RIA EXCHANGE LIMITED

Procedures of

Anti-Money Laundering

And

Counter-Terrorist Financing

Version: 2019

Add: *Room 1113, Tower B, Hung Hom Commercial Centre, 37 Ma Tau Wai Road, Hung Hom, Hong Kong.*

RELATED FORMS

F1-Personal Customer Due Diligence Form

F2-Corporate Customer Due Diligence Form

F3-Declaration for MSO Partners

F4-Test for Simplified Customer Due Diligence

F5-Declaration for MSO Partners

F6-Unsual Transaction Report

F7-Third Party Source account Declaration

SECTION 1: INTRODUCTION

PURPOSE

As a Money Service Operator registered under the Hong Kong Customs and Excise ("HK C&ED"), we (or "our Company") are subject to strict responsibility to follow the regulatory requirements of the HK C&ED. Among other requirements, we must comply with the Anti-Money Laundering and Counter Terrorist Financing Ordinance, Chapter 615, Laws of Hong Kong ("AMLO") and all applicable laws and regulatory requirements that are relevant to anti-money laundering ("AML") or counter terrorist financing ("CTF"). With this regard, we, taking our business nature and operation pattern into account, develop and execute these Procedures and all relevant documents to set out the AML framework within which our business operates.

APPLICABILITY

These Procedures and relevant documents are used to avoid any person/entity from making use of our money services as channels to commit money laundering, terrorist financing or any criminal activities. These Procedures is not applicable for any matters irrelevant to AML/CTF.

These Procedures and relevant documents are designed to help all staff understanding respective responsibilities under applicable AML and CFT regulatory requirements, and implementing our Company's AML and CFT systems during their normal course of employment. Performing job functions under the AML and CFT framework under these Procedures provides the relevant staff with a solid defence to the offence ML and TF.

The management and Compliance will review these Procedures and relevant documents on annual basis, and make appropriate modification if necessary.

RESPONSIBILITY

All staff must strictly follow these Procedures. Management will regularly assess the effectiveness of these Procedures. Management will also continue to review these Procedures based on the requests made by the HK C&ED and the latest regulations issued from time to time.

REFERENCE

These Procedures and relevant documents are designed based on the applicable laws, regulatory requirements and guidelines issued by the HK C&ED, these include but not limited to:

- AMLO
- Drug Trafficking (Recovery of Proceeds) Ordinance
- Organized and Serious Crimes Ordinance
- United Nations (Anti-Terrorism Measures) Ordinance
- United Nations Sanctions Ordinance
- Weapons of Mass Destruction (Control of Provision of Services) Ordinance
- Guideline on Anti-Money Laundering and Counter-Terrorist Financing (for Money Service Operator) issued by the C&ED ("the AML Guideline")
- Circulars published by C&ED from time to time

Should there is any deviation between these Procedures and the abovementioned Ordinances or documents, the relevant ordinances or documents prevails.

SECTION 2: AML CONTROL STRUCTURE

1. To ensure the effectiveness of AML control and establish the AML culture from top to the bottom within our Company, our management implements the following control measures:
   - Exercise oversight control by our management
   - Appoint Compliance Officer ("CO") and Money Laundering Reporting Officer ("AMLO")
   - Deploy Compliance and audit function
   - Conduct staff screening and deliver training
   - Perform institutional ML/TF risk assessment

Senior management oversight

2. Senior management (including directors and the delegates) shall review the existing AML systems on a periodic basis in order to address any potential money laundering ("ML") and/or terrorist financing ("TF") risk, and to take a proactive approach to mitigate the identified ML/TF risk. Senior management will ensure the existing operation process allows staff to escalate potential or identified ML/TF issues on a timely basis.

Appointment and duties of CO

3. A Compliance Officer to take full responsibility for the establishment and maintenance of our Company's AML/CFT systems. The principal function of CO is to act as the focal point within our Company for the oversight of all activities relating to the prevention and detection of ML/TF, and to ensure that ML/TF risks are adequately managed. In particular, CO should assume responsibility for:
   (a) developing and/or continuously reviewing our Company's AML/CFT systems to ensure they remain up-to-date and meet current statutory and regulatory requirements;
   (b) overseeing all aspects of our Company's AML/CFT systems which include monitoring effectiveness and enhancing the controls and procedures where necessary;
   (c) communicating key AML/CFT issues and compliance deficiencies with senior management; and
   (d) ensuring AML/CFT staff training is adequate, appropriate and effective.

4. In order to effectively discharge these responsibilities, CO should consider a number of areas which include:
   (a) the means by which the AML/CFT systems are managed and tested;
   (b) the identification and rectification of deficiencies in the AML/CFT systems;
   (c) reporting numbers within the systems, both internally and disclosures to the Joint Financial Intelligence Unit (JFIU);
   (d) the mitigation of ML/TF risks arising from business relationships and transactions with persons from countries which do not or insufficiently apply the FATF

Recommendations;

(e) the communication of key AML/CFT issues with senior management, including, where appropriate, significant compliance deficiencies;
(f) changes made or proposed in respect of new legislation, regulatory requirements or guidance;
(g) AML/CFT staff training.

Appointment and duties of MLRO

5. A Money Laundering Reporting Officer is appointed as MLRO who is responsible for identifying and reporting any suspicious transactions. Principal functions of MLRO include:
   (a) receiving and reviewing all internal unusual transaction disclosures and exception reports and, in light of all available relevant information, determining whether or not it is necessary to make a report to the JFIU;
   (b) providing acknowledge receipt of all internal unusual transaction disclosures and exception reports; and maintaining all records related to such internal disclosures and reports;
   (c) providing guidance on how to avoid "tipping off" if any disclosure is made; and
   (d) acting as the main point of contact with the JFIU, law enforcement, and any other competent authorities in relation to ML/TF prevention and detection, investigation or compliance.

Compliance and audit functions

6. We will assign CO or engage external professional firm to conduct regular review of AML/CFT systems on an annual basis.

