holding political position or the person holding high-level position.” By this, it was revealed that the customer is in the group of persons having political status (closely related person) and, this, classified as a high-risk customer although he/she has several low risk factors.

Stage 2: In the second case: risks assessment for the customer required to provide additional information

If, in the stage prior to customer identification, it was found that additional information is required from the customer, the responsible officer must examine additional information, such as, information of the establishment of natural person customer who is owner of the business, information on the beneficiary of the customer, information on the second source of income, etc., and linking all customer information with the risk factors determined by the reporting entity in its measures/guidance/rules. This group of customers may be classified into low-risk type, should it be found that there is no connection with any high-risk factors.

Stage 3: Determining customer having multiple risks factors

In the case of finding that the customer having both low-risk and high-risk factors, the officer responsible for classifying the risk level must consider the risk ratio as the key criteria as follows:

A natural person having high-risk factors related to the source or income and the category of services but also having low-risk factors on transaction limits, the discretion shall be used by consideration of risk ratio.

For example, the customer being employed in a high-risk country and using cross-border money transfer service for making transactions in low amount of money less than fifty thousand baht per month, it shall be considered that the low-risk ratio may have higher chance of changing than the changing of high-risk factor, namely, the customer may have more chance to make transactions at

higher amount of money but has lesser chance to change the source of income and service category. Thus, the customer carries higher ratio of high-risk factors than low-risk factors. However, as the customer stated the intended purpose at the establishment of relationship that he/she wishes to make transactions in the amount of 30,000 baht per month for expenditures of the family in Thailand, hence, the officer may use discretion in two ways as follows:

- First option: Identifying risk level of the customer as low risks and setting the transaction limits for adjusting the risks at 50% (which means that should the customer make a transaction 50% higher than the regular amount, the customer risks shall be adjusted to the medium or high risk level, etc.) or

- Second option: Identifying risk level of the customer as medium or high risks (depending on internal rules of the reporting entity) and setting the conditions to reduce the risks (For example, should the said customer make transactions in normal amount throughout the period of 12 months, the risks shall be reduced to low-level, etc.).

In case of using discretion with regards to other facts.....

Stage 4: Approving customer risk assessment: the reporting entity should have a screening process to recheck the customer risk assessment conducted by its officer, specifically when the customer has been assessed as medium or high risk. This screening process could be done by higher level staff or executive level or setting up a task force.

Stage 5: Approving acceptance of high risk customer: the reporting entity must have the process for approving acceptance of high-risk customers by appointing the executive or task force in which executives are member to consider information of the customer prior to approve the establishment of relationship as high-risk customers pose the reporting entity at higher risks of money laundering and financing of terrorism than other customers. The executive should be aware of the proportion of high-risk customers at that time. It should be understood that if the reporting entity has a high proportion of high-risk customers as compared to the total number of customers, the burden for examination and monitoring of financial movements and the transactions of the said group of customers will increase. Besides, the reporting entity is more vulnerable to misuse for money laundering and financing of terrorism.

Stage 6: Refusal for establishment of relationship with customer: the reporting entity should have the process in place in obtaining approval from the executive in the case that the responsible officer indicated that a customer acceptance will pose ML/FT risks on the reporting entity, thus, suggested that business relationship be rejected. This means that the staff finds sufficient information or facts to suspect that the said customer may be connected with money laundering, financing of terrorism or predicate offenses or have numerous high-risk factors such that it poses the reporting entity at risk of being used as the channel of money laundering or financing of terrorism. Therefore, it is necessary to appoint the executive or a task force (with the inclusion of the executive) for

consideration and approval. The reporting entity must also consider whether or not a suspicious transaction report should be submitted to AMLO.

### **2.3 Principle of ongoing customer risk management**

The reporting entity must continuously undertake ML/FT risk management, specifically customer risk management. The assessment so as to classify the risk level extends beyond the customer acceptance stage to include the carrying out of business relationship stage until the termination of relationship. Therefore, the clear measures/guidance or rules concerning customer risk management must be prescribed as follows:

2.3.1 The ongoing customer risk management must be consistent with the monitoring process for examining financial movements or the making of transactions of the customer

Whereas the principle must be prescribed such that the assessment classifying the risk level of each customer will be used for determining the intensity of the examination and monitoring of customer's financial movements or transactions or relationships under the principle that "the group of customers at low-risk level shall be subjected to the process of examining and monitoring the financial movements or transactions with less enhancement than the group of customers at high-risk level".

2.3.2 Updating of customer information as an essential element in risk management

Reporting entity must examine the risks of customer upon receiving new information from the customer. Therefore, there must be a scope for regular revision of customer information which may be based on the same principle as Clause 2.3.1, namely, carrying out the revision of information for the group of customers at low-risk level may be less frequent than the process of revising information for the group of customers at high-risk level.

2.3.3 Revision of risks in accordance with the assessment of financial movements or transactions or relationships

The reporting entity must set out conditions or patterns relating to the results of examination of financial movements or transactions of customer which will be used as a basis for revising the risks of customer, such as, identifying percentage of transaction limits when the customer having financial movements different from the original or identifying the pattern of transaction execution when the customer having movements in transaction execution different from the original. Therefore, criteria for reducing or increasing the risks level of customer should be in place.

2.3.4 Report to the executive when adjusting the risks level of each customer to high risks

The reporting entity set up a procedure for reporting the results of analysis or assessment and request approval from the executive or task force in which the executives are members when adjusting customer risks to high risks (in this respect, the reporting entity may also set the process of reporting to the executive when adjusting customer risks to other levels). The reporting



entity may assign the executives having positions in hierarchical order in accordance with the levels of the assessment, such as, in reducing risk level, approval shall be obtained from mid-level executive; in increasing to high risk level, approval shall be obtained from high-level executive.

#### 2.3.5 Recording information of risks management

The reporting entity shall record information and data concerning each revision of risks of each customer and make them available for future use, e.g. in the examination whether or not the present measures of risk management have the tendency to increase the number of customers having higher risks, thus indicating the need to revise the measures/guidance/rules on risk management of the organization.

The ML/FT risk management of the persons obliged to comply with AMLA (including also the CTF law), includes also internal audit specific for the compliance with the measures on AML/CFT. The internal audit examines the compliance unit, performance of the tellers, the stage of risks management, the stage of monitoring the business relationship, the stage of examining the information accompanying electronic fund transfer order, the stage of examining the agents and reliance on third person, supervision of branches or affiliated companies, including the system of efficient storage of information.

## **Customer Due Diligence (CDD)**

(Examination and verification of customer's financial movements or transactions)

Customer due diligence (CDD) herein means steps to examine customer's financial movements or transactions or movements in customer's business relationships. These steps are a key part in the process of CDD. They inform us of the extent to which each customer carries risks of money laundering and financing of terrorism, and how to take risk management measure suitable for each customer.

Examination and verification of customer's financial movements or transactions or movements in customer's business relationships is a step that the reporting entity must take after establishing relationships and categorizing risk levels, and this process must be continued until the termination of relationships.

### **1. Objective of CDD**

The reporting entity must understand the following objectives in order to set forth the method of examination and verification of financial movements or transactions or business relationships appropriate for the customer and their own business.

(1) To find out that the customer is still carrying out normal relationships with the reporting entity, with no behavior or suspicious activity such as carrying out the same pattern of transactions, having a normal frequency of transactions or a frequency consistent with the period of initial relationships or with that examined and recorded in a previous round;

(2) To find out that the customer is still carrying out relationships in line with the objective declared in the process of establishing relationships, or no other hidden agenda is found which may deviate the course of relationships (which can be seen from overall financial movements or transactions under (1) and the request for establishing additional relationships in other services or products);

(3) To find out that the value of the customer's financial movements such as investment value, transaction value, the average value of money revolving in the movements of the customer's relationships is still at the same level or whether it shows an unusual increase in value;

(4) To find out whether the customer's information may have changed and has not been reported to the reporting entity, or whether the reporting entity must enquire after or examine customer's current information to find cause or correspondence with examination results from (1), (2), and (3) such as information on source of funds or income, occupation, political office holding;

(5) To find out whether the customer should enter a process to adjust risk level. If results from (1) - (4) show no change or are normal, there is usually no need to adjust the customer's risk levels. However, if results from (1)-(3) be it only one or several show change, this might result in the adjustment of the customer's risk level;

(6) To find out whether the reporting entity should continue carrying out business relationships with the customer or should end the relationships

## **2. Specifying CDD Method**

The reporting entity must specify the method for examining movements in relationships with the customer which is in line with the customer's business type or transaction type. The method to examine information must be specified as follows:

### **(1) Examine customer's transaction value throughout the course of the business relationships**

The reporting entity must specify method to examine or analyze money limit in customer's transactions from the start of the relationships. After a period of carrying out the relationships, the reporting entity must go over transactions from the period of the beginning of the relationships to the period where the examination takes place and must be able to conclude the value or the figure or the average money value for transactions in said customer's transaction period to be used as the basis for the next evaluation whether the customer continues to have overall transactions which are equal to or close to the value or figure or level estimated previously. If there is a clearly noticeable change, the reporting entity must specify steps in verifying related information in order to analyze which factor is related to the new changed value or average and whether to increase or decrease risk level. Methods in this step must be in line with the type of service provision and the method of relationships carried out between the customer and the reporting entity.

