RIA EXCHANGE LIMITED

AML POLICY DOCUMENT

GLOSSARY OF TERMS

AML	Anti-Money Laundering
AMLO	Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance, Cap 615 (the AMLO)
Beneficial Owner	The individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted.
Business Relationship	A business, professional or commercial relationship between a relevant person (i.e. someone to whom the AMLO apply) and a customer, which is expected by the relevant person, at the time when the contact is established, to have an element of duration.
Cash	Notes, coins and traveller's cheques in any currency.
CCE	The Commissioner of Customs and Excise.
CO	Compliance Officer
Criminal Conduct	Conduct which constitutes an indictable offence under the laws of Hong Kong, or would constitute an indictable offence under the laws of Hong Kong if it had occurred here.
Criminal Property	Any money or other assets which constitutes a person's benefit from criminal conduct.
Customer due diligence (CDD)	Identifying and verifying the identity of the customer and any beneficial owner of the customer, and obtaining information on the purpose of intended nature of the business relationship.
Enhanced due diligence	Additional customer due diligence measure that must be applied:

(EDD)	• Where the customer has not been physically present for identification purposes. • Where the customer is a Politically Exposed Person or • In any other situation which by its nature can present a higher risk of money laundering or terrorist financing
FATF	Financial Action Task Force
Identification	Ascertaining the name of, and other relevant information about, a customer or beneficial owner.
Internal Report	A report made to the Nominated Officer or Compliance Officer.
JFIU	Joint Financial Intelligence Unit
Money Laundering	The term "Money Laundering" means an act intended to have the effect of making any property: (i) That is the proceeds obtained from Criminal Conduct; or (ii) That in whole or in part, directly or indirectly, represents such proceeds, Not to appear to be or to represent such proceeds. Thus the phrase "Money Laundering" covers all procedures to change the identity of illegally obtained money so that it appears to have originated from a legitimate source.
Money Service Business	An undertaking which by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means or which cashes cheques which are made payable to customers.
Occasional transaction	A transaction (carried out other than as part of a business relationship) amounting to USD 1,000 or more, whether the transaction is carried out in a single operation or several operations that appear to be linked.

Ongoing monitoring of a business relationship	• Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile, and • Keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up to date.
Politically Exposed Person (PEP)	An individual who is or has, at any time in the preceding year, been entrusted with prominent public functions, or an immediate family member of such an individual, or a known close associate, of such persons.
Prejudicing an Investigation	The making of any disclosure or falsifying, concealing, or destroying, or being complicit in these, of any documents that are relevant to a money laundering investigation.
Regulated Sector	Persons and firms which are subject to Money Laundering Regulations.
SAR	Suspicious Activity Report made to JFIU.
Senior Management	The directors and senior managers (or equivalent), of a firm who are responsible, either individually or collectively, for management and supervision of the firm's business.
Senior Manager	An individual, other than a director (or equivalent), who is employed by the firm, and to whom the board (or equivalent) or a member of the board, has given responsibility, either alone or jointly with others, for management and supervision.
Simplified due diligence	An exception to the obligation to apply the customer due diligence measures for specified customers, e.g. financial institutions subject to the Money Laundering Directive or equivalent legislation and supervision. It is also available for some categories of products and transactions which may be provided by financial institutions.
Terrorist Financing	The term "Terrorist Financing" means: (a) The provision or collection, by any means, directly or indirectly, of

	any property – (i) With the intention that the property be used; or (ii) Knowing that the property will be used, In whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used); or (b) The making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate; or (c) The collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate.
Tipping off	A tipping-off offence is committed if a person knows or suspects that a disclosure falling under AMLO has been made, and he makes a disclosure which is likely to prejudice any investigation which may be conducted following the disclosure.
Transaction	The provision of any advice by a business or individual to a client by way of business, or the handling of the client's finances by way of business.
Verification	Verifying the identity of a customer, by reference to reliable, independent source documents, data or information, or of a beneficial owner through carrying out risk-based and adequate measures.

INTRODUCTION

This manual is designed to be used by the employees of RIA EXCHANGE LIMITED, as a guide to the AML responsibilities of both the company and the staff.

In particular, it contains the information which all members of staff need to be aware of in order to prevent the business being used to launder the proceeds of crime or terrorist financing. All members of staff are at risk of committing a criminal offence if they assist in a criminal transaction by missing the warning signs.

At the heart of this document is the risk based approach (see below). The risk-based approach means that we focus our resources on the areas of greatest risk.

The possibility of being used to assist with money laundering and terrorist financing poses many risks for our company including:

1. Criminal and disciplinary sanctions

2. Civil action against the firm, as whole and individual directors

3. Damage to reputation leading to a loss of business

These risks must be identified, assessed and mitigated. If we know our customers well and understand their instructions thoroughly, we will be better placed to assess risks and spot suspicious activities. We will always start from the premise that most of our customers are not launderers or terrorist financers but we must assess the risk level particular to our firm and implement reasonable and considered controls to minimise those risks.

No matter how thorough our risk assessment or how appropriate our controls, some criminals may still succeed in exploiting us for criminal purposes. But an effective, risk-based approach and documented, risk-based judgments on individual customers will enable us to justify our position on managing the risk to law enforcement, courts, CCE and JFIU.

POLICY STATEMENT

The Directors are committed to operating the business in a transparent and open manner consistent with their regulatory obligations. The directors and CO will always ensure that all suspicious activities are reported to the authorities.

As part of this commitment RIA EXCHANGE LTD will adopt strict compliance of all applicable AML rules and regulations with specific emphasis on the AMLO (laws in Hong Kong).

RIA EXCHANGE LTD is aware that MSOs have in the past been targets of organised crime seeking to launder the proceeds of illicit activity. RIA EXCHANGE LTD will always seek to disrupt this activity by cooperating fully with the authorities and reporting all suspicious activity to JFUI.