Staff screening

7. Our Company's new joiners and existing employees are all subjected to appropriate screening in order to ensure high standards when hiring employees, and they should attend regular AML trainings and monitoring in order to fulfill the firm's integrity requirement.

Institutional risk assessment ("IRA")

8. We will perform periodic ML/TF risk assessment every two years (or when trigger events occur) to understand how and to what extent our Company is vulnerable to ML/TF risk. Before the performance of each IRA, our Company shall make sure the risk assessment's scope and methodology [1] is documented and accepted by the senior management.

9. The IRA must be capable of identifying from internal and external sources the various risk factors exposed to our Company. The management, CO and their delegates will determine risk control measures in response to each identified risk factor subject to our Company's ML/TF risk appetite.

[1] Our Company's ML/TF risk assessment should cover a range of factors including customer risk, country risk, product/service/transaction/delivery channel risk and all other relevant risk factors.

SECTION 3: PERSONAL CUSTOMER DUE DILIGENCE ("CDD")

STEP 1: COMPLETE "F1-PERSONAL CUSTOMER[2] DUE DILIGENCE FORM"

1.1 For a customer applying for a remittance transaction of amount equals to or over HK$8,000 (or equivalent foreign currency), whether carried out in a single operation or a series of linked occasional transactions[3], the responsible staff should not execute the customer's application until confirming that the customer has completed the whole personal CDD procedures set out in this Section.

1.2 For a customer who applies for a remittance transaction of amount between HK$5,000 and HK$8,000 (or equivalent foreign currency), the responsible staff should request the customer to provide its full name and contact number proceeding his remittance application.

1.3 For a customer applying for a foreign exchange ("FX") transaction of amount equals to or over HK$120,000 (or equivalent foreign currency), whether carried out in a single operation or a series of linked occasional transactions[4], the responsible staff should not execute the customer's application until confirming that the customer has completed the whole personal CDD procedures set out in this Section.

1.4 For a customer who applies for a FX transaction of amount between HK$50,000 and HK$120,000 (or equivalent foreign currency), the responsible staff should request the customer to provide its full name and contact number proceeding his remittance application

1.5 If a customer is expected to visit our Company periodically, or in situation where CO deems it is necessary for risk control purposes (e.g., when the veracity or adequacy of any information of the customer is in doubt, the rationale of using our money services is suspicious, etc.), the responsible staff should request the relevant customer to completed the whole personal CDD procedures set out in this Section, or the relevant customer's application for any money service will be rejected.

1.6 Where a customer is requested to complete CDD procedures subject to paragraphs 1.1 to 1.5 above, and the customer's applied money service must be completed before the

[2] We can assume a personal customer is not acting for any underlying beneficial owner unless there is indication that the customer is not acting on his own behalf. If a personal customer is identified to be the person purported to act for an underlying beneficial owner, we must apply perform CDD against the beneficial owner as if the beneficial owner is the direct personal customer before executing any transactions applied by the personal customer.

[3] An example of a series of linked occasional remittance transactions: the client visits our Company several times within a short period of time for remittance service. All the remittance transactions are supported by the same source of funds (e.g., bank account held by the same party, cheques issued by the same party, or cash delivered by the same party), designated to the same beneficiary, and of very similar transaction amount.

[4] An example of a series of linked occasional FX transactions: the client visits our Company several times within a short period of time for FX. The FX transactions are of same currencies, and the transaction volumes are very similar.

required CDD procedures are completed due to specific reason, the responsible staff should escalate the situation to COCO. In situation where COCO believes that all relevant risk can be effectively managed, CO can grant a one-off exemption for the customer, allowing the customer's application to be proceeded before he completes the required CDD procedures. CO should record his rationale of granting such exemption, and requesting the customer to complete the remaining parts of CDD procedures within specific period of time as stipulated in Step 6, the customer's application for money service in the future will be rejected otherwise.

1.7 For the sake of clarity, CO will only consider granting a one-off exemption for the customer who cannot provide relevant document(s) for the verification of his identity or authority to act. Any customers who refuse to provide necessary identity information during the CDD process should be rejected and escalated for further actions (which may include reporting the customer to JFIU, please refer to Section 6 below).

STEP 2: REQUESTING RELEVANT DOCUMENTS FOR CUSTOMERS' IDENTITY VERIFICATION

2.1 Customers ("**Customers**" hereunder refer to those who are subject to CDD requirements based on paragraphs 1.1 to 1.5 above) are requested to disclose his full name, date of birth, nationality and unique identification number, and to provide the following identity documents for the purpose of verifying his identity:

Customer Type	**Document(s) Required**
Hong Kong Permanent Resident	➢ Hong Kong Permanent Residential ID Card
Hong Kong non-Permanent Resident[5]	➢ Hong Kong ID Card; ➢ Valid Travel Document[6]; or ➢ Government-issued document that certifies nationality (e.g., local identity card, driving licence)
Foreigner	➢ Valid Travel Document; or ➢ Government-issued document that certifies nationality (e.g., local identity card, driving licence)

2.2 Customer should also be requested to provide his residential address information.

2.3 The responsible staff should verify and record a customer's identity documents (if the customer provides a passport as his identity document, make a copy of the "biodata"

[5] **Hong Kong non-Permanent Residents** are persons qualified to obtain Hong Kong ID card ("HKID") but have no right of abode. According to the Registration of Persons Ordinance, (Cap 177), all residents of age 11 or above who are living in HK for longer than 180 days must register for an HKID.

[6] Valid travel document refers to an unexpired passport or some other document furnished with a photograph of the holder establishing the identity and nationality, domicile or place of permanent residence of the holder. The responsible staff must ensure that the customer arrives Hong Kong through legitimate access by checking whether the passport has been duly stamped by the HK C&ED officers.

page of the passport). For documents in foreign language, appropriate steps should be taken so that we are reasonably satisfied that the document in fact provides evidence of the customer's identity. (e.g., ensuring that staff assessing such documents are proficient in the language or obtaining a translation from a suitably qualified person).