#### Examples:

(1) The reporting entity providing service to the customer mainly through electronic network may specify method to examine customer's transaction value by focusing on money value transfer and giving less importance to E-payment, etc.;

(2) The reporting entity provides business service where the customer has frequent movements. The reporting entity cannot assess results from transactions in one short period of time. The reporting entity must have a method to assess the whole transactions in a period long enough to see the customer's average transaction value and to estimate an average or;

(3) The reporting entity provides one-off business service or in the form which the customer has no time to carry out relationships under conditions resulting in few transactions made by the customer, or one-off transaction which has lasting binding effect. The reporting entity does not need to apply the method under Example (2), but is to have method for examining suspicious behavior related to occasional transactions.

### **(2) Examine customer's transaction pattern throughout the course of the business relationships**

The reporting entity must have method to examine the pattern of the customer's transactions and specify process to examine the customer's long-term movements to see whether the customer

changes their transaction pattern be it a change as a result of type of financial product, use of service, or choice of service channel because transaction pattern will be used to determine customer's behavior change which affects the customer's risk adjustment.

The reporting entity must have method to examine transactions in line with their business. If the reporting entity provides various types of product, service, or service channel, they must have a system (in this respect including Information Technology (IT) system and operational system) which can record or determine suitable transaction pattern when using each type of product, service, or service channel provided. The reporting entity must be able to analyze the changes in customer's transaction pattern that may create risks related to commission of offense and finally must be able to answer to the question whether "the customer has transactions related to products or service including use of service channel which is different from the beginning of the relationships or from the previous verification and analysis, and whether said change in transactions creates more money laundering risks related to the product, service and service channel than that from the beginning of the relationships or from the previous evaluation".

Example:

In case where the reporting entity provides several services and service channels, it might be found that in the beginning of the relationships, the customer makes a deposit transaction through a domestic branch of the reporting entity but after overall evaluation it is found that the customer has later conducted transactions through automated withdrawal machine abroad. Therefore, the reporting entity must analyze that there is a risk related to use of service channel abroad and examine the extent to which said country carries risks in order to conclude that in this evaluation period the customer has changed his transaction pattern and matches some high-risk factors, namely use of service channel and may be related to risk areas or countries. Having analyzed all information, the reporting entity may conclude that:

- The customer makes transactions different from that stated with the reporting entity at the time of the establishment of the relationships

- The transactions related to service channel has changed: the customer conducts transactions through automated withdrawal machine which carries more risks and the location of the transactions has changed giving rise to higher risks

- The change of the transaction pattern may affect the objective of the relationships. The customer makes transactions in risk areas or countries (after verification with information on risk factors regarding risk areas or risk countries) which results in a change of objective from normal savings to international transactions with "to repay debt" stated in the request

- Other factors have no change

- Suggestion: The time limit for examining customer information may be extended to 15 days. If the customer cannot be reached or if the customer does not give information corresponding to analysis results, the customer's risk level must be adjusted to level ..., for example.

### **Additional suggestions on guideline**

#### **Analyzing transactions making against objective of relationships**

From the examination of financial movements or transactions or course of relationships focusing on threshold and transaction pattern, the reporting entity can see all linkages as the value of transactions and conduct of transactions, either financial products, service types, or service channels, will always be in line with the objective of relationships. The point is whether they will correspond to the objective information stated by the customer at the time of the establishment of the relationships.

If all evaluation results have been determined and found to correspond to another objective different from what stated while establishing the relationships or in the previous evaluation round, the reporting entity must specify evaluation guideline to consider risks which may incur from such increased or changed objective.

The reporting entity should specify linkages of all types of transaction pattern and objective of establishing customer relationships.

#### **Example:**

Savings objective

Corresponds to the following transaction pattern:

Opening deposit account or financial instrument deposit

Depositing cash

Receiving electronic money transfer

Withdrawal in an amount lower than the deposit

Corresponds to the following transaction channel:

Transactions at a branch or office

Transactions through automated deposit and withdrawal machines

Transactions through Internet

Corresponds with the following transaction value:

No transaction value limit. Depends on customer's income.

Investment objective .....

Borrowing objective .....

International debt payment objective .....

Foreign currency exchange objective .....

Securities investment objective .....

Investment in futures trade objective .....

Investing in funds objective ..... etc.

### **(3) Examining other information to complement analysis results from examination and verification**

When the aforementioned steps have been completed, the reporting entity must specify a process to examine other information to find facts to support analysis results in order to evaluate each CDD.

The reporting entity should not specify the type of information to be further acquired, should allow related officer to find information freely, but may specify a framework for finding information especially regarding the credibility of the information.

Example

The reporting entity must specify duties for related officer to find facts or additional information to support analysis results of examination and verification of customer's financial movements or transaction conduct or course of relationships, especially in the following cases:

(1) In the case where analysis results reveal that the customer shows behavior which is different from the conduct of relationships at the beginning or from previous evaluation

(2) In the case where the analysis shows the tendency that the customer's risks should be adjusted to a higher level, the reporting entity should specify guideline for finding credible information or facts to support analysis results.

Example

Officer related to the duty of verifying analysis results of customer's financial movements or transaction conduct or course of relationships should find information or facts to support analysis results in the case where the analysis shows that the customer shows different or unusual behavior. The information or facts used to support the results should be in line with the following principles:

- Be facts acquired through direct questioning of customer
- Be information or facts acquired from the department overseeing products or services within the organization
- Be information or facts legally acquired from other financial institutions
- Be information or facts legally acquired from a credible source such as database the state or the same business sector has created under agreement
- In the case where the officer is not sure whether the information obtained is credible or not, the officer should specify the source and opinion that the information is obtained from an open source and should use several information sources to corroborate the information

..... etc.

### **(5) Summarizing evaluation results**

When the above steps have been completed, the reporting entity must specify a step to summarize evaluation results. Said summary must undergo examination and verification by related officer together with the superior in order to affirm that the said process has been carried out appropriately.

In summarizing evaluation results, the reporting entity must answer the following questions:

(1) Whether said customer's financial movements or transaction conduct or course of relationships has changed, especially regarding value of transactions and transaction pattern or behavior in the carrying out of relationships, and the extent of the change

(2) If the result in (1) leads to customer's risk adjustment (as appropriate to the overall customer structure), which factors contributed to the need to adjust customer's risks. After acquiring further information and facts, whether it can be confirmed that the factors found should lead to adjust customer's risk level.

(3) Should customer's risk adjustment enter the approval process by the chief supervision department

(4) Whether relationships should continue. If not the reason must be shown whether the customer's risks will affect the organization's operations and may be related to offense under the AMLA (money laundering offense or predicate offense or offense related to CTF law). If it can be believed that the customer's business relations should be related to offense or shows extreme unusual behavior for the same customer group using the same product/service/service channel, the officer should submit a summary report to high-level management to file a suspicious transaction report with the AMLO.

Records on CDD of each customer must be kept 5 years from the date relationships with the customer are ended.

## **3. Specifying Steps to Approve Evaluation Results and Record Evaluation Results**

### **Approving evaluation results**

The reporting entity must specify a process of consideration and approval by chief of supervision department in case of the following findings:

(1) The customer's conduct of transactions necessitates a high level of risk adjustment and/or filing STRs to the AMLO.

(2) The customer's conduct of transactions led to the necessity to end relationships which would due to high risks of affecting the organization's operations (specify cause of risks) and/or may necessitate filing of STR to the AMLO.

The reporting entity may authorize high-level manager or a committee who has the authority to sign to approve evaluation results before proceeding to adjust risks or end relationships or file STR to the AMLO, as the case may be.

**Recording information**

The reporting entity must record information and store the following information for 5 years from the date relationships with the customer are ended:

- (1) Information related to examination and verification of the customer's financial movements, transactions, or course of business relationships
- (2) Analysis and summary of evaluation results
- (3) Information on whether it is approved or not and the result affecting each customer's risk management

All the key information in this section applies to regular CDD. In case of simplified CDD and enhanced CDD processes, use principles in the next sections specifically referring to said processes.



## **Enhanced Customer Due Diligence (CDD) for High-Risk Customers**

Customer due diligence (CDD) for high-risk customer refers to a rigorous and robust process to deal with customer identification, risk management, monitoring of financial movements or transactions and revision of the customer's information step.

In applying the CDD process to high-risk customer, hereinafter, will be referred to as "enhanced CDD", reporting entity must have a policy or measure or standard on risk management by identifying risk factors which are in line with provisions in the CDD Ministerial Regulation and related notifications. In establishing enhanced CDD process, the following steps in line with this guideline are:

1. Enhanced identification and verification of customer's identify
2. Risk management to categorize high-risk level
3. Enhanced examination of financial movements, transactions, or the carrying out of relations

### **Step 1: Enhanced identification and verification of customer's identity**

#### **Step 1.1: Requesting information for enhanced identification and verification of customer's identity**

As previously stated under the subject "customer approval", reporting entity must have steps to determine whether the customer requesting the establishment of relations should be required to give additional information, aiming at assessing whether the customer has a high-risk of money laundering and financing of terrorism. See examples of conditions or factors in guideline regarding approval for customer acceptance (assessing needs for additional information from customer).

In the case where reporting entity found that additional information is required from the customer due to the set conditions, for example, the customer stated intended purpose for relationship and requested high-risk service, or customer is a legal person whose beneficial owners have a complex structure and use high-risk services or large amount of money value, or the customer stated in the document that he holds a political status or are related to a politically exposed persons (see guideline regarding approval for customer acceptance: assessing needs for additional information from customer), reporting entity must set out guideline for its officers to obtain information or verify customer's information regardless of being a natural person, legal person, or legal arrangement.