All staff must take steps to ensure compliance with this policy and ensure that they fully understand the material contained in this manual.

It is the policy of RIA EXCHANGE LTD that staff must receive AML training on commencement of their duties. Staff will be given a copy of this manual and will be tested on its contents before starting any client facing duties. The CO holds copies of all training materials. Updated AML training is given annually. Records of all training including dates delivered and by whom are kept both centrally and on staff personnel files.

The CO of RIA EXCHANGE LTD is VINOD MENON. His deputy is NITISH. All issues relating to SAR must be referred to the CO in the first instance.

A copy of this manual will be provided to all RIA's subsidiaries, Branches and all directors, staff and agents.

WHAT IS MONEY LAUNDERING

As stated above, the phrase 'Money Laundering' covers all procedures to change the identity of illegally obtained money so that it appears to have originated from a legitimate source.

Cash is the common medium of exchange in the world of crime, be it Drug Trafficking or Organized crime. Criminals need to seek ways and means to change the form of such illegally transacted cash.

Hence it is necessary for them to:

1. Conceal the true ownership and the origin of the money.
2. Change the form of money
3. Take control of the money

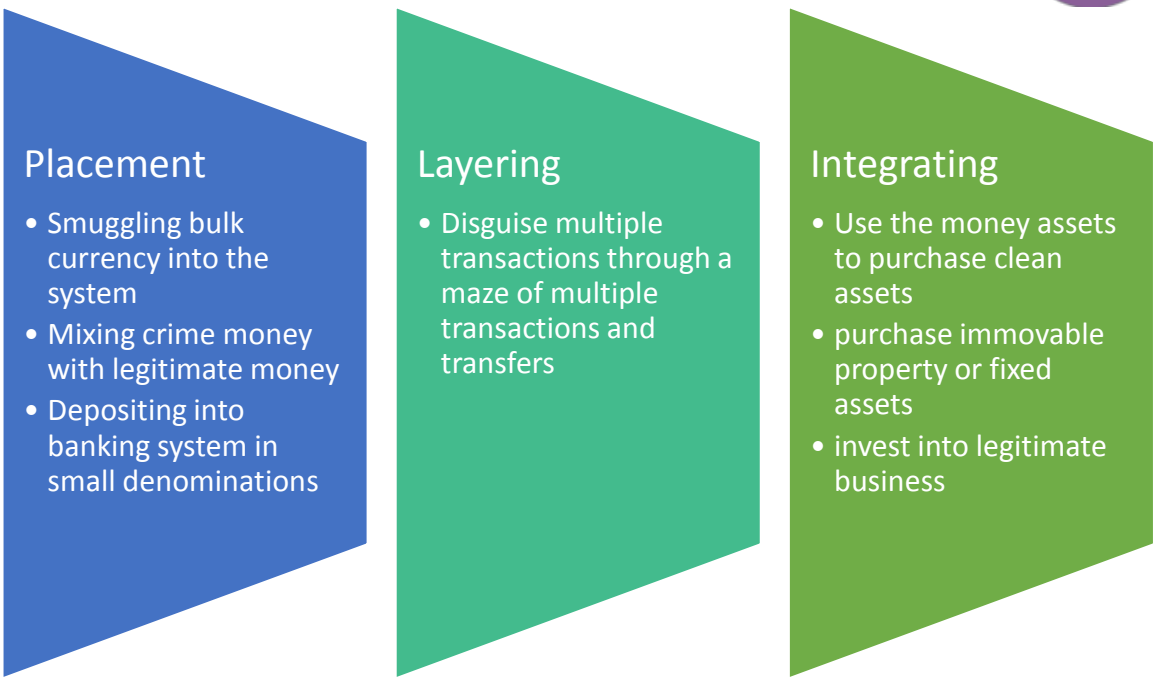
This is achieved by feeding the illegally obtained cash into the financial system, through deposit into the banking network or through financial intermediaries like RIA.

Stages of Money Laundering

There are three stages of Money Laundering:

a. Placement – the physical disposal of illegally obtained cash proceeds.
b. Layering – creating complex layers of financial transactions with the purpose of disguising audit trail, provide anonymity and thereby separate illicit cash from their source.
c. Integrating – the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds

The above is summarised as follows:


Placement
• Smuggling bulk currency into the system
• Mixing crime money with legitimate money
• Depositing into banking system in small denominations
Layering
• Disguise multiple transactions through a maze of multiple transactions and transfers
Integrating
• Use the money assets to purchase clean assets
• purchase immovable property or fixed assets
• invest into legitimate business

ROLES AND RESPONSIBILITIES

Senior Management

Responsible for overall compliance policy of RIA EXCHANGE LTD and ensuring adequate resources are provided for the proper training of staff and the implementing of risk systems. This includes computer software to assist in oversight. Senior management will be sent monthly updates by the CO on compliance. They will also receive and consider the annual CO report and implement any recommendations made within it. Assistance may be given to the CO in the preparation of the AML manual.

CO

Responsible for receiving internal disclosures and making reports to JFIU. First point of contact for all compliance issues from staff. Prepares annual report for consideration of senior management and conducts risk assessments of compliance systems. Undertakes regular random analysis of transactions including assessment of documentary evidence provided by customers. Visits agents and overseas branches to ensure compliance with group strategy. Assists in making any necessary amendments to AML manual in line with increase/decrease in risk. Considers all compliance issues for group undertakings including daily consideration of compliance forms.

Staff

Responsible for considering the AML manual and understanding responsibilities. Ensure company procedures adhered to and obtain all documentary evidence as outlined within manual. Ensure that all suspicious circumstances are reported to CO.