STEP 3: NEGATIVE CHECKING

3.1 The responsible staff should screen customer's identity by Dow Jones to ensure the customer is not among the sanctions list or list of politically exposed person ("PEP").

3.2 If the checking result of Dow Jones shows that the customer may be a sanctioned party[7], a terrorist or is located/domiciled in sanctioned jurisdiction[8] or jurisdiction of high ML/TF risk, the responsible staff should take necessary steps (e.g. checking the customer's birthday and nationality) to settle the suspicion. If the customer is confirmed to be a sanctioned party, a terrorist or located/domiciled in Restricted Jurisdictions, we should suspend the CDD process and prepare a ***Suspicious Transaction Report ("STR")***.

3.3 A domestic (i.e. those located in Hong Kong, the People's Republic of China and Macau) or foreign PEP is an individual who is or has been entrusted with a prominent public function in any government, including head of state, head of government, senior politician, judicial or military official and etc. Their spouse, partner, child or parent and close associate are also defined as PEPs.

3.4 An international organization PEP is an individual who is or has been entrusted with a prominent function[9] by an international organization. Their spouse, partner, child or parent and close associate are also defined as international organization PEPs.

3.5 Our Company adopts a more stringent approach to PEP by applying the same standard for all kinds of PEPs.

3.6 If the customer is a PEP, before (i) establishing a business relationship or (ii) continuing an existing business relationship where the customer is subsequently found to be a PEP, apply all the following Enhanced Due Diligence measures: obtaining approval from senior management; taking reasonable measures to establish the customer's source of wealth and the source of the funds; and applying enhanced monitoring to the customer's transactions.

STEP 4: RISK SCORING

[7] Sanctioned party refers to individuals/entities subject to sanctions implemented by the Chief Executive of HKSAR under the United Nations Sanctions Ordinance, United Nations (Anti-Terrorism Measures) Ordinance, US President's Executive Order 13224 and all the relevant ordinances, regulatory requirements that are applicable to MSOs.

[8] Countries subject to United Nations Sanctions as enacted under the United Nations Sanctions Ordinance and its subsidiary regulations

[9] A prominent function includes, for example, director, deputy director, members of the board or equivalent functions, of the relevant international organization, but does not include a middle-ranking or more junior official.

4.1 ***C***ustomers' ML/TF risk levels (low, medium or high ML/TF risk) based on customers' respective risk factors. Customers who are identified as PEPs or classified as high-risk customers due to other reasons should be subject to enhanced due diligence. By adopting a risk-based approach, we determine the extent of the CDD measures, on-going monitoring and risk-mitigation measures based on the ML/TF risk score of the customer. Please make use of ***"F3-Customer Risk Assessment Table".***

4.2 The four risk factors below are used to determine the ML/TF risk score:

a) Country Risk

High-risk jurisdictions are:

- Countries that have been identified by the FATF as jurisdictions with strategic AML/CFT deficiencies;
- Countries which are vulnerable to corruption; and
- Countries that are believed to have strong links to terrorist activities

For example, a customer will be considered as having high country risk if he has a high portion of transactions originated from or designated to high-risk jurisdictions; or if his place of birth, nationality or place of domicile is relevant to high-risk jurisdictions.

b) Customer Risk

Examples of customers with higher Customer Risk:

- Customers without a regular source of income
- Customers that have involvement with or connection to PEPs

c) Product/Service/Transaction Risk

To ensure we maintain the most stringent AML compliance, we classify all the services provided by MSO as high-risk services.

A remittance or FX transaction will be considered as having high-transaction risk due to various reasons, for example:

- abnormal transaction volume or frequency
- transactions irrelevant to customer's background or business nature
- originated from or designated to high-risk jurisdictions
- involving sanctioned parties/jurisdictions
- involving high-risk countries
- conducted before completing CDD procedures for the customers
- conducted before obtaining all the required information as set out in AMLO / AML Guideline

d) Delivery Channel Risk

The distribution channel of products affects the risk profile of a customer. This may include placing FX exchange or remittance orders via online, postal or telephone channels, or conducting KYC through non-face-to-face manner, please refer to paragraph 7.1 for details (But in reality, we do not accept non-face-to-face KYC).

STEP 5: PREVENTIVE/MITIGATING MEASURES TO BE IMPLEMENTED ACCORDING TO RESPECTIVE ML/TF RISK LEVEL

5.1 If a customer is classified as having high ML/TF risk level, the responsible staff should obtain further information. Necessary risk-control measures should be taken according to the risk level so calculated, e.g. requesting the customer to provide additional information and/or documents about his identity, employment/business nature, source of income/wealth, the rationale of establishing business relationship with us. Requesting the customer to make his first payment to us through a FATF bank account in his name may be another appropriate measures to mitigate the ML/TF risks relevant to the customer.

5.2 CDD information should be updated periodically according to the ML/TF risk level of the customer, or when a trigger event occurs:

- Normal risk customer: every 3 year
- High risk customer: every 1 year

5.3 Examples of trigger event for CDD review include (not exhaustive):

- Significant transaction[10] is to take place
- The customers' business natures or transaction patterns have been changed substantially Documentation standards change substantially
- When our Company is aware that it lacks sufficient information about the customer
- Reactivation of a dormant customer
- Change in beneficial ownership or control of the customer
- The customers are reported to the JFIU due to their background or their involvement in suspicious transaction(s)
- Our Company identifies that the customers' identity information has been changed substantially.
- The customers apply for suspicious transaction(s), for examples, the applied transactions are deviated from the customers' CDD information, or the transactions are of abnormally high volume, etc.

5.4 Customers relevant to any trigger events for CDD review are prohibited from conducting transactions before their CDD information is renewed.

5.5 Customers are treated as dormant customers if they have not transacted with our Company for 2 years. Dormant customers are required to re-perform CDD in order to reactive their account status.

STEP 6: HANDLING CUSTOMERS WHO HAVE NOT COMPLETE CDD PROCESS

[10] "Significant" is not necessarily linked to monetary value. It may include transactions that are unusual or not in line with the FI's knowledge of the customer.