##### (1) Intensity of requesting information of natural person customer

In the case where the customer is a natural person and reporting entity initially assessed that said customer should be subject to further verification which may be due to the suspicion that the customer is acting on behalf of another person and not disclosing authorization; or the customer has information matching a well-known person with political status or gives employment information as a

holder of high-level position or political office; or the customer wished to establish relationship or use high-risk services which do not correspond to income level stated in the application; or the customer matches certain conditions specified by reporting entity.

The reporting entity should request additional information or other information which can be used to assess the customer's ML/FT risk as follows:

(1.1) Information regarding source of income (both main source and other sources)

(1.2) Information regarding beneficial owner (in the case where it is suspected that the customer may be establishing a business relationship for other person's benefit)

(1.3) Specific objective in establishing relationship (in the case where it is suspected that the customer requests service for a certain objective such as international money transfer service aiming at making profits from the strengthening or the weakening of foreign currency, or an opening of account to invest in certain business as a natural person, for example)

(2) Intensity of requesting information of legal person customer or legal arrangement

In the case where the customer is a legal person or legal arrangement and reporting entity initially determined that said customer should be subject to further verification which may be due to complexity of its structure; or list of executive board is related to politically exposed persons; or when customer requesting the establishment of relationship or services with a very high money limit or high-risk; or the customer matches the conditions specified by reporting entity, for example,

Reporting entity should request additional information or examine other information for assessing customer's ML/FT risks as follows:

(2.1) True objectives of the customer's activities (in the case where it is found that the customer has several activities which generate main and additional income or customer does not state clear objective in his application)

(2.2) Customer's important structure, i.e. the key structure that operates the business such as structure of principal shareholders or structure of management from high level to operational level or structure of company and subsidiaries. This information will be beneficial for the examination of the customer's beneficial owner and credibility of the customer's business operations.

(2.3) Top executive, i.e. information of natural person or group of persons operating in management position and has the highest authority to establish policy or drive said legal person. This may be person holding position which has important authority regarding customer's operations and finances. At least the information that should be acquired is full name, identification number or nationality which allows verification with the list as specified by law, including other database which is beneficial to the customer's risk management (see notification issued by virtue of ministerial regulation on guideline in customer identification and customer's beneficial owner).

(2.4) Beneficial owner (or ultimate beneficiary) which is a natural person: Reporting entity must set out procedures for examination or request of information from the customer in line with the law and international standard, at least including:

(2.4.1) Related officers shall examine document or evidence of shareholding which shows the receiving of benefits in appropriate percentages, taking into account the standard or guidance followed by reporting entity in the same business type in the country or abroad.

(2.4.2) In the case where it is not possible to examine by the above means, related officers are bound to use effort to find controlling person whose information may not appear in official documents. The officers may search for the information from facts or other information which does not need to appear in official documents or official database, but may come from public or other information sources. The officers may indicate credibility of information sources together with the recording of information (for example, retrieved from website or article in journals with no official certification).

(2.4.3) In the case where all the above methods are not helpful for the validation of the beneficial owner, a guideline should be set forth for the officers to use judgment that the customer's beneficial owner may be one or many natural persons with the authority to control the customer's business. It should be specified that this information examination is based on assumption since it cannot be discovered from other methods. So reporting entity can further examine transactions made between the customer and outside persons, and if these transactions were highly frequent in high amount, such person may be related to the customer's beneficial owner.

(2.4.4) It is proper to set out other methods of examination, but only after the aforementioned methods have been exhausted. In the case where reporting entity requested that the customer identify beneficial owner, the reporting entity's officer must examine or identify linkages or relationship between the customer and its beneficial owner.

(2.5) Income or financial source related to the customer means area or country where the customer operates business or is a joint venture or the place where customer's commercial partner or investment source is located.

Reporting entity may have its officers request further information other than that aforementioned for the benefit of managing ML/FT risk.

### **Step 1.2: Process to verify customer's identity**

After step 1.1 has been completed, reporting entity must have measures to verify and validate the customer's identity which includes a step to verify the facts and credibility of the customer information and a step to validate it with list of names as stipulated by law.

#### (1) Step to verify customer's information

Reporting entity must have standards for its officers to verify information or facts informed or exhibited by the customer. Level of credibility should also be specified as a basis for judgment; conditions and guidance should be in place in case of obtaining false unreliable or incomplete information.

#### Example

- Credibility level 1: Information which reporting entity has verified by state agencies or certified by state agencies or official documents or copies of documents certified by state agencies

- Credibility level 2: Information accredited in accordance with international standard for business undertaking (such as certified by an authorized or credible person or organization); information verified by credible service provider.

- Credibility level 3: Information which reporting entity has acquired, verified and validated according to internal rules and determined that it should be kept as customer record (such as information found from public database on the Internet or from customer's internal information which the customer was requested to use as reference).

(2) Step to validate with list of names as stipulated by law

Reporting entity may consider taking this step either before or after the information has been verified in step (1) above. But taking the step after verification helps ensure that the information validated with the list of names as stipulated by law is reliable. Reporting entity must validate list of customer and beneficial owner, all board members with authority, management with executive power. In the case of an insurance policy where the beneficiary of the policy is identified, the reporting entity must also verify the beneficiary (If found a list of natural persons or legal persons or legal arrangement which is related to the customer's establishment of relationship or key risk factors, reporting entity should comprehensively validate them with list of names as stipulated by law):

(2.1) List related to terrorism and financing of terrorism according to the CTF Act, 2013 which is subject to stringent verification by the provision of the law (see guideline regarding approval for customer acceptance: examination with name list information prescribed by the law).

(2.2) List related to terrorism and other serious offense specified by other agencies apart from (2.1) which reporting entity considers that the information is reliable and should be verifies with the customer's information. The reporting entity should conduct enhanced CDD if the list is identified by these agencies as a high-risk list, thus posing the reporting entity's ML/FT risks, in particular for the reporting entity who is obliged to examine list of other countries where a branch or subsidiary, commercial partner, agent is located (this is optional and is not stipulated by law).

### **Step 1.3: Refusal after identification**

After identification in step 1.2, reporting entity must conduct assessing the risk level of each customer so as to examine movements and other processes appropriate to said risk assessment except:

Case 1: When it is found that the customer, beneficial owner, one of executive board members, management with executive power, including beneficiary of insurance policy or person with an important role to the customer has been listed (according to the CTF Act, 2013), reporting entity must proceed as follows:

(1) Refuse the establishment of relationship with the customer. The customer's information which has been examined is to be kept including copies of evidence or document provided by the

customer for the benefit of providing information to the AMLO (according to the AMLA and CTF law). Reporting entity may return the evidence and documents to the customer (after customer's information has been copied).

(2) Report as a STR to the AMLO according to the AMLA.

(3) Report information to the AMLO according to the CTF law

Case 2: When reporting entity has determined that although the customer does not have information matching the list specified by the law but has information or facts which may cause reporting entity to risk of violation of the AMLA or has an extremely high-risk to potentially cause reporting entity to become part of the ML/FT syndicate or cause impact on its business and legal issues from headquarters abroad, subsidiary companies or commercial partner business operator abroad, the reporting entity may consider as follows (this is up to reporting entity's judgment. However, the judgment should be based on ML/FT risk assessment):

(1) Refuse establishment of customer relationship (not required to keep or make copies of information provided by the customer. But this can be useful when the reporting entity has to file a STR with the AMLO).

(2) If there is a suspicion that the customer may be related to money laundering, predicate offense, file a STR to the AMLO according to the AMLA.

## **Step 2: Risk Management to Categorize High-risk Level**

For reporting entity to undertake this step, reporting entity must have policy or measure or standard to manage risk including factors to consider the customer's risk (see ML/FT risk management section).

In principle, most customers undergone enhanced CDD would match with high-risk factors. When they enter this step, they can either be assessed as normal or high-risk customers (depending on other information and classification of risk levels and risk factors by each reporting entity). But mostly they will not fall in the group of low-risk customers because if their characteristics match low-risk factors they will not enter the enhanced CDD process in the first place, except information matching high-risk factors is later found.

Risk management when risks are high must be in accord with the verification of customer's identity:

(1) Customer has information or facts matching high-risk factors and there are no other low-risk factors which can reduce the high risk. For example, it is evident that the natural person customer has established business relationship for another person's benefit and has investment objective in a very high amount or it is found that legal person customer has business objective which is a high-risk profession and related to higher risk areas or countries related to money laundering and financing of terrorism and using high-risk services.

(2) Customer has information or facts matching highest risk factors (see this type of factors guideline regarding money laundering and financing of terrorism risk management: high-risk factors). For example, the customer is a politically exposed person (domestic, foreign, or international PEPs) or customer is named as the persons whose assets have been seized or frozen or transactions suspended or forfeited to the state, or legal person closely related to list of persons whose property has been attached according to the CTF law.

**Step 2/1: Approval from senior management having decision power at important steps**

Since the identification and risk management in the first time are usually carried out in tandem or in a close period of time and must be completed before the approval for customer acceptance and/or performing the first transaction, reporting entity must have the following special principles for acceptance of high-risk customers:

(1) Require that such customer acceptance must be approved by senior management with authority, who acts as the representative of the corporation's management committee who should use their authority to decide whether or not to accept high-risk customer in the final stage. Before granting approval, said senior management should receive sufficient information related to the said customer.