RIA EXCHANGE LIMITED BUSINESS PROFILE

RIA EXCHANGE LTD is an authorised payment institution licensed by CCE, in Hong Kong. We do not have any branches. We provide money exchange and remittance facilities to all members of the public, who opens an account with us.

ANTI MONEY LAUNDERING SYSTEMS AND CONTROLS

Under the AMLO, we are required to establish appropriate risk-sensitive policies and procedures in order to prevent activities related to money laundering and terrorist financing including those policies and procedures, which provide for:

- Identification and scrutiny of complex or unusually large transactions, unusual patterns of transactions with no apparent economic or lawful purpose and other activities regarded by the regulated person as likely to be of the nature of money laundering or terrorist financing;
- Prevention of use of products favouring anonymity;
- Determination of whether a client is a PEP;
- Customer due diligence i.e. procedures designed to acquire knowledge about our customers and to verify their identity, as well as monitor business relationships and transactions before executing the remittances;
- Internal reporting including the appointment of a CO to receive the money laundering reports required under law and a system for making those reports;
- Record keeping, including details of customer due diligence and supporting evidence for business relationships, which need to be kept for seven years after the end of a relationship and records of transactions, which also need to be kept for seven years;
- Internal control, risk assessment and management, compliance monitoring, management and communication; and
- In addition, we are required to take measures to make employees aware of the law relating to money laundering and terrorist finance, and to train those employees in how to recognise and deal with transactions which may be related to money laundering or terrorist financing.

THE RISK BASED APPROACH

- A risk based approach allows us to target resources and effort where the risk is greatest and, conversely, reduce requirements where the risk is low.

- We must establish adequate and appropriate policies and procedures relating to risk assessment and management in order to prevent operations related to money laundering or terrorist financing. We have done this by preparing a risk matrix to be adopted by all staff.

- We must :
  (a) determine the extent of customer due diligence measures on a risk-sensitive basis depending on the type of client, business relationship, or services to be provided;
  (b) be able to demonstrate to CCE that the extent of customer due diligence measures is appropriate in view of the risks of money laundering and terrorist financing. Our CDD measures are set out in this manual.

- We are required to take a risk-based approach and have adequate measures to verify the identity of beneficial owners so that we are satisfied that we know who the beneficial owner of our customer is and what the control structure of a corporate client is. Every personal customer is asked about any beneficial owners on compliance form __. Corporate customers undergo thorough beneficial ownership assessment in line with our obligations under the AMLO.

- We are required to scrutinise transactions and other activities throughout the course of any business relationship to ensure consistency with our knowledge of our customers, their business and risk profile. The CO will conduct ongoing monitoring of all high risk accounts identified by the senior management. In addition to this the CO will undertake random monthly checks upon customer accounts and provide a report to the board of directors on his findings.

- We must also keep up to date the information collected in applying CDD measures. All ID will be retaken on the expiry of any documents used to verify customers. Customer accounts will be placed on hold until the relevant CDD checks have been undertaken or documents provided.

- We must apply CDD measures at appropriate times to existing clients on a risk-sensitive basis. The CO will assess the existing CDD database to identify those customers that may require further/updated CDD checks.

- We must apply EDD where the customer is of another MSO. The CO will visit the MSO to ensure that they are carrying out CDD and checking the relevant records for specific transactions.

- In compliance with the Privacy Ordinance, when the customer is another MSO we may not request full information from their customer, just the full name of the customer, amount, recipient name and country and the unique reference number of each transaction. However the MSO must be prepared to disclose any information if required by us. Also we conduct due diligences on the MSO before starting a relationship with them to certify that the MSO carries out appropriate Customer Due Diligence. Where the customer is a money transmission business we check if they are registered with the relevant authorities. If they are not registered we will not accept the customer.

- We must apply EDD on third party payments. RIA only accepts Third Party Payments for Countries that are not considered high risk jurisdictions by FATF and when the beneficial owner is identified.

- We apply EDD on the overseas recipient requesting the proof of payment such as invoices and checking if they are genuine.

- When the customer is a corporate customer, we apply EDD before starting the relationship with the customer. We will check the company's and Directors' names on sanctioned lists, Safe Credit website, director's disqualified list, the purpose to send the transaction, the annual turnover, the list of customer's beneficiaries and the relationship with the them, beneficiaries' names on FATF lists and other sanctioned lists. We will also define limits of amounts a corporate customer can send in a given period.

- When an overseas customer wants to carry out a transfer of funds to a beneficiary in HK, his KYC documents must be verified by our correspondents and made available to us, on demand.

- We provide payment services to agents subject to prior acceptance by us. To comply with AMLO requirement, we must obtain from the agent: name and address of the agent, description of AML Internal controls mechanism (must meet the RIA procedure), identification of directors and responsible persons, and fit and proper test assessment. New agents will only start operating after the authorisation from statutory authorities is granted.

- We have established internal procedures for investigating any complaint that may be made against us in relation to any transaction. In accordance with our complaints procedure, any complaint a customer may make relating to any transaction must be made or confirmed to us in writing to the CO at 16B Man Hing Commercial Building, 79-83 Queen's Road, Central, Hong Kong, or by electronic message to vinod@riaexchange.com. We will respond to the customer promptly. If the customer is still dissatisfied following our response to any complaint, he has a right to refer the complaint concerning the transaction to the the Director at 16B Man Hing Commercial Building, 79-83 Queen's Road, Central, Hong Kong or by electronic message to sailesh@riaexchange.com.