6.1 When we cannot form a reasonable believe that the true identity of a customer is known because the customer does not provide all relevant documents to verify his identity information, we will do the following:

(a) Suspend or terminate the business relationship with the customer unless there is a reasonable explanation

(b) determine whether it is necessary to file a suspicious transaction report if deemed necessary

6.2 CO and responsible officers will follow up with the customers regularly to request for the missing documents. The principle of tolerance is as follows:

(a) Tolerant 30-day delay for missing connected parties' identity verification documents, but judgment of CO is needed

(b) Tolerant 90-day for missing address verification, but judgment of CO is needed

6.3 The incomplete CDD status and follow-up record shall be escalated to the senior management on a regular basis.

6.4 In general, further extension should not be allowed unless the delay is due to uncontrollable factors or customer is not identified as high-risk customers. CO shall justify and document the reasons and risk control measures (if necessary). CO and/or MLRO should assess whether the failure of providing verification documents provides grounds for filing suspicious transaction reports with the JFIU.

NON-FACE-TO-FACE CDD REQUIREMENTS

7.1 In situation where it is not practical to perform CDD procedures with customers through a face-to-face manner, or when our Company starts to implement electronic CDD procedures, the responsible staff shall take supplementary measures to verify a customer's identity information, e.g., requesting the customer to take selfie and compare the facial identity of the customer with his identity documents. Further, the first payment made into the customer's account is received from an account in the customer's name with a bank operating in HK or equivalent jurisdiction.

SECTION 4: CORPORATE CUSTOMER DUE DILIGENCE

STEP 1: COMPLETE "F2-CORPORATE CUSTOMER DUE DILIGENCE FORM"

1.1 For a customer applying for a remittance transaction of amount equals to or over HK$8,000 (or equivalent foreign currency), the responsible staff should not execute the customer's application until confirming that the customer has completed the whole corporate CDD procedures set out in this Section.

1.2 For a customer who applies for a remittance transaction of amount between HK$5,000 and HK$8,000 (or equivalent foreign currency), the responsible staff should request the customer to provide its full name and contact number proceeding his remittance application.

1.3 For a customer applying for a foreign exchange ("FX") transaction of amount equals to or over HK$120,000 (or equivalent foreign currency), the responsible staff should not execute the customer's application until confirming that the customer has completed the whole corporate CDD procedures set out in this Section.

1.4 For a customer who applies for a FX transaction of amount between HK$50,000 and HK$120,000 (or equivalent foreign currency), the responsible staff should request the customer to provide its full name and contact number proceeding his remittance application.

1.5 If a customer is expected to visit our Company periodically, or in situation where CO deems it is necessary for risk control purposes (e.g., when the veracity or adequacy of any information of the customer is in doubt, the rationale of using our money services is suspicious, etc.), the responsible staff should request the relevant customer to completed the whole corporate CDD procedures set out in this Section, or the relevant customer's application for any money service will be rejected.

1.6 Where a customer is requested to complete CDD procedures subject to paragraphs 1.1 to 1.5 above, and the customer's applied money service must be completed before the required CDD procedures are completed due to specific reason, the responsible staff should escalate the situation to CO. In situation where CO believes that all relevant risk can be effectively managed, CO can grant a one-off exemption for the customer, allowing the customer's application to be proceeded before he completes the required CDD procedures. CO should record his rationale of granting such exemption, and requesting the customer to complete the remaining parts of CDD procedures within specific period of time as stipulated in Step 6, the customer's application for money service in the future will be rejected otherwise.

1.7 For the sake of clarity, CO will only consider granting a one-off exemption for the customer who cannot provide relevant document(s) for the verification of its identity or the authority to act of the customer's representative. Any customers who refuse to provide necessary identity information during the CDD process should be rejected and escalated for further actions (which may include reporting the customer to JFIU, please refer to Section 6 below).

STEP 2: REQUESTING RELEVANT DOCUMENTS FOR CUSTOMERS' IDENTITY VERIFICATION

2.1 A corporate customer ("**Customers**" hereunder refer to those who are subject to CDD requirements based on paragraphs 1.1 to 1.5 above) is required to disclose the following information:

(a) Full name
(b) Date of incorporation, establishment or registration
(c) Place of incorporation establishment or registration
(d) Unique identification number (e.g., incorporation number or business registration number)
(e) Document type
(f) Principal place of business (if different from the address of the registered office)

2.2 A corporate customer should provide any or some of the following documents to allow us to verify its identify information given under 2.1 above:

(a) a copy of the certificate of incorporation and business registration (where applicable)

(b) a copy of the customer's memorandum and articles of association which evidence the powers that regulate and bind the customer

(c) a copy of the certificate of incumbency/ certificate of good standing

(d) the details of the ownership and structure control of the customer, e.g. an ownership chart

(e) partnership deed (for partnership)

(f) company search report issued within the last 6 months (if available)

(g) other relevant documents provided by a reliable and independent source (e.g., government body)

2.3 For documents in foreign language, appropriate steps should be taken so that we are reasonably satisfied that the document in fact provides evidence of the customer's identity. (e.g., ensuring that staff assessing such documents are proficient in the language or obtaining a translation from a suitably qualified person).

2.4 If the corporate customer is in the form of partnership or other unincorporated bodies, the responsible staff should understand the legitimate purpose of the organization, and try to understand if the customer is relevant to any professional or trade association.

2.5 The responsible staff should also try to obtain below information if CO deems necessary:

(a) jurisdictions where the customer have branches

(b) annual business volume amount

(c) source of fund (e.g.: internal transfer, investor, ordinary business etc.)