(2) Require that senior management with authority is the final decision maker in the refusal and termination of relationship according to AML measures, including the filing of a STR when refusing or ending business relationship with the customer, or freezing assets and reporting to the AMLO according to the CTF law.

(3) Require that the senior management is responsible for acknowledgment and approval when there are changes to risk level of high-risk customer during the course of verification and monitoring of money movements, or performing transaction or carrying out of relationship, or identification of data or when conducting large-scale transaction or suspicious transaction that could be related to money laundering or predicate offense, and when considering filing a STR to the AMLO.

In the case where the verification and validation found that the customer's information is matching with high-risk factors which may be related to predicate offense or money laundering, reporting entity must present the matter to senior management to approve the filing of STR to the AMLO.

### **Step 3: Enhanced Examination of Financial Movements, Transactions, or the Carrying Out of Relationship**

This step applies to high-risk customer (in the case where reporting entity specifies several high-risk levels, the degree of enhanced examination must be in line with each risk level of high-risk customer).

In the setting out of measures for enhanced examination of financial movements, transaction, or carrying out of relationship, reporting entity must have enhanced measures while taking into account the type or nature of business relationship between the customer and reporting entity:

Enhanced examination of financial movements, transaction, or carrying out of relationship should at least incorporate the following guidance (Reporting entity may undertake all or each of the guidance appropriate to the type of business relationship):

(1) Having enhanced system for screening, verification and validation on transaction, financial movements, or carrying out of relationship with reporting entity against behavior pattern which may be unusual or related to offense when compared to transactions performed by other customers.

(2) Having a shorter or more frequent period for revising past customer relationship.

(3) Requiring enhanced system to examine, analyse and approve report by senior management.

(4) Enhancing the examination and verification of customer's identification especially in the following matters:

(4.1) Income source, source of funds and property which is related to the carrying out of business relationship between the customer and reporting entity

(4.2) Identification of customer's beneficial owner

(4.3) In the case of high-risk customer who is a PEP, the removal or maintenance of the customer's political status should be mentioned (including the case where the customer is a child or spouse or others according to notification under the ministerial regulation regarding politically exposed persons)

Reporting entity may have enhanced CDD guideline on high-risk customer in line with respective customer relationship or add other examination measure other than this guideline, but with due regard to secrecy or tipping-off under clause 8 of the ministerial regulation.

## **Simplified Customer Due Diligence (CDD) for Low-Risk Customers**

The reporting entity shall take into consideration general principles regarding arrangement for customer identification, customer acceptance, risk management, and examination of financial movements, transactions, or the carrying out of relations including record keeping in order to increase understanding about the principles in carrying out customer due diligence (CDD).

The key principle is that the reporting entity has a duty to perform risk assessment on all customers and when considering the standard principle in the previous paragraph it can be seen that the CDD process begins with arranging for customer identification according to basic information stated in the ministerial regulation on method of identification for customer of financial institutions and the professions under Section 16 and enters the process of identification according to the CDD ministerial regulation, 2013. Hence, before performing CDD for low-risk customers according to the ministerial regulation, the reporting entity must arrange for all customers to identify themselves strictly according to the ministerial regulation on method of identification for customer of financial institutions and the professions under Section 16.

### **Step 1: Identification of Low-Risk Customers**

When the reporting entity obtained identification information from the customer and found that:

(1) The customer having been an entity or low-risk business according to the AMLO Secretary-General's notification on guidance for determining risk factors for low-risk customers.

(2) The customer having established relationship for low-risk products or services without connection to other high-risk factors (for low-risk products, services, or channels, see notification issued pursuant to the ministerial regulation on guideline for determining risk factors for low-risk customers).

(3) The customer having nature or characteristics matching risk factors for low-risk customers as specified by the reporting entity according to policy, standard, or guideline within the organization (This must be not contradictory to the provisions by law and related ministerial regulations).

1.1 The reporting entity may simplify the identification process as follows:

Guideline 1: In the case where the customer is a natural person and has no suspicious behavior or has facts falling under (1)-(3) above, the reporting entity may initially consider that the customer establishes relationship for himself (meaning there is no beneficial owner in the establishment of business relationship with the reporting entity). When there are no suspicious facts, it can be assumed that the person has income and intended purpose of business relationship consistent with the type of product or service.

Guideline 2: In the case where the customer is a legal person or a legal arrangement and has characteristics as identified in (1)-(3) and has no suspicious behavior, which means the customer is a



low-risk legal person or legal arrangement according to the nature of entity or characteristics specified in the policy or standard or internal guideline of the reporting entity, the reporting entity may consider to relax the step of examining the natural person who is the beneficial owner of said customer by examining only the information of board of directors which appears in the registration document and other information appearing in the process of identification, and may consider to simplify the request of certain information such as information on business structure and on the top executive if it is certain that the existing information is sufficient to perform risk management process.

### **1.2 The reporting entity may not omit the following steps:**

Step 1: Identification of customer's identity to know whether each customer's characteristics or nature of entity are in accord with low-risk factors specified in the Secretary-General's notification regarding guideline for determining risk factors for low-risk customers. The reporting entity must obtain complete identification information as there is no legal provision to exempt the customer identification step.

Step 2: Step to check with list of names related to financing of terrorism. The law stipulates that the reporting entity must cross examine information of customer, know beneficial owner (as revealed by the customer or found in the shareholding structure), board of directors including board members with signatory authority delegated to establish relationship, the authorized person to carry out activity with the reporting entity, or list of persons or legal persons found in the identification process significantly related to the customer, with the designated list stipulated by law (see guideline regarding approval for customer acceptance). Reporting identity is obliged to carry out its duty according to this step. Failing to comply will pose the reporting entity at risk of violating the CTF law.

### **Step 2: Risk Management and Assessment of Low-risk Customer**

In carrying out this step, the reporting entity must clearly specify policy, standard, or guideline within the organization related to the specification of low-risk factors (see guideline regarding money laundering and financing of terrorism risk management: specification of low-risk factors; also see guideline for identifying factors concerning low-risk customers as announced by the Secretary-General).

In implementing risk management and assessment of low-risk customer, the reporting entity may specify policy, standard, or guideline within the organization as appropriate to the course of business relationship, but must not violate provisions in the ministerial regulation and guideline for identifying factors concerning low-risk customers as announced by the Secretary-General. However, please note that the notification pursuant to the ministerial regulation has the purpose of permitting the reporting entity to adopt and apply the principles for reducing the CDD process, except for the key provisions in the notification that specify how the reporting entity identifies low-risk factors. Hence, if the reporting entity set forth its internal policy for examination of the group of customer as set out in

the said guideline in a stringent manner, the reporting entity can do so and this will not be deemed as violation of the law (but they must not contradict the key provisions of the notification on low-risk factors which allows the reporting entity to set its internal policy).

**(1) Approving low-risk and business relationship**

As mentioned in the risk management process, the reporting entity must complete each customer's risk (first time establishment of relationship) before approving the customer. This means that after the identification process, the reporting entity must carry out ML/FT risk assessment before or immediately at the time of the approval of the establishment of relationship. In the process of approving risk level of low-risk customers alongside the approval of establishment of business relationship, the reporting entity may simply and speed up the process as follows:

(1.1) Require the person with the highest position or senior officer at the branch or office of the reporting entity has the authority to approve risk assessment result and customer acceptance without having to file a report to or seek approval from senior management.

(1.2) Allow low-risk customers to receive faster service than other customer group such as being able to carry out transaction as soon as they have been assessed as low-risk customers or shorten the time for approving the establishment of business relationship.

**(2) Specifying conditions of low-risk adjustment**

The reporting entity should specify policy, standard, or guideline within the organization which states that low-risk customers may have their risk adjusted to a higher level if the customer's behaviors match certain conditions or facts, by applying risk factors of higher-risk customers as a threshold, or referring conditions/facts in carrying out one or many transactions as indicators for low-risk customers to have their risk adjusted to a higher level. The following guideline may be considered:

(2.1) Specify threshold for performing transactions such as in the case where low-risk customer carries out transactions that increase value in his account or more benefits in specified amount or percentage or proportion, the reporting entity should take these facts into consideration whether risk level should be increased. The reporting entity may verify relevant information before adjusting to a higher level or automatically adjust it when the facts conforms with the set conditions.

(2.2) Specify threshold amount for the examination and monitoring of financial movements, transactions, or the carrying out of relations. For example, when examining and monitoring low-risk customer's financial movements, transactions or carrying out of relations, the reporting entity should take into account average value of money in the account or in the business being carried out with the reporting entity. The threshold amount may be specified in a monetary value, percentage, or proportion that changed from previous round of examination.

(2.3) (Condition covered by law) when low-risk customers whose transactions had been filed as a STR to the AMLO and in the event that the AMLO has not confirmed that the cause for reasonable suspicion would not pose any risk, report entity must categorize such customers as high-

risk customers as soon as the reporting entity considers filing report to the AMLO. The reporting entity is obliged to set out this condition in accordance with the provisions in the ministerial regulation.

### **Step 3: Monitoring Financial Movements, Transactions, or the Carrying Out of Relations for Low-Risk Customers**

Provisions in the ministerial regulation require the reporting entity to determine the extent of its monitoring of financial movements, transactions or carrying out of relations in line with each customer's risk level. Hence, when the customer is low-risk of money laundering and financing of terrorism, the reporting entity shall perform a more simplified examination measure for this customer group.