OUR MONEY LAUNDERING RISKS

AND WHAT WE WILL DO TO REDUCE THEM

Risk	Explanation	Triggers	Mitigating these risks
Customers	It is important to have a general understanding of the risk profile of our customers based on the type of customers, purpose of transactions, source and destination of funds and the expected value of frequency of transactions. This will enable the identification of unusual transactions or patterns of transactions without an obviously economic or lawful purpose, which could be suspicious.	Face-to-face customers conducting transactions of more than HKD 8,000 Beneficial ownership Customer undertaking transactions on behalf of third party Unwillingness of the customer to provide information	Verify the customers' identity by physical inspection of their original HKID or passport and proof of address Determine on whose behalf an account is maintained, corroborating wherever possible with evidence. In addition to verify and recording the identity of the customer, we should also take the full particulars of the instructing party If the customer fails to co-operate in the CDD process, we should refuse the transaction.
Product / Transaction Types Overseas Remittance	Overseas remittances can be used by criminals and terrorists to move	Complex or unusually large transactions.	We have put in place robust systems to identify unusual

	criminal cash outside conventional banking system in order to reduce the likelihood of detection.	Unusual patterns of transactions which have no apparent economic or visibly lawful purpose. A sudden increase in business from an existing customer that is not consistent with known sources of income. Peaks of activities at particular locations or at particular times. Large number of transactions slightly below the limits for verification of ID.	transactions or patterns of transactions. Each client is set a limit of how much they may send without further information being required. Staff should also consider whether Suspicious circumstances exist and refer to the reporting procedures within the manual if necessary.
Channels Cash Transactions Agency Relationships	Agency relationship; where we are dependent on an agent for customer contact this can create a risk of regulatory non-compliance and weaknesses that could be exploited by criminals or terrorists.	Little communication exists between the money transmission business and the agents.	We will always ensure agents undergo “fit and proper” type scrutiny.
Geographies	The countries in which we operate and to which we send monies to may give rise to a higher risk of money laundering because of a generally higher crime rate or likelihood of money laundering or terrorist financing.	Source or destination of funds from or to areas of high level of drugs crime, terrorist activity etc. Lack of knowledge regarding origin or destination of funds.	We will always keep up to date with news on money laundering or terrorist financing cases. We will screen all transactions through OFAC / Dow Jones List.

			In appropriate cases, we will do Enhanced Due Diligence.

CUSTOMER DUE DILIGENCE

Corporate Customers

The following documents or information should be obtained in respect of corporate customers that are registered in Hong Kong (comparable documents, preferably certified by qualified persons such as lawyers or accountants in the country of registration, should be obtained for those customers which are not registered in Hong Kong):

(a) Certificate of Incorporation and Business Registration Certificate;

(b) Memorandum and articles of association;

(C) Resolution of the board of directors to open an account and confer authority on those who will operate it; and

(D) Satisfactory evidence of the identity of the principal shareholders, at least two directors (including the managing director) and all authorized signatories in line with the requirements for individual applicants, as well as evidence of the nature of the business.

This is in addition to recording and verifying the identity of any individual purportedly representing the company. The account opening form should specify the individual's authority to transact on their behalf.

Any change in the ownership of the company should be verified by obtaining copies of Annual Returns filed every year. If there is a complex structure of ownership by way of multiple holding subsidiary relationship, we should ensure that information of the ultimate beneficiary at the end of the hierarchy tree is obtained. If this information is not available, we should refuse to transact with the client.

Run the name of the corporate customer and all its' directors and shareholders on the OFAC / Dow Jones List to ensure that there are no publicly available adverse information relating to them.

Unincorporated Businesses

In the case of partnerships and other unincorporated business customers, satisfactory evidence should be obtained of the identity of the managing partners.

A declaration by the firm giving the list of partners should be obtained on an annual basis. Satisfactory evidence of the identity of the principle partners should be obtained.

This is in addition to recording and verifying the identity of the individual who performs the transaction.

Run the name of the partners or sole proprietor on the OFAC / Dow Jones List to ensure that there are no publicly available adverse information relating to them.

Agency Relationships

The Company has multiple Agency Relationships to support Inward and Outward remittances. In these cases, the following documents should be obtained:

a. Institution Profile
b. Organisation Chart / Structure of the Institution
c. Trade License / Business Registration / Other Regulatory Licences as may be applicable in that country.
d. Certificate of Incorporation
e. Memorandum and Articles of Association
f. Duly filled AML / KYC Questionnaire
g. Passport copies of all directors and principle shareholders
h. AML Policy and Procedures

Individual Walk-in customers

Obtain a copy of the HKID / Passport and the proof of address for walk-in customers. Also inquire into the source of funds and where required, proof of the source of funds, such as invoice copies may be obtained. Enquire into the purpose of remittance.

Where transaction appears to be of suspicious nature, submit the SAR to CO.

Run the name of the individual on the OFAC / Dow Jones List to ensure that there are no publicly available adverse information relating to them.

RECORD KEEPING REQUIREMENTS

Record Keeping Requirements for Remittance Transactions of $8,000 or More

Record keeping is vital to ensure that law enforcement authorities have sufficient opportunity to reconstruct transactions for investigation.

Section 24C of OSCO requires that for all remittance transactions of $8,000 or more or its foreign currency equivalent, businesses must record and retain the following information:

Outward remittance to a place outside Hong Kong

(a) Transaction reference number

(b) Transaction type, currency, amount and value date of the remittance

(c) Date of remitter's instructions

(d) Instruction details (including name, address and account number of beneficiary, name and address of beneficiary bank, and remitter's message to beneficiary, if any)

(e) Name, HKID number (or any other document of identity or travel document number with place of issue) of remitter or his representative must be verified if he appears in person

(f) Telephone number and address of remitter

Inward remittance from a place outside Hong Kong

(a) Transaction reference number

(b) Transaction type, currency, amount and value date of the remittance

(c) Date of remitter's instructions

(d) Instruction details (including name and address of beneficiary, name and address of remitter and remitting bank, and remitter's message to beneficiary, if any)

(e) Name and identity card number (or any other document of identity or travel document number with place of issue) of beneficiary which must be verified where the beneficiary appears in person (F) Telephone number and address of remitter.