(d) major counterparts (supplier / buyer) and their respective jurisdictions

(e) reason of using MSO services

2.6 Peer licensed MSOs who want to or have established partnerships with us are subject to specific CDD procedures as they are expected to strictly comply with all the requirements set forth by the HK C&ED, the AML Guideline and all applicable laws and regulatory requirements relevant to AML and CFT. A MSO partner must complete and provide the following documents for CDD purpose:

(a) ***"F5-Declaration for MSO Partners***"

(b) Internal AML policy, procedures or operational manual

(c) AML audit report

2.7 CO may further request a MSO partner to provide its annual financial statement, quarterly report submitted to HK C&ED and/or external audit report with regard to their internal AML control when CO deems it is fit to do so.

STEP 3: CDD OF ASSOCIATED PERSONS

3.1 The due diligence procedures for a corporate customer involve identifying the customer's associated persons (namely, the customers' beneficial owners and connected parties, and the persons purporting to act on behalf of the customers ("PPTA")), and verifying their identify information on a risk-based approach.

<u>CDD against a Beneficial Owner</u>

3.2 The AMLO defines beneficial owner of a corporation as:

(i) an individual who:

a) owns or controls, directly or indirectly, including through a trust or bearer share holding, more than 25% of the issued share capital of the corporation;

b) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights at general meetings of the corporation; or

c) exercises ultimate control over the management of the corporation; or

(ii) if the corporation is acting on behalf of another person, means the other person

3.3 The AMLO defines beneficial owner of a partnership as:

(i) an individual who:

a) is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership;

b) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights in the partnership; or

c) exercises ultimate control over the management of the partnership; or

(ii) if the partnership is acting on behalf of another person, means the other person

3.4 The AMLO defines beneficial owner of an unincorporated body other than a partnership as:

(i) an individual who ultimately owns or controls the unincorporated body:

(ii) if the unincorporated body is acting on behalf of another person, means the other person

3.5 We must identify a beneficial owner and request for his identity document on the same standard of a personal customer, please refer to paragraphs 2.1 to 2.3 under Section 3 above.

CDD against a Person Purporting to Act ("PPTA")

3.6 The AMLO defines a PPTA as a person who is appointed to act on behalf of the direct corporate customer to establish business relationship and/or give instructions to our Company to conduct activities through the business relationship established.

3.7 An account signatory or the attorney of a corporate customer should be treated as the corporate customer's PPTA.

3.8 We must identify a PPTA and request for his identity document on the same standard of a personal customer, please refer to paragraphs 2.1 to 2.3 under Section 3 above.

CDD against a Connected Party

3.9 A connected party of a customer that is a legal person, a trust or other similar legal arrangement:

(a) in relation to a corporation, means a director of the customer;
(b) in relation to a partnership, means a partner of the customer;
(c) in relation to a trust or other similar legal arrangement, means a trustee of the customer;
(d) a natural person holding a senior management position or having executive authority in the customer.

3.10 A corporate customer must provide the full names, identity numbers and nationalities of all its connected parties. At least one of its connected parties must provide a copy of his identity document (e.g., passport or HK ID card) for verification purpose.

3.11 For a corporate customer that is of high ML/TF risk, or subject to CO's judgment, we may request more than one connected parties of a corporate customer to provide their identity documents, we may further request particular connected party(ies) to disclose their source of income/funds or business/employment history.

3.12 For the sake of clarity, if a connected party of a corporate customer is also the beneficial owner and/or PPTA of the customer, the connected party shall provide his identity document for the verification of his identity.

STEP 4: APPLICABILITY TEST OF SIMPLIFIED DUE DILIGENCE ("SDD")

4.1 If the customer may fall into one of the categories below, it should be subjected to the SDD test by referring to ***"F4-Test for Simplified Customer Due Diligence"***. After the test, if it is confirmed that the business nature of the Customer really belongs to one of the category below, SDD can be applied for the customer is deemed to present a relatively low ML/TF risk:

(a) Hong Kong Financial Institution

(b) Equivalent Financial Institution

(c) Listed Company

(d) Government and Public Body

(e) Transaction conducted by customer relates to Pension, Retirement Scheme or Insurance

(f) Solicitor's Client Account[11]

4.2 Adopting a SDD means the verification and/or name screening requirements of the customer's beneficial owner is exempted. Other aspects of CDD must still be undertaken, despite the frequency of CDD updates and degree of ongoing monitoring (see Section 5 below) can be reduced subject to CO's judgment.

4.3 If a customer is not itself a SDD customer, but has in its ownership chain an entity that falls within one of the SDD categories above, we are not required to identify or verify the beneficial owners of that entity in that chain when performing CDD for the customer. However, we should still identify and take reasonable measures to verify the identity of beneficial owners in the ownership chain that are not connected with that entity.

STEP 5: NEGATIVE CHECKING (BENEFICIAL OWNERS, DIRECTORS, AUTHORIZED PERSONS/REPRESENTATIVES, PARTNERS) (COLLECTIVELY REFERRED TO AS "ASSOCIATED PERSONS")

5.1 All connected parties, beneficial owners and PPTA of a corporate customer must be screened by Dow Jones.

5.2 If the checking result of Dow Jones shows that the customer or its associated persons may be a sanctioned party[12], a terrorist or is located/domiciled in sanctioned jurisdiction[13] or jurisdiction of high ML/TF risk, the responsible staff should take necessary steps (e.g. checking the customer's birthday and nationality) to settle the suspicion. If the customer or its associated persons is confirmed to be a sanctioned party, a terrorist or located/domiciled in Restricted Jurisdictions, we should suspend the CDD process and prepare a ***Suspicious Transaction Report ("STR")***.

[11] The moneys or securities of the solicitor's client account must be mingled. If a client account is opened on behalf of a single client or there are sub-accounts for each individual where funds are not co-mingled, the identity of the underlying clients must be identified

[12] Sanctioned party refers to individuals/entities subject to sanctions implemented by the Chief Executive of HKSAR under the United Nations Sanctions Ordinance, United Nations (Anti-Terrorism Measures) Ordinance, US President's Executive Order 13224 and all the relevant ordinances, regulatory requirements that are applicable to MSOs.