In establishing principle for monitoring financial movements, transactions, or carrying out of relations applying simplified process, the reporting entity may consider the following guidance (they may apply all or each item as appropriate to the type of business relations where practicable).

(1) Having simplified system for screening, verification and validation on transaction, financial movements, or carrying out of relationship with reporting entity against behavior pattern which may be unusual or related to offense when compared to transactions performed by other customers.

(2) Having a longer or less frequent period for revising information of transaction, financial movement, or carrying out of relations with reporting entity than other customer group

(3) Specifying system to approve analysis report which is more relax or less intense than other customer group. The person in the highest position or personnel in senior positions stationed at the branch or office which examines said customer may be empowered to approve the results for this customer group (except when low-risk customers have their risk adjusted to a high level, enhanced CDD measures for high-risk customers must be performed immediately).

(4) Having an examination and verification of identification information which is more simplified than other customer group. The period to update the information or type of information to be examined and verified may be less intense than other customer groups.

The reporting entity may specify its guidance for simplified CDD for low-risk customers other than guideline suggested herewith, with due regard to key principle on risk management, which is "risk can be adjusted and if low-risk customers have their risk adjusted to higher risk, the reporting entity must immediately apply enhanced measures with the customer."

## **Reporting of Suspicious Transactions**

The reporting entity has a duty to comply with the AMLA in the reporting of 3 types of transactions which are:

Type 1: Cash transactions

Type 2: Property-related transactions

Type 3: Suspicious transactions

Rules, timing and procedures for filing each type of transaction report by the reporting entity are set forth in ministerial regulation issued pursuant to the Anti-Money Laundering Act, 1999 (see ministerial regulation issued in 2011).

The key issue to be considered in complying with the ministerial regulation on customer due diligence (CDD), 2013 is related to guidance for reporting of suspicious transactions in which the definition and procedures have been revised.

### **Examining suspicious transaction**

In examining which transaction is unusual and carries risk related to money laundering, predicate offense, and financing of terrorism and should be reported as suspicious transaction to the AMLO, please refer to the definition in the Anti-Money Laundering Act (No. 4), 2013.

“Suspicious transaction” means a transaction with reasonable grounds to believe that it is conducted to avoid the application of this Act, or transaction connected or possibly connected with the commission of a predicate offense or terrorist financing offense, notwithstanding the transaction being single or multiple, and shall include an attempt to conduct such a transaction.

### **1. Principle for determining suspicious transaction**

It can be seen that the law does not specify any pattern of behaviors that triggers a suspicious transaction. Rather the law specifies results of the use of reporting entity’s judgment if it suspects or has reasonable grounds to suspect the following transaction and behavior;

(1) The person carrying out transaction intends to avoid having his/her transactions examined by the reporting entity or the AMLO. The intention to avoid may come from a corrupt purpose or avoidance of detection of offense or,

(2) The transaction carried out may be related to any criminal offense (predicate offense currently comprises of all property-related criminal offense. See list of predicate offense under Section 3 of the Anti Money Laundering Act, 1999, codified edition). In practice, the reporting entity does not need to have enough knowledge to specify the predicate offense but may be able to identify it based on facts known by the reporting entity or if it is related to financing of terrorists or terrorist groups or,

(3) The person intended to carry out transaction, but found to be suspicious according to (1) or (2). The person hence cancelled or refused to make the transaction. Said action is therefore deemed as an attempted transaction whereby the reporting entity is obliged to report it as a suspicious transaction.

In performing duty according to (3), the reporting entity must overhaul its working procedures in the identification of customer's identity and immediately record the information before the completion of the transaction to enable the reporting entity to file a suspicious transaction together with the customer's identification in the case of attempted transaction.

## **2. Further considerations in filing a suspicious transaction report**

Apart from reporting of suspicious transaction due to doubts as described under 1, it also includes the following cases:

(1) When it is found that the act of establishing business relationship is unusual and doubtful as described in 1. and when risk assessment indicated such high risk level that the reporting entity has to refuse the establishment of relationship or the conduct of said transaction and considers filing a report to the AMLO.

(2) At the stages of customer identification or risk management or monitoring of financial movement, making transactions or carrying out of ongoing customer relationship, it is found that the customer (or person carrying out occasional transactions) is listed as the person subject to examination by the provision of the laws. Proceeding to report suspicious transactions according to the AMLA does not include "freeze the asset and inform the AMLO" according to the Counter Terrorism Financing Act, 2013.

(3) When the monitoring of financial movement or conduct of transactions or carrying out of ongoing customer relationship reveals that the customer's activity is extremely unusual and doubtful as stated in 1., the reporting entity is obliged to adjust the customer's risk to a high level or consider to end relationship and file a suspicious transaction report to the AMLO.

## **3. Specifying screening process before filing suspicious transaction report**

The reporting entity must specify steps to ascertain the facts found according to the guidance provided in 1. – 2. before filing report with the AMLO. The following guidance may be considered:

(1) After finding such suspicious behaviors stated in 1., the reporting entity should review or recheck information to ascertain that it is necessary to file report with the AMLO;

(2) Specify principle for examining related information to ensure that there is sufficient reason for suspicion before filing report to the AMLO. In other words, in considering to file suspicious transaction report to the AMLO, the reporting entity should have step for verifying facts related to the transactions and persons involved (to the extent possible since the examination is not an

investigation in criminal justice procedures). At least, the reporting entity should report facts together with underlying reasons for the suspicions.

(3) Approval for filing transaction report must be sought from senior management. In other words, before filing the report to the AMLO, the reporting entity must assign an executive (i.e. in compliance operations according to the AMLA), who may delegate his/her authority, to approve report submission, including all facts stated in the report. The reporting of suspicious transactions is crucial for AMLO investigation into money laundering offenses as well as credibility of the reporting entity. If the suspicious transaction reports lack sufficient supporting facts or proper verification, it would reflect deficiencies on the part of the reporting entity's operations and pose the risks of carrying out transactions for a large number of persons connected with the commission of offense.

### **Key principle in examining transaction report**

It must be aware that the decision to conduct suspicious transaction is subject to the reporting entity since the law permits it to consider although the transaction or person carrying out the transactions is suspicious. However, it does not mean that such transaction or person will definitely be related to committing offense. Hence, using judgment to continue making the transaction subject to be reported as a suspicious transaction will depends on underlying facts and grounds for reporting. If the officer deems that carrying out the transaction definitely risks violating the provisions on money laundering, the reporting entity should consider to refuse making the said transaction.

What is stated in the previous paragraph shows that it is of extreme imperative for the reporting entity to employ capable officers who have proper expertise in fields appropriate to the CDD process and use of judgment before considering whether to report suspicious transaction and whether to conduct said transaction. For this reason, the law requires senior management to make judgment (as the law expects credibility in use of judgment in the examination and decision-making from said person or group of persons).

## **Transmission of Information Accompanying Wire Transfers**

(For banks and professions under Section 16 (9) Who provide or receive electronic funds transfer services)

The reporting entity who provides electronic funds transfer (including electronic payment) is duty bound to arrange for customer identification, to manage risks of money laundering and financing of terrorism (ML/FT) and to monitor financial movements or transactions in accordance with the general principle in the ministerial regulations. However, as the electronic funds transfer is a channel of transaction that poses high ML/FT risks, there shall be requirements for the ordering institution and beneficiary institution concerning the transmission of information accompanying a wire transfer and examination of the information that accompanied the transfer. Cross-border funds transfer shall be subject to more enhanced examination than the domestic transaction.

### **1. Policy for the ordering and beneficiary financial institution**

The reporting entity must set out internal policy, rules or guidance for the ordering and beneficiary financial institutions in performing their duties, including the intermediary in the payment chain as follows:

(1.1) if the wire transfer is a domestic wire transfer, a reporting entity that is an ordering institution using the system of transmitting transfer order in electronic network should make initial examination whether or not is there agreement to request, to provide or to transmit information to the party concerned with the money transfer. Although the law does not strictly require the ordering institution to transmit information accompanying the wire transfer, and the beneficiary institution to obtain information accompanying the wire transfer, but the reporting entity must be certain that if the AMLO request information together with a wire transfer order, the reporting entity that is the ordering or beneficiary institution is able to provide the information without delay.

Remark: Reporting entity will be exempt from the obligation to transmit information with a domestic wire transfer on the principle that the reporting entities providing domestic money transfer service use the central network for money transfer and are under supervision of the central supervisory agency. This means that it should have very low risks to cause limitations in requesting or receiving information between the reporting entity operating the same business type and relying on each other. Therefore, if there are limitations in the money transfer network system or different supervisory standards that cause higher risks in requesting or receiving information between the reporting entities operating the same business type and relying on each other, thus, causing the risks of not being able to efficiently track the domestic wire transfer, AMLO may consider issuing the rules concerning information accompanying domestic wire transfer in stringent manner as it does with the cross-border money transfer order.