Money exchange transactions, exceeding $ 100,000

(a) Transaction reference number

(b) Date and time of transaction

(c) Currencies and amount exchanged

(d) Exchange rate

(e) Name, identity card number (or any other document of identity or travel document number with place of issue) of customer which must be verified

(f) Telephone number and address of customer

Section 24C of OSCO requires the above information to be retained for six years1 after the date of the transaction.

Failure to record and keep the prescribed records is an offence subject to a maximum fine of $100,000 and 3 months imprisonment.

An important objective is for businesses at all stages in a transaction to be able to retrieve relevant information, to the extent that it is available, without undue delay.

Although businesses are not required by law to verify a customers' address, they may request verification if they have doubts as to the accuracy of the information provided, e.g. by requesting sight of a recent utility or rates bill, etc. If the customer is unwilling to provide his address and telephone number, the transaction should be refused.

Retention may be by way of original documents, stored on microfilm, or in computerized form in situations where the records relate to on-going investigations, or transactions that have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed.

Originator Information Accompanying Remittance Transactions of $8,000 or more

An ordering business (i.e. the originator) should for all remittance transactions of $8,000 or more or its foreign currency equivalent always include in the remittance message:

(a)The name of the originating customer;

(b) the customer's account number where one exists or a unique transaction number; and

(c) the address of the originating customer or, alternatively , the customer's Hong Kong identity card number or passport number, or date and place of birth.

In accordance with international best practice, an ordering business may choose not to include any of the above information in the remittance message accompanying a remittance of less than $8,000 or its foreign currency equivalent.

An ordering business should adopt a risk-based approach to check whether certain remittances may be suspicious, taking into account such factors as the identity of the beneficiary, the destination and amount of the remittance, etc.

In particular, an ordering business should exercise care if there is suspicion that a customer may be effecting a remittance transaction on behalf of a third party. If a remittance carries the name of a third party as the ordering person or otherwise does not appear to be consistent with the usual business / activity of the customer, the customer should be asked to provide further explanation of the nature of the remittance.

A business acting as an intermediary in a chain of remittances should ensure that the information in paragraph 9.1 remains with the remittance message throughout the payment chain.

A business handling incoming remittances for a beneficiary valued at $8,000 or more or its foreign currency equivalent should screen the remittance messages to ensure they contain complete originator information.

The absence of complete originator information may be considered as a factor in assessing whether a remittance is suspicious and, if appropriate, reported to Ria Exchange Limited in accordance with the procedure detailed in Section 16. The business may also need to consider restricting or terminating its relationship with a remitting business that fails to incorporate adequate originator information in remittance messages for transactions valued at $8,000 or more.

Existing Customer Accounts

Businesses should take steps to ensure that the records of existing customers remain up-to-date and relevant. Where necessary, additional evidence of the identity of existing customers should be obtained to ensure that these comply with the businesses' current standards.

To achieve this, a business should undertake periodic reviews of existing records of customers. An appropriate time to do so is upon certain trigger events. These include:

(a) when a significant or unusual transaction is to take place;

(b) when there is a material change in the way the account is operated;

(c) when the businesses' customer documentation standards change substantially; or

(d) When the business is aware that it lacks sufficient information about the customer.

(e) On the annual anniversary of the formation of the company, when BR is due for renewal.

On-going Monitoring

Businesses should take steps to ensure that the records of existing customers remain up-to-date and relevant. Where necessary, additional evidence of the identity of existing customers should be obtained to ensure that these comply with the businesses' current standards.

In order to satisfy its legal and regulatory obligations, a business needs to have systems in place to enable it to identify and report suspicious transactions. It is not enough to rely simply on the initiative of front-line staff to make ad hoc reports. It is advisable for a business to have management information systems (MIS) to provide managers and compliance officers with timely information on a regular basis to enable them to detect patterns of unusual or suspicious activity.

MIS reports used for monitoring purposes should be capable of identifying transactions that are unusual either in terms of amount (for example, by reference to predetermined limits for the customer in question or to comparative figures for similar customers), type of transaction, or other relevant risk factors.

This also requires the business to have a good understanding of what is normal and reasonable activity for particular types of customers, taking into account the nature of the individual customer's business. Among other measures, a business should act appropriately to satisfy itself about the source and legitimacy of funds to be credited to a customer's account. This is particularly the case where large amounts and/or higher risk customers are involved.

A further relevant consideration in respect of funds derived from outside Hong Kong is whether the transfer of such funds may have breached the exchange controls of the country of origin.

Politically Exposed Persons (PEPs)

PEPs are defined as individuals being, or who have been, entrusted with prominent public functions, such as heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of public organisations and senior political party officials. The concern is that there is a possibility, especially in countries where corruption is widespread, that such PEPs may abuse their public powers for their own illicit enrichment through corrupt activities.

Business relationships with individuals holding important public positions as well as persons or companies clearly related to them, (i.e. family members, close associates, etc.) expose businesses to particularly significant reputation or legal risks. There should be enhanced due diligence in respect of such PEPs, such as the verification of origins and circumstances of the transaction.

Whilst it is acknowledged that the majority of transactions are performed on behalf of occasional customers, business should Endeavour to screen such transactions for the involvement of PEPs, their relatives or close associates. Businesses are expected to be vigilant and when in doubt gather sufficient information from a customer, and check publicly available information to establish whether the customer is a PEP.

A risk-based approach may be adopted for identifying PEPs and focus may be put on persons from countries that have a higher prevalence of corruption (reference can be made to for example to publicly available information such as the Corruption Perceptions Index

The involvement of a PEP in a transaction may be a factor in determining whether or not to file a

disclosure.