[13] Countries subject to United Nations Sanctions as enacted under the United Nations Sanctions Ordinance and its subsidiary regulations

5.3 A domestic (i.e. those located in Hong Kong, the People's Republic of China and Macau) or foreign PEP is an individual who is or has been entrusted with a prominent public function in any government, including head of state, head of government, senior politician, judicial or military official and etc. Their spouse, partner, child or parent and close associate are also defined as PEPs.

5.4 An international organization PEP is an individual who is or has been entrusted with a prominent function by an international organization. Their spouse, partner, child or parent and close associate are also defined as international organization PEPs.

5.5 Our Company adopts a more stringent approach to PEP by applying the same standard for all kinds of PEPs.

5.6 If the customer or its associated persons is a PEP, before (i) establishing a business relationship or (ii) continuing an existing business relationship where the customer is subsequently found to be a PEP, apply all the following Enhanced Due Diligence measures: obtaining approval from senior management; taking reasonable measures to establish the customer's source of wealth and the source of the funds; and applying enhanced monitoring to the customer's transactions.

STEP 6: RISK SCORING

6.1 ***C***ustomer's ML/TF risk levels (low, medium or high ML/TF risk) are based on customers' respective risk factors. Customers who are associated with PEPs or classified as high-risk customers due to other reasons should be subject to enhanced due diligence. By adopting a risk-based approach, we determine the extent of the CDD measures, on-going monitoring and risk-mitigation measures based on the ML/TF risk level of the customer. Please make use of ***"F3-Customer Risk Assessment Table".***

6.2 The four risk factors below are used to determine the ML/TF risk level:

a) Country Risk

High-risk jurisdictions are:

- Countries that have been identified by the FATF as jurisdictions with strategic AML/CFT deficiencies;
-
- Countries which are vulnerable to corruption; and
- Countries that are believed to have strong links to terrorist activities

For example, a customer will be considered as having high country risk if it has a high portion of transactions originated from or designated to high-risk jurisdictions; or if its place of registration is relevant to high-risk jurisdictions.

b) Customer Risk

Examples of customers with higher Customer Risk:

- Customers without solid transaction history to prove its business nature
- Customers that have PEPs as its associated persons

c) Product/Service/Transaction Risk

To ensure we maintain the most stringent AML compliance, we classify all the services provided by MSO as high-risk services.

A remittance or FX transaction will be considered as having high-transaction risk due to various reasons, for example:

- abnormal transaction volume or frequency
- transactions irrelevant to customer's background or business nature
- originated from or designated to high-risk jurisdictions
- involving sanctioned parties/jurisdictions
- involving high-risk countries
- conducted before completing CDD procedures for the customers
- conducted before obtaining all the required information as set out in AMLO / AML Guideline

d) Delivery Channel Risk

The distribution channel of products affects the risk profile of a customer. This may include placing FX exchange or remittance orders via online, postal or telephone channels, or conducting KYC through non-face-to-face manner, please refer to paragraph 9.1 for details (But in reality, we do not accept non-face-to-face KYC).

6.3 We need not verify the details of the intermediate companies in the ownership structure of a company. However, complex ownership structures (e.g. structures involving multiple layers, different jurisdictions, trusts, etc.) without an obvious commercial purpose pose an increased risk and may require further steps to ensure that we are satisfied on reasonable grounds as to the identity of the beneficial owners.

6.4 The need to verify the intermediate corporate layers of the ownership structure of a company will depend upon our overall understanding of the structure, its assessment of the risks and whether the information available is adequate in the circumstances for us to consider if it has taken adequate measures to identify the beneficiary owners.

6.5 Where the ownership is dispersed, we should concentrate on identifying and taking reasonable measures to verify the identity of those who exercise ultimate control over the management of the corporate company customer.

STEP 7: PREVENTIVE/MITIGATING MEASURES TO BE IMPLEMENTED ACCORDING TO RESPECTIVE ML/TF RISK LEVEL

7.1 If a customer is classified as having high ML/TF risk level, the responsible staff should obtain further information. Necessary risk-control measures should be taken according to the risk level so calculated, e.g. requesting the customer to provide additional information and/or documents about its business pattern, business nature, source of income/wealth, the rationale of establishing business relationship with us. Requesting

the customer to make its first payment to us through a FATF bank account in its name may be another appropriate measures to mitigate the ML/TF risks relevant to the customer.

7.2 CDD information should be updated periodically according to the ML/TF risk level of the customer, or when a trigger event occurs:

- Normal risk customer: every 3 year
- High risk customer: every 1 year

7.3 Examples of trigger event for CDD review include (not exhaustive):

- Significant transaction[14] is to take place
- The customers' business natures or transaction patterns have been changed substantially Documentation standards change substantially
- When our Company is aware that it lacks sufficient information about the customer
- Reactivation of a dormant customer
- Change in beneficial ownership or control of the customer
- The customers are reported to the JFIU due to their background or their involvement in suspicious transaction(s)
- Our Company identifies that the customers' identity information has been changed substantially.
- The customers apply for suspicious transaction(s), for examples, the applied transactions are deviated from the customers' CDD information, or the transactions are of abnormally high volume, etc.

7.4 Customers relevant to any trigger events for CDD review are prohibited from conduct transactions before their CDD information is renewed.

7.5 Customers are treated as dormant customers if they have not transacted with our Company for 2 years. Dormant customers are required to re-perform CDD in order to reactive their account status.

STEP 8: HANDLING CUSTOMERS WHO HAVE NOT COMPLETE CDD PROCESS

8.1 When we cannot form a reasonable believe that the true identity of a customer is known because the customer does not provide all relevant documents to verify its identity information, we will do the following:

(a) Suspend or terminate the business relationship with the customer unless there is a reasonable explanation

(b) determine whether it is necessary to file a suspicious transaction report if deemed necessary

8.2 CO and responsible officers will follow up with the customers regularly to request for the missing documents. The principle of tolerance is as follows:

(a) Tolerant 30-day delay for missing connected parties' identity verification

[14] "Significant" is not necessarily linked to monetary value. It may include transactions that are unusual or not in line with the FI's knowledge of the customer.

documents, but judgment of CO is needed

(b) Tolerant 90-day for missing address verification, but judgment of CO is needed

8.3 The incomplete CDD status and follow-up record shall be escalated to the senior management on a regular basis.

8.4 In general, further extension should not be allowed unless the delay is due to uncontrollable factors or customer is not identified as high-risk customers. CO shall justify and document the reasons and risk control measures (if necessary).