(1.2) If the wire transfer is a cross-border funds transfer, the reporting entity must set out the measures as follows:

(1.2.1) Arranging for its officer to request information from the customer on the recipient person and objectives of the transaction as much as possible. The officer must also identify all and accurate information contained in the system of transmitting the wire transfer order as required by law. Although it is able to transmit complete wire transfer order to the beneficiary institution, but if an obstruction of network system occurs or because of any other cause that results in incomplete information to the reporting entity who is the beneficiary party, the beneficiary party may deny the said transfer order or request the ordering financial institution to send additional information. Under the international standard, the recipient's information is more crucial than the transferor's information. This is because once money has been transferred to the recipient, it is difficult to trace. Therefore, the guideline should be strictly prescribed for the officer to request information, perform customer due diligence of the recipient and discreetly consider objectives of funds transfer.

(1.2.2) Establishing appropriate agreements and procedures for sending/receiving additional information in case of mistake that resulted in transmitting of incomplete information. Timeline and type of information which can be sent to the beneficiary financial institution upon request should be clearly spelled out.

(1.2.3) Setting measures for examining the terrorist list on the risk-based principle. Cross-border wire transfer poses higher ML/FT risks than other category of monetary transactions. Therefore, prior to sending or receiving wire transfer order and making payment to the customer or occasional customer, as the case may be, the reporting entity should consider examining the name list of persons or legal persons or legal arrangement related to the cross-border electronic funds transfer transaction, namely, examination of information of the customer or occasional customer sending the transfer order and the customer or occasional customer receiving the transfer order. On the other hand, the reporting entity receiving the transfer order should consider examining the information of the customer or occasional customer receiving the money and the customer or occasional customer ordering the transfer against the name list prescribed by the CTF law (2013) (i.e. terrorist list issued by the U.N. and circulated by AMLO; designated persons by court order and announced by AMLO) except when the reporting entity is certain that while sending or receiving the transfer order and making payment to the recipient person, the sender or receiver of money would not definitely be the designated persons.

(1.3) In case of receiving cross-border wire transfer order, the reporting entity must have measures in place as follows:

(1.3.1) Establishing an operation system (whether being the system carried out by technology or the system carried out by personnel) capable of examining that whether or not the originator information is complete information as prescribed by law, specifically in receiving the money transfer order of large transaction. After an initial examination carried out by technology, the



reporting entity should assign its officer to recheck and determine which information is defective and whether or not it is necessary to obtain additional information;

(1.3.2) Establishing procedures for requesting information, warning or others to reduce the risks of the reporting entity in violating the law when it makes transmission of information accompanying a cross-border wire transfer. This shall include appropriate agreement and stage in sending/receiving additional information in case of mistake that caused sending of incomplete information. Timeline and type of information should be clearly spelled out;

(1.3.3) Setting sanction measures against the ordering financial institution who fails to provide cooperation in sending/receiving important information or fails to act in compliance with the law;

(1.3.4) Information of the ordering person and the recipient person must be checked with the name list as prescribed by law (see the details of Clause (1.2.3) above).

(1.4) In the case of an intermediary institution where the reporting entity acts as intermediary in receiving wire transfer order from overseas ordering financial institution in order for transferring to the recipient person (who stays in the country), or performs as intermediary in sending a wire transfer order from domestic ordering financial institution in order for transferring to the beneficiary financial institution who is its partner bank abroad, the reporting entity must have the following measures in place:

(1.4.1) Ensuring that the relevant personnel gives complete information accompanying wire transfer order from domestic or foreign ordering financial institution to the beneficiary financial institution;

(1.4.2) Establishing an operation system (whether being the system carried out by technology or the system carried out by personnel) capable of examining that whether or not the received wire transfer order has complete information as prescribed by law (complete information accompanying a wire transfer must be transmitted to the beneficiary financial institution at destination);

(1.4.3) Establishing appropriate agreements and procedures for sending/receiving additional information in case of mistake that resulted in transmitting of incomplete information. Timeline and type of information which can be requested to the ordering or the beneficiary financial institution, as the case may be, should be clearly spelled out;

(1.4.4) Establishing record keeping system for storing information and wire transfer order in case of mistake in the information transmission system that obstructed the reporting entity in transmitting complete information accompanying wire transfer order to the beneficiary financial institution. Procedures for sending additional information to the beneficiary party should also be set out;

(1.4.5) Having sanction measures against the ordering or beneficiary financial institution who fails to provide cooperation or acts in compliance with the law.

## 2. Procedures for additional examination of cross-border electronic funds transfer

In the cross-border wire transfer, it is necessary for the reporting entity to carry out some additional stages for conducting general transaction beside to the CDD process as follows:

(2.1) Sending information accompanying cross-border wire transfer: the wire transfer order usually consists of code number or alphabets combined with number for specific money transfer reference, money amount, ordering date and time, code number of the beneficiary service provider, etc. However, the ministerial regulations in combination with international standards on AML/CFT prescribe that other essential information that accompanied a wire transfer must also be transmitted to the beneficiary financial institution. Thus, the reporting entity is obliged to send the following information accompanying the cross-border wire transfer to the beneficiary party:

- (1) Information on full name of the person ordering money transfer;
- (2) Information on account number or examinable reference number of the person ordering money transfer;
- (3) Information on national ID number<sup>4</sup> or address or date and place of birth of the person ordering money transfer;
- (4) Information on amount of money and currency being ordered for transfer;
- (5) Information on name or code showing name and branch of the reporting entity sending money transfer order;
- (6) Information on full name of the person receiving money;
- (7) Information on account number or examinable reference number of the person receiving money;
- (8) Information on name or code showing name and branch of the service provider receiving money transfer order.

(2.2) If the reporting entity is the beneficiary party, the reporting entity must check whether information under Clause (2.1) together with money transfer order are complete. In the case of not receiving, or receiving incomplete information, actions shall be taken in accord with organization policy as stated in Clause 1;

(2.3) Whether or not the ordering person and the receiving person money is a customer or occasional customer of the reporting entity, the reporting entity must perform customer identification under Section 19 (3) of the ministerial regulation regarding procedures for examining customer information (occasional customer) with name list prescribed by the law prior to sending transfer order in the case it is the ordering financial institution, or prior to transferring money in the case it is the beneficiary financial institution;

---

<sup>4</sup> Including also passport number or other ID card of alien customer and ID number of juristic person customer or the number used in self-identification of customer under legal agreement

(2.4) The reporting entity must have efficient operation system for suspending, stopping or refusal in case of finding that the wire transfer may be connected with money laundering or predicate offense or financing of terrorism, especially upon finding that the person connected with the wire transfer is a designated person. If the reporting entity sends a wire transfer order to the recipient person knowing that either one party is the designated person or listed by the U.N., the reporting entity may commit an offense for not complying with the procedures set for customer refusal under the AML law and in case of already making payment to the recipient person, it may be charged for not complying with the examination and asset restraint measures under the CTF law.

### **3. Exemptions:**

In case of an electronic funds transfer having the following nature or objectives, the reporting entity is not required to send information accompanying wire transfer order or to examine the originator information under the ministerial regulations:

(3.1) A transmission of ordering or receiving wire transfer having the value less than fifty thousand baht and not having suspicious circumstance that it may be connected with money laundering or committing predicate offenses;

(3.2) Such electronic funds transfer is an electronic payment connected with the payments for goods and services (from electronic money card or invoice having electronic reference code), or using a credit card (making payment in accordance with the limit prescribed in electronic card and the customer is required to make repayment within time limit set by the credit card company) or using a debit card (making payment within limit of money deposit in bank account where the payment information is equivalent to the withdrawal information in deposit account of the customer). See details in the guideline announced by the Secretary-General, Re: Guideline for electronic funds transfer exempt from sending information with money transfer order.

(For details on exemptions, see the announcement made under the ministerial regulation, Re: Guideline for electronic funds transfer exempt from sending information with money transfer order).

## Record Keeping

The Anti-Money Laundering Act, 1999, (see the code), including the ministerial regulations and international standard on anti-money laundering and combating the financing of terrorism (AML/CFT) prescribed fundamental principle that financial institutions and designated non-financial businesses and professions (DNFBPs), including money value transfer services, must keep the customer information for at least five years from the date terminating business relationship, or five years from the date of making transactions for occasional customers.

Record keeping herein means all the information and evidence, whether or not being the originals or copies and the reporting entity may keep them by any means but finally they can be transformed into readable documents and used as evidence.

The categories of information kept by the reporting entity for the period of five years in paragraph one under the anti-money laundering law and ministerial regulations are namely:

(1) Ongoing transaction information (including electronic fund transfer, both domestic and cross-border, together with the original or recipient information accompanying the electronic money transfer orders).

(2) The identification information, self-identity, results of the examination and verification obtained from the stage of customer identification and risks management, analyses obtained from carrying out customer due diligence (CDD), alteration of assessment or analysis, revision of customer information, findings and examination as well as the reporting of suspicious transactions and other information relevant to CDD.

The reporting entity must keep the above information to be readily available for examination upon request by the AMLO.

## **Foreign Branches and Subsidiaries**

The term “branch” herein refers to foreign branch offices of the reporting entity (for foreign branch offices located in the country, they are deemed an integral part of organization, thus not having the issues in the enforcement of Thai law).

The term “subsidiaries” herein refers to reporting entity’s majority-owned subsidiaries (sufficient for having authority to set out management policy) which is located abroad; and the said subsidiaries are businesses or professions under obligation of this ministerial regulation.