Businesses should also ascertain the source of funds before accepting a PEP as customer. The decision to conduct a transaction on behalf of a PEP should be taken at a senior management level.

Risk factors a business should consider in handling a business relationship (or potential relationship) with a PEP include:

(a) Any particular concern over the country where the PEP is from, taking into account his position;

(b) Any unexplained sources of wealth or income (i.e. value of assets owned not in line with the PEP's income level);

(c) Expected receipts of large sums from governmental bodies or state-owned entities;

(d) Source of wealth described as commission earned on government contracts;

(e) Request by the PEP to associate any form of secrecy with a transaction; and

(f) Use of accounts at a government-owned bank or of government accounts as the source of funds in a transaction.

Suspicious Transactions

As the types of transactions that may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. A suspicious transaction will often be one, which is inconsistent with a customer's known legitimate business or personal activities or with the normal business for that type of account. Therefore, the first key to recognition is knowing enough about the customer's business to recognize that a transaction, or a series of transactions, is unusual.

Reporting of Suspicious Transactions

Section 25A(1) of both DTROP and OSCO and section 12 of UNATMO impose a statutory duty on every person, who knows or suspects that any property is the proceeds of crime or terrorist property to make a disclosure (a suspicious transaction report) to an authorized officer.

The Police and Customs and Excise Department jointly operate Ria Exchange Limited. The unit is housed within Police Headquarters in Wanchai and its primary responsibilities are the reception, analysis and dissemination of suspicious transaction reports (STR).

In addition to acting as the point for receipt of STR made by any organization or individual, the unit also acts as domestic and international advisors on money laundering generally and offers practical guidance and assistance to the financial sector on money laundering and terrorist financing. The Unit is also responsible for the day-to-day maintenance of the register of remittance agents and money changers.

The obligation to report is on the individual who becomes suspicious of a transaction. Each institution should appoint a designated officer or officers (Compliance Officer(s)) who should be responsible for reporting where necessary, in accordance with section 25A of both DTROP and OSCO and section 12 of

UNATMO and to whom all internal reports should be made.

Compliance Officers should keep a register of all reports made to the Ria Exchange Limited and all reports made to them by employees. Compliance Officers should provide employees with a written acknowledgement of reports made to them, which will form part of the evidence that the reports were made in compliance with the internal procedures.

Where an employee of a business knows that a customer has engaged in criminality and where the customer exchanges or transfers funds, this information should be promptly reported to the Compliance Officer who, in turn, should immediately report the details to the Ria Exchange Limited.

Where an employee of a business suspects or has reasonable grounds to believe that a customer might have engaged in criminality and where the customer exchanges or transfers funds, this information must promptly be reported to the Compliance Officer. The Compliance Officer must promptly evaluate whether there are reasonable grounds for such suspicion and must then immediately report the case to the Ria Exchange Limited unless he must considers, that there are no reasonable grounds to support the suspicion. In any case, the Compliance Officer’s findings and supporting reasons should be documented and feedback to the reporting employee.

Businesses must take steps to ensure that all employees concerned with the holding, receipt, transmission of funds (whether in cash or otherwise) are aware of these procedures and that it is a criminal offence to fail to report either knowledge or circumstances which give rise to a reasonable suspicion of criminality.

Businesses should refrain from carrying out transactions which they know or suspect to be related to money laundering until they have informed the Ria Exchange Limited which consents to the business carrying out the transactions. Where it is impracticable to refuse the transaction or if this is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering operation, businesses may carry out the transactions and notify the Ria Exchange Limited on their own initiative and as soon as it is reasonable for them to do so.

Where it is known or suspected that a report has already been disclosed to the Ria Exchange Limited and it becomes necessary to make further enquiries of the customer, great care should be taken to ensure that the customer does not become aware that his name or activities have been brought to the attention of the law enforcement agencies.

Following receipt of a disclosure and analysis by Ria Exchange Limited, the information may be referred to trained financial investigation officers in the law enforcement agencies for further investigation including seeking supplementary information from the institution making the disclosure, and from other sources. Discreet enquiries may be made to confirm the basis for suspicion.

Access to the disclosed information is restricted to financial investigating officers within the law

enforcement agencies. In the event of a prosecution, production orders will be obtained to produce the materials to court. Section 26 of both DTROP and OSCO and section 12 of UNATMO imposes strict restrictions on revealing the identity of the person making the disclosure. Maintaining the integrity of the relationship, which has been established between law enforcement agencies and the financial sector, is considered to be of paramount importance.

All STR are dealt with in the strictest confidence as required by the provisions of the three ordinances (DTROP, OSCO and UNATMO).

THE LAW

In 1990, the FATF, put forward forty recommendations aimed at improving national legal systems, enhancing the role of financial systems, and strengthening international co-operation against money laundering. Hong Kong, China is a member of the FATF and is required to be fully compliant with these forty recommendations.

Legislation has been developed in Hong Kong to address the problems associated with the laundering of proceeds from drug trafficking, serious crimes, and more recently terrorist financing. The Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP) came into force in September 1989. It provides for the tracing, freezing, and confiscation of the proceeds of drug trafficking and creates the criminal offence of money laundering in relation to such proceeds.

The Organized and Serious Crimes Ordinance (OSCO), which was modelled on the DTROP, was brought into operation in December 1994. It extends the money laundering offence to cover the proceeds of indictable offences in addition to drug trafficking.

Amendments to both Ordinances were made and came into effect on 1 September 1995. These amendments have tightened the money laundering provisions in both Ordinances and have a significant bearing on the duty to report suspicious transactions. In particular, there is now a clear statutory obligation to disclose knowledge or suspicion of money laundering transactions.