NON-FACE-TO-FACE CDD REQUIREMENTS

9.1 In situation where it is not practical to perform CDD procedures with customers through a face-to-face manner, or when our Company starts to implement electronic CDD procedures, the responsible staff shall take supplementary measures to verify a customer's identity information, e.g., requesting the customer to take selfie and compare the facial identity of the customer with his identity documents. Further, the first payment made into the customer's account is received from an account in the customer's name with a bank operating in HK or equivalent jurisdiction.

SECTION 5: TRANSACTION MONITORING

REAL-TIME MONITORING

1. For each applied transaction, the responsible staff should justify transactions based on available information from respective request and only execute the transactions which are of no suspicion result identified by Dow Jones. Responsible staff should not execute any transaction if they have any knowledge or suspicion that the transaction or the relevant customer is relating to money laundering, terrorist activities or any criminal activities.

2. When necessary, the responsible staff should request a customer to clarify the nature and purpose of each transaction. Where the source of funds of an applied money service transaction originates from an account held in the name of a person or an entity other than the applicant, the applicant is required to sign ***"F7-Third Party Source Account Declaration"*** to elaborate the reasons of using third party as the source of fund, and the relationship between the applicant and the holder of the source account before the applied transaction will be executed.

3. In situation where customers claim that they apply for the transaction on behalf of a third party, the relationship between the customer and the beneficial is suspicious, the transaction is relevant to jurisdictions with high ML/TF risk or there are suspicious indicators relevant to the transaction arisen, the responsible staff or CO should take necessary actions to control any potential ML/TF risk, these include requesting the beneficial owner/fund originator to perform customer due diligence procedures, explain the relationship between all relevant parties and rationale behind the transaction, review CDD information of the customer or report the transaction to JFIU. The responsible staff should use ***"F6-Unusual Transaction Report"*** to handle such unusual/suspicious transaction[15].

4. If a person claims that he represents a corporate customer to deposit cash into our Company for future transactions, responsible officer must request the person to present his identity document for record, a copy of the identity document should be made for future reference. The person should also sign off a receipt slip. The responsible staff should take necessary actions to ensure the deposited cash matches the instructions of the corporate customer.

5. For incoming funds by cheque or TT relevant to customers' transactions, particulars of source of funds (e.g. Payee Name, Bank Name, and Cheque Number) will be recorded. If beneficiary bank (i.e. the bank receiving customer's fund on behalf of us) requests us to clarify the purpose of transaction, CO or the responsible staff will request with customer to provide further identity information. The information provided by customer should be kept together with other relevant documents of the transaction as transaction record. If customer provides information orally, the responsible staff should record the oral

[15] When a staff submits an Unusual Transaction Report, MLRO or its designate shall return a response to the reporting staff as an acknowledgement. Reminder of the risk of tipping off to avoid the report being released to unauthorized third party.

information in written format and maintained it the same way as other relevant transaction record.

6. If the funds are transferred to/from an account maintained with a bank incorporated in Hong Kong or FATF jurisdiction, it is assumed that the money laundering/terrorist financing risk of the funds are accepted by the bank. Otherwise, CO may request further transaction or CDD information to mitigate the risks that may be incurred by the funds.

NON-REAL TIME MONITORING

7. All the relevant documents (e.g. bank's credit record, customers' written execution and etc.) are known as transaction record, they should be maintained in files or computer systems for purpose of regular review, on-going monitoring and reporting suspicious transactions.

8. If CO or the responsible staff, in the course of conducting periodic transaction record review, indicate that there are executed transactions which show suspicious indicators, they should make use of ***"F6-Unusual Transaction Report"*** to take necessary actions for the control of ML/TF risk, these include requesting customers to give proper explanation. If no proper explanation or justification can be obtained, CO should report the transaction to JFIU.

9. Pursuant to Chapter 5 of the Guideline, CO should regularly monitor business relationship with customers by:
   (a) reviewing documents, data and information relating to the customer to ensure that they are up-to-date and relevant;
   (b) monitoring the activities of the customer to ensure that they are consistent with the nature of business, the risk profile and source of funds; and
   (c) identifying transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose and which may indicate money laundering/terrorist financing.

10. During the exercise of periodic transaction record review, CO will keep a close eye on transactions with the characteristics of:
   (a) Abnormal size
   (b) Abnormal frequent transactions without proper explanation
   (c) Abnormal frequent transactions with the same entity in a short period of time
   (d) Unusual cash deposits
   (e) Transactions relevant to non-FAFT jurisdictions/suspicious geographic origin and etc.
   (f) Transactions deviates from customers' background
   (g) Transactions without apparent economic of lawful purposes

11. Where the basis of the business relationship changes significantly, the responsible staff should carry out further CDD procedures to ensure that the ML/TF risk involved and basis of the relationship are fully understood. Ongoing monitoring procedures must take account of the above changes.

RECORD KEEPING

12. Where transactions that are complex, large or unusual, or patterns of transactions which have no apparent economic or lawful purpose, CO should examine the background and purpose, including where appropriate the circumstances, of the transactions. The findings and outcomes of these examinations will be properly documented in ***"F6-Unusual Transaction Report"*** to assist the regulators, other competent authorities and auditors. Such examinations may include asking the customer questions based on common sense but do not constitute tipping off.