In principle, the reporting entity is duty bound to supervise its branch offices or subsidiaries, whether located abroad or in Thailand, to strictly comply with the anti-money laundering law and the counter terrorism financing law in the same manner as the reporting entity which is the head office or parent company. However, in order not to also cause confusion in the setting out of policy or guideline in line with Thai laws and laws of the countries in which the branch offices or subsidiaries are located, the reporting entity is required to consider establishing the following guidance in supervising its branch offices and subsidiaries:

### **Supervision and policy for branch offices or subsidiaries**

(1) In establishing foreign branch offices or subsidiaries, the areas or countries not having risks of money laundering and financing of terrorism should be chosen as the first priority;

This means that when the reporting entity considers the factor in expanding its business by establishing foreign branch offices or subsidiaries, the reporting entity should consider selecting the establishment in the areas or countries not having high risks of money laundering and financing of terrorism as the first factor. But it does not mean that the law will forbid the reporting entity to establish branch offices or subsidiaries in the areas or countries having high risks. For the establishment in the said high-risk areas or countries, the reporting entity must prescribe more stringent measure and supervision as to be further described.

(2) Having measures in examining stringency of laws and enforcement of the laws governing AML and the law governing CTF in the areas or countries in which the branch offices or subsidiaries are located;

The examination of stringency of the said laws allows the reporting entity to consider whether or not its foreign branch offices or subsidiaries are able to comply with the laws of the areas or countries in which they are located in case AML/CFT laws of such areas or countries are more stringent than Thai laws, or if Thai laws are more stringent, it must be considered that whether or not the compliance with any part of Thai laws may obstruct the operations in such areas or countries.

(3) Establishing policies in compliance with the Thai AML and CTF laws as the primary objective;

Although the branch offices or subsidiaries of the reporting entity are located in other areas or countries but they are still under the jurisdiction of Thai law according to the principle of nationality of the reporting entity. Therefore, compliance with Thai laws must be the main policy that the reporting entity has to strictly observe.

(4) Prescribing guidelines or measures in case of having different legal provisions between the two countries

In case of having different provisions of AML and CTF laws between Thailand and the areas or countries in which the branch offices or subsidiaries are located, apart from the consideration in compliance with Thai laws, under the principle of sovereignty, the branch offices and subsidiaries must also comply with the laws of the areas or countries in which they are located. Therefore, if Thai laws are more stringent, the reporting entity is duty bound to supervise the branch offices or subsidiaries to strictly comply with the measures under Thai law. However, should the laws of the areas or countries in which they are located have more enhanced provisions, the reporting entity must also have additional policies or measures in place in order to be able to comply with the laws of the areas or countries in which the branch offices or subsidiaries are located.

(5) Prescribing policies and measures for enhanced CDD for the branch offices or subsidiaries located in the areas or countries having high risks of money laundering and financing of terrorism.

In case of the reporting entity establishing branch offices or subsidiaries in the areas or countries having high risks of money laundering and financing of terrorism, the reporting entity must have enhanced policies or measures as follows:

(1) Stringent supervision: The reporting entity must require its foreign branch offices or subsidiaries to undertake internal audit in compliance with the Thai AML and CTF laws in a more strict and stringent manner than those located in low-risk areas or countries.

(2) Risk monitoring and assessment: The reporting entity must require that such branch offices and subsidiaries located in high-risk areas or countries are subject to ML/FT risk assessment regularly. Should it be found that the branch offices and subsidiaries have high risks in the business operations and may cause damages to the head office owing to incompliance with the laws (whether Thai laws or laws of the countries in which they are located), it is necessary for the head office to set forth special measures in order to solve the problems, such as, changing the management staff at the branch offices or subsidiaries and enhancing the supervision of work, etc.

(3) Notifying messages or information relevant to money laundering and financing of terrorism issues

As the branch offices or subsidiaries are located in high-risk areas or countries, the head office should require such branch offices or subsidiaries to follow up the development of AML/CFT, including legal and social problems which may affect their business operations and regularly report to the head office in order for the head office to consider prescribing guideline for timely preventing or solving the problems which may be caused by the said risks.

However, no matter the reporting entity has established the branch offices or subsidiaries in the areas or countries of whatever risks, the reporting entity must regularly set out internal audit policy in compliance with the AML and CTF laws. Intensity of audit function depends on risk level or risk factors faced by each branch office or subsidiaries located in the area or country which may have different problems.

## **Correspondent Banking Relationship and Reliance on Third Party**

### **1. Correspondent banking relationship**

Correspondent Bank means a financial institution providing banking service for its trading partner's customer, usually being the business of same category, namely, a bank. Therefore, the correspondent financial institution under this ministerial regulation specifically means a bank (i.e. foreign or international bank) or the reporting entity operating banking business as the case may be. Whereas a bank which is the reporting entity is the service user of foreign or international financial institution, it will be a "Respondent Bank" and, vice versa, it may provide the service as a "Correspondent Bank" for foreign or international financial institution.

Providing service as a correspondent bank may include banking service to respondent bank's customer and also to trading partner who is the respondent bank in cash management, whereby the respondent bank deposits large amount of foreign currency in cash and earns interest from the correspondent bank or payment by check for end customer, or receives money transfer order for end customer or acts as intermediary financial institution in the chain of electronic fund transfer, or provides currency exchange service, or provides payable-through account service (Note: not provided by banks in Thailand owing to high risks of money laundering; the respondent bank is obliged to perform customer due diligence).

### **Principle in establishment of relationship and carrying out relationship with correspondent bank**

When a bank which is the reporting entity establishes a correspondent relationship with foreign or international bank, it is obliged to carry out money laundering and financing of terrorism (ML/FT) risk management for correspondent bank, whereas such risk management is different from a risk management for customer.

**(1) The reporting entity must have measure for risk management before the establishment of correspondent relationship** with due regard to:

In determining risk factors for assessing risks of the correspondent bank, the reporting entity should have due regard to:

- results of assessment in accord with AML/CFT international standard conducted by reliable international organization;
- the quality of supervision (may be considered from the reliability of the supervisory agency);
- reputation of the institution regarding observance of AML/CFT international standard (e.g. record of punishment owing to not complying with or in violation of the rules under the anti-money laundering law (AMLA) and the counter terrorism financing law (CTF law)).



The reporting entity may consider other additional factors as appropriate, e.g., the factors related to the area or country at risks of serious crimes or offenses related to corruption or country subject to economic sanctions, etc.

**(2) Set out measure for monitoring and risk assessment**

Upon having determined the risk factors for conducting risk assessment of correspondent bank, the reporting entity must have measures in place, namely, the procedure to examine and assess the risks of correspondent financial institution, the request of information, the examination of reliability, or the determination of relationship level consistent with the results of risk assessment. In this respect, the reporting entity must set out policy, rules or guidance in carrying out risk management of correspondent bank by taking into consideration as follows:

(2.1) Setting out policy of refusal for establishing relationship with high risk correspondent bank: the reporting entity may consider the results of ML/FT risk assessment in order to set level of business relationship with the correspondent financial institution. Also, there are factors for determining whether such correspondent bank abroad is a high risk institution that poses the reporting entity at risk of committing offenses or whether it is connected with money laundering or financing of terrorism, as follows:

- The financial institution operates as a shell bank (see the meaning in the ministerial regulation);
- The financial institution has been sanctioned by developed countries, whereas the reporting entity has established relationship with correspondent banks of those developed countries.

The provision regarding shell bank is a legal obligation (see the ministerial regulation), while the other guidance are deemed alternatives which may be additionally set out by the reporting entity and may be considered from information of correspondent financial institutions abroad or information from national economic agencies or international organization relevant to AML/CFT or the standard performed by businesses in the same category.

(2.2) Set out rules and procedures for requesting information or examining information and analyzing the risks: the reporting entity should have clear principle in determining relevant factors in order to assess risks:

For example

Stage 1: After having selected or identified the correspondent bank with which the relationship is to be established (usually the reporting entity had earlier considered its reliability), the reporting entity must appraise risk factor concerning area or country having deficiency in AML/CFT;

Stage 2: In case of finding low risks of the area or country, other risk factors shall be examined, namely, the risk factors related to the quality of supervision (whether or not the supervision is stringent); AML/CFT law to be complied by the correspondent financial institution (whether it is more or less stringent than Thai law);

Stage 3: In case of finding low risks on the supervision and having the law with stringency equal to or more than Thai law, the reporting entity should further examine the results of assessment of compliance with the AML/CFT standard or the results of law enforcement to determine whether or not the financial institution wishing to establish correspondent relationship had been assessed with low level of compliance or previously punished under the relevant law;

Stage 4: In case of finding low risks on every factor above, the reporting entity must request for information on policy, principle or practice relevant to the compliance with the AMLA and the CTF law or other relevant laws as practiced by the correspondent bank. Where it is believable that such correspondent bank is reliable and has enhanced AML/CFT measure, the reporting entity may only request the confirmation without having to examine much insight information;

Stage 5: Verifying information of beneficial owner, authorized signatory director together with the name list prescribed by the law;

Stage 6: Upon entering the stage of assessing risks of the correspondent bank, the reporting entity must examine the conditions contained in the correspondent banking agreement whether it is contrary to internal law of each party or whether the reporting entity or the correspondent bank must carry out additional actions to be consistent with the relevant law of each party;

Stage 7: The reporting entity must obtain approval from senior management before establishing correspondent relationship regardless of its risk level.

....., etc.

(2.3) The reporting entity must have policy, principle or practice prescribed to regularly carry out risk management of the correspondent bank until the termination of relationship.