Section 25(1) of DTROP and OSCO creates the offence of dealing with any property, knowing or having reasonable grounds to believe it in whole or in part directly or indirectly represents the proceeds of drug trafficking or of an indictable offence respectively. These offences carry a maximum sentence of 14 years' imprisonment and a maximum fine of $5 million.

It is a defence under section 25(2) of both DTROP and OSCO for a person to prove that he intended to disclose as soon as is reasonable such knowledge, suspicion or matter to an authorized officer, or has a reasonable excuse for his failure to make a disclosure in accordance with section 25A(2) of the Ordinances.

Section 25A(1) of both DTROP and OSCO impose a statutory duty on a person, who knows or suspects that any property in whole or in part directly or indirectly represents the proceeds of drug trafficking, or was or is intended to be used in that connection, to make a disclosure to an authorized officer. Section 25A(7) makes it an offence for a person to fail to make such disclosure. The offence carries a maximum penalty of a fine of $50,000 and imprisonment for 3 months.

It should be noted that section 25(4) of OSCO provides that references to an indictable offence in section 25 and 25A include a reference to conduct, which would constitute an indictable offence if it had occurred in Hong Kong. That is to say, it shall be an offence for a person to deal with the proceeds of crime, or fail to make the necessary disclosure under section 25A(1) even if the principal crime is not committed in Hong Kong provided that it would constitute an indictable offence if it had occurred in Hong Kong.

Section 25A(2) of DTROP and OSCO provides that if a person who has made the necessary disclosure does any act in contravention of section 25(1) and the disclosure relates to that act he does not commit an offence if –

(a) The disclosure is made before he does that act and the act is done with the consent of an authorized officer; or
(b) The disclosure is made after the person does the act and the disclosure is made on the person's own initiative and as soon as it is reasonable for him to make it.

Section 25A(3) of DTROP and OSCO provides that disclosures made under section 25A(1) shall not be treated as a breach of contract or of any enactment restricting disclosure of information, and shall not render the person making the disclosure liable in damages for any loss arising out of disclosure. Therefore businesses need not fear breaching their duty of confidentiality owed to customers when making a disclosure under the Ordinances.

Section 25A(4) of DTROP and OSCO extends the provisions of section 25A to disclosures made by an employee to an appropriate person in accordance with the procedures established by his employer for the making of such disclosure in the same way as it applies to disclosures to an authorized officer. This provides protection to employees of authorized institutions against the risk of prosecution where they have reported knowledge or suspicion of money laundering transactions to the person designated by their employers.

A "tipping-off" offence is created under section 25A(5) of DTROP and OSCO, under which a person commits an offence if knowing or suspecting that a disclosure has been made, he discloses to any other person any matter which is likely to prejudice an investigation into money laundering activities. The "tipping-off" offence carries a maximum penalty of three years' imprisonment and a fine of $500,000 under both DTROP and OSCO.

The Organized and Serious Crimes (Amendment) Ordinance 2000 came into operation on 1 June 2000. It required remittance agents and money changers to keep records of customers' identity and particulars of remittance and exchange transactions of $20,000 or more, or of an equivalent amount in any other currency.

On 26 January 2007, the Organised and Serious Crimes Ordinance (Amendment of Section 24C(1) and Schedule 6) Notice 2006 came into operation. This lowered the threshold for customer identification and record keeping from $20,000 to HK$8,000.

Where a business suspects that a transaction is related to money laundering, it should promptly make a report to the JFIU. Precise details on how to file a report can be found in Section 15.

Terrorist Financing

Terrorist financing generally refers to the carrying out of transactions involving funds that are owned by terrorists, or that have been, or are intended to be, used to facilitate the commission of terrorist acts. This has not previously been explicitly addressed under money laundering legislation where the focus is on the handling of criminal proceeds, i.e. the source of funds is what matters. In terrorist financing, the focus is on the destination or use of funds, which may have been derived from legitimate sources.

Since 9/11 the FATF has expanded its scope of work to cover matters relating to terrorist financing. In this context, it has produced nine Special Recommendations on Terrorist Financing.

The United Nations Security Council (UNSC) has passed various resolutions to require sanctions against designated terrorists and terrorist organizations. In Hong Kong, regulations issued under the United Nations (Sanctions) Ordinance give effect to these UNSC resolutions. In particular, the United Nations Sanctions (Afghanistan) Regulation provides, among other things, for a prohibition on making funds available to designated terrorists. The list of designated terrorists is published in the Gazette from time to time.

In addition, the United Nations (Anti-Terrorism Measures) Ordinance (UNATMO) was enacted on 12 July 2002. This ordinance implements the mandatory elements of the UNSC Resolution 1373. The latter is aimed at combating international terrorism on various fronts, including the introduction of measures against terrorism financing. The UNATMO also implements the most pressing elements of the FATF's nine Special Recommendations.

Section 7 of the UNATMO prohibits the provision or collection of funds for terrorists or terrorist associates. This offence carries a maximum of 14 years imprisonment and an unspecified fine. As with the above-

mentioned Regulations, a list of terrorist names will be published in the Gazette from time to time for this purpose.

Section 12(1) of the UNATMO also makes it a statutory requirement for a person to report his knowledge or suspicion that any property is terrorist property to an authorized officer. Section 14(5) makes it an offence for a person to fail to make such a disclosure. The offence carries a maximum penalty of a fine of $50,000 and imprisonment for 3 months.

Section 12(2) of the UNATMO provides that if a person who has made the necessary disclosure does any act in contravention of section 7 (see paragraph 4.5 above) and the disclosure relates to that act he does not commit an offence if –

(a) The disclosure is made before he does that act and the act is done with the consent of an authorized officer; or
(b) The disclosure is made after the person does the act and the disclosure is made on the person's own initiative and as soon as it is reasonable for him to make it.