SECTION 6: HANDLING SUSPICIOUS TRANSACTIONS

1 When conducting customer due diligence, real-time monitoring or non-real time monitoring, if staff discover any suspicion which cannot be properly explained by customer or any transactions that are relevant to Restricted Jurisdictions, the responsible staff have to report the transaction to JFIU. All JFIU reports and relevant documents (including feedback and instruction form JFIU after reporting) will be safe-kept by MLRO. All irrelevant staff are prohibited from reviewing the JFIU reports and relevant documents. The soft copies of the JFIU reports and relevant will be maintained in separate computer folder or hard-disk, which can only be reviewed by MLRO or staff designated by MLRO. CO should take necessary actions against specific customers to control ML/TF risk.

2 In case where staff have questions or problems in handling unusual/suspicious transaction, they should report to their direct supervisor, CO or MLRO for their further instructions. These instructions may include investigating customer's transaction records, evaluating customer information and transaction information, reporting to JFIU and etc.

3 The JFIU report must include details of the date of the disclosure, the person who made the disclosure, and information to allow the papers relevant to the disclosure to be located.

4 All staff are prohibited from revealing to any irrelevant person any information which might prejudice JFIU's investigation; otherwise, the staff will be accused of committing criminal crime of tipping off.

5 MLRO and CO should proactively involve in identifying and handling suspicious transaction, this should include regular reviewing ***"F6-Unusual Transaction Report"***.

6 All staff have the obligation to report a transaction if they know or doubt that the transaction may be related to money laundering/terrorist financing. Suspicion is subjective, staff are not necessary to know the nature of the underlying criminal activities. The key is knowing enough about the customer's business to recognize that a transaction, or a series of transactions, is unusual and, from an examination of the unusual, whether there is a suspicion of ML/TF. Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, etc., the transaction should be considered as unusual and staff should be put on alert.

7 The following is a (non-exhaustive) list of examples of situations that might give rise to suspicion in certain circumstances:

- transactions or instructions which have no apparent legitimate purpose and/or appear not to have a commercial rationale
- transactions, instructions or activity that involve apparently unnecessary complexity or which do not constitute the most logical, convenient or secure way to do business
- where the transaction being requested by the customer, without reasonable explanation, is out of the ordinary range of services normally requested, or is outside the experience of the financial services business in relation to the particular customer
- where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that has previously emerged

- where the customer refuses to provide the information requested without reasonable explanation or who otherwise refuses to cooperate with the CDD and/or ongoing monitoring process
- where a customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation
- the extensive use of trusts or offshore structures in circumstances where the customer's needs are inconsistent with the use of such services
- transfers to and from high risk jurisdictions without reasonable explanation, which are not consistent with the customer's declared business dealings or interests
- unnecessary routing of funds or other property from/to third parties or through third party accounts

8 Customer who has been reported to JFIU for a specific transaction will not be exempted for another report to JFIU if such customer is related to another suspicious transaction. Staff should keep reporting suspicious transactions to MLRO or CO even though such suspicious transactions are relevant to customers who have been reported to JFIU previously for same nature of transaction. MLRO or CO is the one to determine if he should make suspicious report to JFIU.

9 A consent response from JFIU to a reported transaction should not be construed as "clean bill of health" for continued operation of the account or an indication that the account does not pose a risk of ML/TF. The responsible staff, CO and MLRO should take reasonable steps to control any ML/TF risk. If JFIU make injunction or restraint order against a customer, the responsible staff should ensure that they can freeze the relevant property that is the subject of the order.

10 We are not obliged to continue business relationships with customers if such action would place us at risk. Management is suggested to indicate any intention to terminate a relationship in the initial disclosure to the JFIU, thereby allowing the JFIU to comment, at an early stage, on such a course of action.

SAFE APPROACH

11 Screen-Ask-Find-Evaluate ("SAFE") approach shall be applied when handling suspicious transactions:

(i) **Screen** the account for suspicious indicators: Recognition of a suspicious activity indicator or indicators
(ii) **Ask** the customer appropriate questions
(iii) **Find** out the customer's records: Review the information already known when deciding if the apparently suspicious activity is to be expected.
(iv) **Evaluate** all the above information: Is the transaction suspicious?

TIPPING-OFF

12. An MSO should be aware that making enquiries to customers, when conducted properly and in good faith, will not constitute tipping off. However, if the MSO reasonably believes that performing the CDD process will tip off the customer, it may stop pursuing the process.

SECTION 7: STAFF TRAINING

1. Staff should be trained in what they need to do to carry out their particular roles with respect to AML/CFT. We shall provide appropriate training to staff accordingly.

2. AML/CFT training will occur:
   (i) at the initiation of the AML Program,
   (ii) when new hires aboard, and
   (iii) at least annually for existing staff.

3. Staff should be made aware of:
   - Our company's and staff's personal statutory obligations and the possible consequences for failure to report suspicious transactions under the DTROP, the OSCO and the UNATMO
   - any other statutory and regulatory obligations that concern our Company's and themselves under Drug Trafficking (Recovery of Proceeds) Ordinance ("DTRPO"), Organized and Serious Crimes Ordinance ("OSCO") and United Nations (Anti-Terrorism Measures) Ordinance ("UNATMO"), United Nations Sanctions Ordinance ("UNSO") and the AMLO, and the possible consequences of breaches of these obligations
   - our Company's policies and procedures relating to AML/CFT, including suspicious transaction identification and reporting
   - any new and emerging techniques, methods and trends in ML/TF to the extent that such information is needed by the staff to carry out their particular roles in our Company with respect to AML/CFT

4. We will monitor and maintain records of who have been trained, when the staff received the training and the type of the training provided. We will also regularly monitor the effectiveness of training.

SECTION 8: RECORD KEEPING

1. All the CDD documents of a customer mentioned in these Procedures should be maintained throughout the continuance of the business relationship with the customer and for a period of at least five years after the end of the business relationship.

2. We should maintain the original or a copy of the documents, and a record of the data and information, obtained in connection with each transaction our Company carries out, both domestic and international, which should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. All these should be kept for a period of at least five (5) years after the completion of a transaction, regardless of whether the business relationship ends during the period.

3. The staff who communicate with customers over the phone for clearance of any anti-money laundering related matters should record such telephone conversation in writing. The written record should be kept with other documents relevant to the specific transaction for future reference.