In this case, it may be comparable to a risk management for the customer, namely, the reporting entity may determine risk level and set timeline for risk management corresponding to such risk level. If the correspondent bank has high risk, examination of business relationship will be more frequent than the lower risk correspondent banks.

**(3) Set out the process for approving the results of risk assessment and approving the establishment of relationship**

Upon completing the risk management process and having already received relevant information in combination with the results of risk assessment of the correspondent bank, the reporting entity must prescribe the stage in approving the results of risk assessment and consider whether or not to approve the establishment of relationship with the correspondent bank, whereas the authorized person to approve the results of assessment and approve the establishment of relationship with the correspondent bank must be the senior management or may be in the form of the board in which the senior management is represent.

**(4) Set out special measure for risk management of high-risk correspondent financial institution**

If the results of risk management revealed high risk level of any bank with whom the reporting entity will maintain the policy to establish relationship, it is necessary for the reporting entity to have enhanced measure for managing risks from business relationship with the said correspondent bank as comparable with the customer due diligence process in accordance with the following guidance:

(4.1) Requesting information about the beneficial owner, principal shareholder, high level executive board and management structure to carry out customer identification, specifically the verification of information against the name list as prescribed by the related law;

(4.2) Prescribing amount of money or type of service related with the correspondent bank, specifically limiting the use of service with high ML risks, or setting lower threshold for investment in the correspondent bank, etc.

(4.3) Regularly revising information of the correspondent bank and verifying information against the name list as prescribed by the related law in a stringent manner;

(4.4) Requesting information relevant to AML/CFT measures or policies to satisfy itself that the correspondent institution has measures in place for compliance with AML/CFT standard; and regularly monitoring the said information until such correspondent bank has lower level of risks.

In the case the reporting entity has already carried out relationship with the correspondent bank having high ML/FT risks, the measures in Clause (4) shall be immediately applied.

Moreover, the reporting entity should understand that in the case where the correspondent bank met stringent compliance and finds that the reporting entity is a high-risk financial institution, the reporting entity may also be treated on the same principle as Clause (4).

Remark: Non-bank reporting entity may also apply the principle of risk management for business relationship with its trading partner abroad.

## **2. Reliance on third parties**

Reliance on third parties means the reporting entity relies (including receiving mutual benefits and thus relying on each other) on a third party (the second party should mean the customer) to perform some elements of the customer due diligence process. Therefore, in order to be certain that the said reliance would not cause the risks in non-compliance with the law, the reporting entity should consider relying on the third party who is a reporting entity obliged to comply with the ministerial regulation, Re: Customer due diligence, which falls under proper supervision.

When the reporting entity is a service provider abide by business agreement with other financial institution in selling products or providing services of both parties for the benefits of the reporting entity, the financial institution who is the party, and the customer, there occurs a reliance or burden on any one party in complying with the customer due diligence process, i.e. in making face-

to-face transaction or a request for information from the customer. Therefore, when there is an agreement concerning mutual services provision, the financial institution who is the party may act as the principal agency in providing service for customer and accepting the customer, and, thus, the reporting entity has to rely on such financial institution for customer identification when it commences the establishment of business relationship.

Key principles of reliance on third parties are as follows:

(1) Relying on the process of customer identification, initial assessment before requesting additional identity information, verification of the name against the name list as prescribed by the law, and customer approval;

(2) The reporting entity is prohibited from relying on the third party in relation to the conduct of ML/FT risk management, monitoring of financial movements, conducting transactions or carrying out the relationship, regular revision and examination of the names against the name list prescribed by the law, and revision of the risks on a regular basis until the end of the relationship. However, in terms of reliance, the reporting entity may request information from the third party for assessing customer's risks;

(3) Reliance on third parties is different from outsourcing the agent or service provider to carry out the operation system;

(4) The reliance is subject to the third party operations, namely, the reporting entity has no power in setting up the operation system for customer identification, verification of identity information or carrying out the verification with the name list prescribed by the law under its own internal policy. This means the reporting entity has to rely on the third party in carrying out the task in Clause (1) under the operation system set up by the third party or its policy (which is different from outsourcing the agent or service provider, whereas the reporting entity has the power to prescribe agreement in line with its conditions);

(5) The reporting entity should be certain that the third party has the operation system to carry out Clause (1), including efficiency in complying with the customer due diligence process under Thai law;

(6) The reporting entity must always be aware that it bears responsibility and liability for mistakes that may occur under Clause (1) although it is the fault of the third party's operation system. The reporting entity has the duty and responsibility in compliance with the law in Clause (1). Therefore, the reporting entity should request information or perform examination to ensure that the reliance on either one of the third party will not cause it to be at risks of liability due to non-compliance with the AMLA and the CTF law (in the case of the failure of the operation system to observe compliance with the law under Clause (1), apart from liability on the part of the reporting entity, the third party must also be subjected to the same liability as the mutual agreement is about the joint provision of service and abides the third party for liability to its deficient performing of duties in Clause (1));

(7) For reliance on record keeping, the reporting entity can rely on the third party for keeping customer's information obtained from the procedures in Clause (1) should the third party give consent. But, liability remains with the reporting entity. Therefore, in relying on the third party, an agreement should be made to be certain that the third party shall keep the information as carried out under Clause (1) and be able to send the said information to the reporting entity on request or to give copy of the said information to the reporting entity (at the consent of the third party).

The followings are examples of reliance on third parties:

- In the case where the reporting entity is a branch of financial institution abroad and relying on that foreign financial institution in carrying out the procedures under Clause (1) with the customer coming from the country in which the financial institution is located and coming to carry out further relationship with the branch in Thailand, the branch in Thailand is duty bound to be responsible for risk management and due diligence until the end of relationship.

- In the case where a financial institution who provides deposit accounts recommends its customer to invest in unit investment trusts which the reporting entity is the fund manager. Though the financial institution is responsible for customer identification, customer identification during the sale of the unit investment trusts on behalf of the reporting entity is a reliance on third party as well. Therefore, in this case it is deemed that the reporting entity has relied on the financial institution to conduct the procedures under Clause (1) but the burden of liability in performing the duties is still borne by the reporting entity and the reporting entity is duty bound to perform further customer due diligence process, etc.

**Summary of Guideline  
In Compliance with the Law on Anti-Money Laundering (AML) and  
the Law on Counter Terrorism Financing (CTF)**

Subject	AMLA	CTF Law
Objectives	In order for the reporting entity: (1) To manage its risks of money laundering and financing of terrorism; (2) To sort out dirty money from business system of the reporting entity; (3) To enable AMLO to receive quality suspicious transaction report.	In order for the reporting entity: (1) To verify the customer information and occasional transaction with the designated persons (name list of financiers of terrorism) as announced by AMLO; (2) To authorize the reporting entity to quickly disrupt the financial flows of terrorists.

Subject	AMLA	CTF Law
Taking actions in compliance with the law	<p>(1) Arrangement of customer identification and verification, conducting CDD together with management of money laundering and financing of terrorism risks (assessing risks of each customer);</p> <p>(2) Monitoring ongoing financial movement, transaction or business relationship in accordance with customer risks level;</p> <p>(3) Finding customer unusualness from actions taken under Clause (1) and Clause (2) to consider sorting out customer likely connected with money laundering and financing of terrorism from business system;</p> <p>(4) Examining transactions under reasonable suspicion from all transactions of customer;</p> <p>(5) Analyzing and verifying information upon finding suspicious causes from transaction or financial movement/transaction execution/carrying out relationship and consideration for submission as quality suspicious transaction report.</p>	<p>(1) Verification of customer or occasional transaction against the designated persons (financers of terrorism) as announced by AMLO;</p> <p>(2) Immediately “freezing asset” of customer or occasional transaction upon finding information identical to the designated persons (financers of terrorism) as announced by AMLO;</p> <p>(3) “Inform” AMLO of the finding and action under Clause (2), whereas procedure and additional information in making notice shall be as prescribed by the CTF law.</p>

Subject	AMLA	CTF Law
Conditions in compliance with the law	(1) Actions shall be taken with every customer; (2) Actions shall be taken with occasional transaction under the conditions prescribed by the law (relevant to amount of transaction and upon finding suspicious causes); (3) Actions shall be ongoing until termination of the relationship.	(1) Taking actions with customer and occasional transaction with no exceptions; (2) Taking examination prior to approval for establishment of relationship (with a customer), or approval for carrying out transaction (for occasional transaction) and within three working days from the date on which AMLO has announced the designation (including upon AMLO making subsequent announcement to add or delist the designated names); (3) Immediately “freeze the asset” upon finding the facts under Clause (2); (4) “Inform” AMLO within three working days in accordance with rules and procedure prescribed by the law.

<sup>i</sup> For the proportion of shareholding of the natural person showing ultimate beneficial ownership, it shall be considered from the general business practice in such business category. Should different proportion be prescribed, the reason should be stated in the policy or practice or regulation therein.

<sup>ii</sup> The position of top executive, in this regard, means the position of highest management authority or the position capable of prescribing the main policy or significant policy in the business operation of the organization.

<sup>iii</sup> Significance, in this regard, is importance or has important role.

<sup>iv</sup> The party of significance of the customer means in case of the reporting entity of transaction requests the customer (foreign juristic person) to show the evidence of business operation in Thailand, it may request the showing of contract having party in Thailand and should such contract show the party name of business significance under the objectives of the contract, e.g., the signing party (appearing the opposing party name). This case is an example of the term of party of significance which may have more than two parties.