Section 12(3) of UNATMO provides that disclosure made under section 12(1) (see paragraph 4.6 above) shall not be treated as breach of contract or of any enactment restricting disclosure of information and shall not render the person making the disclosure liable in damages for any loss arising out of disclosure. Therefore, institutions need not be concerned about breaching their duty of confidentiality owed to customers when making a disclosure under the Ordinances.

Section 12(4) of the UNATMO extends the provisions of section 12 to disclosures made by an employee to an appropriate person in accordance with the procedures established by his employer for the making of such disclosure in the same way as it applies to disclosures to an authorized officer. This provides protection to employees of authorized institutions against the risk of prosecution where they have reported knowledge or suspicion of terrorist financing transactions to the person designated by their employers.

A "tipping-off" offence is created under section 12(5) of the UNATMO under which a person commits an offence if knowing or suspecting that a disclosure has been made; he discloses to any other person any matter which is likely to prejudice an investigation into terrorist financing activities. The "tipping-off" offence carries a maximum penalty of three years' imprisonment and an unspecified fine.

A business should take measures to ensure compliance with the relevant regulations and legislation on terrorist financing. The legal obligations of the business and those of its staff should be well-understood and adequate guidance and training should be provided to the latter. The systems and mechanisms for identification of suspicious transactions should cover terrorist financing as well as money laundering.

It is particularly vital that a business should be able to identify and report transactions with terrorist suspects. To this end, a business should ensure that it maintains a database of names and particulars of terrorist suspects, which consolidates the various lists (which may include lists of terrorists, terrorist organizations, their agents and terrorist property) that have been made known to it. Alternatively, a business may arrange to secure access to such a database maintained by third party service providers.

Such a database should, in particular, include the lists published in the Gazette and those designated under the US Executive Order of 23 September 2001. The database should also be subject to timely updates whenever there are changes, and should be made easily accessible by staff for the purpose of identifying suspicious transactions.

A business should check the names of both existing and new customers against the names in the database. It should be particularly alert for suspicious remittances and should bear in mind the role which non-profit organizations are known to have played in terrorist financing.

The FATF issued a paper entitled “Guidance for Financial Institutions in Detecting Terrorist Financing” in April 20021. The document describes the general characteristics of terrorist financing with case studies illustrating the manner in which law enforcement agencies were able to establish a terrorist financing link based on information reported by financial institutions.

A business should acquaint itself with the FATF paper and should use it as part of its training material for staff.

It should be noted that the list of characteristics only serves to show the types of transaction that could be a cause for additional scrutiny if one or more of the characteristics is present. The parties involved in the transaction should also be taken into account, particularly when the individuals or entities appear on a list of suspected terrorists.

Where a business suspects that a transaction is terrorist-related, it should make a report to the JFIU. Even if there is no evidence of a direct terrorist connection, the transaction should still be reported to the JFIU if it looks suspicious for other reasons.

In 1990, the FATF put forward 40 recommendations (now known as the “40 Recommendations”) aimed at improving national legal systems, enhancing the role of financial systems, and strengthening international co-operation against money laundering. These 40 Recommendations are now recognised as the international standard to prevent money laundering. In October 2001 and October 2004, the FATF supplemented the 40 Recommendations with 9 Special Recommendations on Terrorist Financing. Hong Kong, as a major international finance centre and a member of the FATF, is required to be fully compliant with all 40 + 9 Recommendations.

To ensure compliance, remittance and money changing businesses should have in place the following policies, procedures and controls:

(a) Businesses should issue a clear statement of policies in relation to anti-money laundering and counter terrorist financing, adopting current regulatory requirements. This statement should be communicated in writing to all management and relevant staff whether in branches, departments, or subsidiaries, and should be reviewed on a regular basis.

(b) Instruction manuals should set out the businesses' procedures for:

- Occasional transactions;
- Account opening;
- Client identification;
- Record keeping; and
- Reporting of suspicious transactions.

(c) Businesses should actively seek to promote close co-operation with law enforcement authorities, and should identify a single reference point within their organization (usually a compliance officer) to which staff are instructed to report suspected money laundering or terrorist financing transactions promptly. This reference point should have a means of liaison with the Ria Exchange Limited, which is responsible for the analysis and dissemination of such reports to the appropriate law enforcement agency. The role and responsibilities of this reference point in the reporting procedures should be clearly defined.

Measures should be undertaken to ensure that staff are educated and trained on matters contained in this Guideline, both as part of their induction procedures and at regular future intervals. The aim is to generate and maintain a level of awareness and vigilance among staff, so as to enable a report to be made if suspicions are aroused. (e) Businesses should instruct their internal audit/inspection departments to verify, on a regular basis, compliance with policies, procedures, and controls against money laundering and terrorist financing activities.

FORMS

SUSPICIOUS TRANSACTIONS REPORTING FORM

Name of the Reporting Officer:

Location:

CUSTOMER BEING REPORTED: (FILL IN AS MUCH DETAILS AS POSSIBLE)

Name:

Account or Reference Number:

Address:

Telephone:

Gender: Nationality:

Date of birth: Passport Number:

DETAILS OF TRANSACTIONS AND REASON WHY SUSPICION HAS AROUSED.

_____

_____

_____

_____


RIA

KYC FORM FOR PERSONAL CUSTOMERS

I, _____ (full name) Passport number _____, place of birth _____ date of birth _____ declare through this document my monthly earnings and the reason I am making money transfers to _____ (country).

The money that I am sending through Ria Exchange Limited comes from _____ (specify).

I have been working as _____ (profession) and receiving a monthly pay after deduction of _____ (HKD) at _____ (name of employer) located at _____ (address of employer). The main purpose of my transfer is _____. My relationship with the beneficiary is _____.

I confirm that the above information is true.

Date:

Signature: