RizonPay LIMITED

ANTI-MONEY LAUNDERING

&

COMBATING TERRORISM FINANCING POLICY

Version 1.1

RizonPay Limited
Level 12, Infinitus Plaza, 199 Des Voeux Road Central, Sheung Wan, Hong Kong

Document Version Control – RizonPay Limited AML/CTF Policy

Revision Date	Document Owner	Version Number	Notes
01.08.2023	Company's Director Mr. Jason Wong	v.1.1	Incorporated effective Regulatory Amendments, made Business Risk Assessment

Contents

1.1 INTRODUCTION

Company Registered Name	RizonPay Limited
Company Trading Name	RizonPay Limited
Registered Business Address	Level 12, Infinitus Plaza, 199 Des Voeux Road Central, Sheung Wan, Hong Kong
MSO Business Premises	Level 12, Infinitus Plaza, 199 Des Voeux Road Central, Sheung Wan, Hong Kong
Registration/Authorization Details	Incorporation No. 3262228
Company Directors	Mr. Jason Wong
Ownership	Mr. Jason Wong 100% ownership
Money Laundering Reporting Officer	Name: Mr. Jason Wong Email: b.parnev@rizonpay.com Contact No +852 9288 9296
Contact Details	Main Office Telephone: +852 9288 9296 Main Office Fax: NA Email ID: j.wong@rizonpay.com General email: b.parnev@rizonpay.com / j.wong@rizonpay.com

RizonPay Limited will hereinafter be referred to as the "Company".

Purpose of this RizonPay Limited AML/CTF Compliance Manual (hereinafter referred to as the **"Manual"**) is to set forth RizonPay Limited procedures to Combat Money Laundering and Terrorist Financing (hereinafter collectively referred as AML/CTF) in accordance with Applicable Regulations. RizonPay Limited offers Remittance & Foreign Exchange Services, to the public through the network of agents, Authorized Partners/Money Transfer Operators, through company-owned Branches and Via Web based Services.

If you are an Agent/Partner of the Company, you have executed an agreement with the Company governing the provision of money transfer services (**Money Service Business or MSB**) and setting forth each party's obligations. As

part of your obligation to the Company under your agreement, you are required to take note of and at all times abide by the provisions of the Manual.

Failure to do so:

- Is considered by the Company to amount to a breach of your agreement, and may result in the Company terminating its agreement with you; and
- In certain cases may amount to breach of applicable legislations, which may result in civil and/or criminal penalties against you.

If you are an employee of the Company, you are required to take note of and at all times abide by the provisions of the Manual. Failure to do so:

- Is considered by the Company to amount to a breach of your duty as an employee, and may result in the Company terminating your employment with the company; whether for just cause (serious misconduct) or for termination of contract; and
- In certain cases may amount to breach of applicable laws, which may result in civil and/or criminal penalties against you.

This Manual is kept under periodical review by the Company, and you may from time to time be notified of revisions to its terms.

Please ensure that all of your staff involved in Money Service Business are familiar with the terms of this Manual and acknowledge this by executing and returning an executed acknowledgement in the form in Appendix VI.

Money Service Business are subject to strict laws and regulations designed to prevent Money Laundering/ Terrorist Financing and to bring those engaged in these illegal activities to justice. Failure to follow these laws and regulations can result in severe civil and/or criminal penalties including fines and imprisonment. The Company has established strict standards of compliance with all Applicable laws and regulations and is committed for the eradication of Money Laundering & Terrorist Financing which are summarised in this Manual. The purpose of the Manual is to explain in simple terms to Agents, Affiliated Partners and their staff and to the Company's Senior Management and Employees how to follow the applicable laws and regulations. If you are an Agent/Affiliated Partner, you are instructed to ensure that each of your staff reads this Manual carefully and completely, and to direct any questions they may have from time to time in the first instance to our Compliance Department.

2.1 SENIOR MANAGEMENT DECLARATION

Date: 1st of August 2023

I, the undersigned, being the Director of RizonPay Limited hereby endorse the policies which have been set down in this Compliance Policy Manual.

The manual covers the following areas:

- Money Laundering & Terrorist Financing Risk to our Business
- Measures we took to mitigate identified Risks
- Customer Due Diligence
- Training and Record keeping
- Suspicious Activity Reporting

These policies may be subject to amendment or addition as required for legislative and business operational reasons.

I confirm that it is the responsibility of the Money Laundering Reporting Officer (MLRO) to monitor Compliance with all of the policy issues mentioned above.

As and when required, the MLRO will make a report to senior management about any operational or strategic issues for the company which arises as a result of the policies set down in this manual.

We also confirm that it is our company policy that all members of staff (and agents, if applicable) must read and confirm in writing their understanding of the policies set down here – and their personal responsibilities arising for them.

In the event that staff members fail to comply as required with the policies in this manual, this will be regarded as a material breach in contractual obligations and may lead to disciplinary proceedings.

Signed by:

Mr. Jason Wong

3.1 MONEY LAUNDERING

The Money Laundering Regulations require a fundamental understanding of the processes that can be involved in money laundering, and require that you respond appropriately to any knowledge or suspicions that these processes may be taking place. This section of the policy explains what money laundering is, the offences and the penalties.

The term “money laundering” (ML) is defined in section 1 of Part 1 of Schedule 1 to the AMLO and means an act intended to have the effect of making any property:

(a) that is the proceeds obtained from the commission of an indictable offence under the laws of Hong Kong, or of any conduct which if it had occurred in Hong Kong would constitute an indictable offence under the laws of Hong Kong; or

(b) that in whole or in part, directly or indirectly, represents such proceeds,

not to appear to be or so represent such proceeds and given the appearance of being legitimate by being exchanged for ‘clean’ money. Participating in the handling of such funds is illegal, and it can also be illegal to become involved in them with knowledge or suspicion.

There are three common stages in the laundering of money, and they frequently involve numerous transactions. An MSO should be alert to any such sign for potential criminal activities. These stages are:

Placement: the physical disposal of cash proceeds derived from illegal activities which means after a crime has been committed, funds are paid into a bank account or used to buy an asset.

Layering: separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail and provide anonymity or in other words to try and hide the source of the proceeds of crime, criminals carry out transactions, which can be complex and numerous.

Integration: creating the impression of apparent legitimacy to criminally derived wealth. In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities, meaning once the origin of the funds has been hidden through sufficient 'layering', the funds are imported back into the financial system.

Being involved in any of these three stages is potentially a criminal activity.

4.1 TERRORIST FINANCING

The term "terrorist financing" (TF) is defined in section 1 of Part 1 of Schedule 1 to the AMLO and 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);

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.

Terrorists or terrorist organizations require financial support in order to achieve their aims. There is often a need for them to obscure or disguise links between them and their funding sources. It follows then that terrorist groups must similarly find ways to launder funds, regardless of whether the funds are from a legitimate or illegitimate source, in order to be able to use them without attracting the attention of the authorities.

5.1 RizonPay Limited AML/CTF POLICIES AND PROGRAM

RizonPay Limited takes all reasonable measures to ensure that proper safeguards exist to mitigate the risks of Money Laundering (ML) and Terrorist Financing (TF) and to prevent a contravention of any requirement under the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance, Chapter 615, Laws of Hong Kong (AMLO) and the related Guideline on Anti-Money Laundering and Counter-Terrorist Financing (AML Guideline).

RizonPay Limited establishes and implements adequate and appropriate Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) policies, procedures and controls taking into account factors including types of customers, products and services offered, delivery channels and geographical locations involved.

RizonPay Limited and its directors and senior management are committed to operating the business in a transparent and open manner that is consistent with regulatory obligations. The directors, senior management, compliance officer and the nominated officer (MLRO) will always ensure that all suspicious activity is reported to the relevant authorities. It is our policy that commercial considerations shall never take precedence over our AML and CFT commitments.

As part of this commitment, RizonPay Limited will adopt strict procedures to comply with all applicable AML and CFT rules and regulations. Specific emphasis will be made on the main pieces of legislation in Hong Kong that are concerned with Money Laundering ("ML"), Terrorism Financing ("TF") and financial sanctions: the Anti-Money Laundering and

Counter-Terrorist Financing Ordinance, Cap.615 ("AMLO"), the Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405 (DTROP), the Organized and Serious Crimes Ordinance, Cap. 455 (OSCO), the United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575 (UNATMO), the United Nations Sanctions Ordinance, Cap. 537 (UNSO) and the Weapons of Mass Destruction (Control of Provision of Services) Ordinance, Cap. 526 (WMD (CPS)O) and FATF Recommendations.

To comply with the listed regulations is extremely important for the Company as the AMLO makes it a criminal offence if an MSO (1) knowingly; or (2) with the intent to defraud the Commissioner of Customs and Excise (CCE), contravenes a specified provision of the AMLO. The "specified provisions" are listed in section 5(11) of the AMLO. If the MSO knowingly contravenes a specified provision, it is liable to a maximum term of imprisonment of 2 years and a fine of $1 million upon conviction. If the MSO contravenes a specified provision with the intent to defraud the CCE, it is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.

Cap. 486 Personal Data (Privacy) Ordinance 2018 (PDO) governs the processing relating to individuals, including obtaining, holding, use of disclosure of information. The Company is committed to ensuring that all data collected is used, retained, and processed in a fair, transparent and secure way. The Data Protection Officer for the Company in Hong Kong is Fermin, Deliuz M. Jr.

Financial Sanctions are prohibitions and restrictions put in place against target countries, legal persons and individuals in order to meet political ends. Most financial sanctions are made through the United Nations Security Committee which has direct reflection in Hong Kong legislation through the United Nations Sanctions Ordinance, Cap. 537 (UNSO) and via periodic circulars about addition or removal of sanctioned entities/individuals. This Ordinance provides for the imposition of sanctions against places outside the People's Republic of China arising from Chapter 7 of the Charter of the United Nations. Regulations are made to implement sanctions, at the instructions made by the Ministry of Foreign Affairs of the People's Republic of China. A number of regulations made under the UNSO are directly relevant to the AML/CFT objectives. These are the United Nations Sanctions (Afghanistan) Regulation 2012, Cap. 537AX, the United Nations Sanctions (Joint Comprehensive Plan of Actions—Iran) Regulation, Cap. 537BV, and the United Nations Sanctions (Democratic People's Republic of Korea) Regulation, Cap. 537AE. The application of financial sanctions constitutes an obligation for both the public and private sector in Hong Kong

Company's operational system is designed to hold (block) a transaction when a customer and beneficiary name match with the one of listed on the Sanctions List for analysis by the compliance department. Any transaction that is processed by the Company that is a potential match against relevant sanctions lists must be escalated to the nominated officer. The system uses fuzzy matching techniques to identify potential matches, and when a potential match occurs the compliance department check whether it is a false positive by analyzing the following fields:

i. For individuals (senders and beneficiaries): nationality, full legal name, address, plus at least one of the following: Date of birth or Hong Kong Identity Card/Passport/Social Security Number/National ID/Tax ID;
II. For Entities (relationship or Transaction): country of domicile, full legal name; doing business as name, physical address.

The compliance officer will monitor **local or regional changes in sanctions regulations** and communicate any such changes to the senior management and key compliance employees.

Fraud has increased substantially in the last years, and therefore managing fraud risk is a key objective for the Company, so as to protect our employees, agents and our system from becoming an instrument for fraudulent activities. Together with this manual, employees and agents received a separate guide on fraud awareness, and this matter is included in the training giving to employees and agents. Any suspicions of fraudulent activity must be reported to the nominated officer. Fraud that is not related with Money Laundering or Financing Terrorist will be reported to the Commercial Crime Bureau of the Hong Kong Police ("CCB").

Fermin, Deliuz M. Jr. is currently Company's nominated officer. Where employees have any questions, uncertainties or concerns in relation to this document, they should contact Fermin, Deliuz M. Jr. or, in his absence, his deputy (if available). Fermin, Deliuz M. Jr. is responsible to receive reports of suspicious activities from employees and agents and decide whether to report them to the Joint Financial Intelligence Unit (JFIU).

Fermin, Deliuz M. Jr. is Company's compliance officer. Deliuz M. Fermin, Jr. is the Executive Director and Compliance Officer for the Company and has an obligation to attend and report regularly on all compliance-related matters to the Hong Kong Customs and Exercise Department. Mr. Fermin is a member of ACAMS, he is currently doing the Certification in AML/CTF Foundations from ACAMS.

We consider that all compliance-related employees, senior managers, and front-line employees dealing directly with customers are relevant employees. We maintain a screening policy for all employees on commencement of employment, and will screen relevant employees to assess their skills, knowledge and expertise, as well as their conduct and integrity.

Legislative References:

International standards of anti-money laundering and counter-financing of terrorism are set by the Financial Action Task Force (FATF). As a member of the FATF, Hong Kong implements recommendations for any companies registered and to combat money laundering and terrorist financing.

The relevant legislation dealing with money laundering and terrorist financing includes the latest versions of:

I. Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) - came into effect on 1 April 2012, imposes on financial institutions requirements regarding customer due diligence and record-keeping;
II. Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP);
III. Organized and Serious Crimes Ordinance (OSCO);
IV. United Nations (Anti-Terrorism Measures) Ordinance (UNATMO);
V. United Nations Sanctions Ordinance (UNSO);
VI. Weapons of Mass Destruction (Control of Provision of Services) Ordinance (WMD(CPS)O);

There are also various associated regulations which have been issued under these main pieces of legislation. Further details are available from Legal Team.

6.1 SENIOR MANAGEMENT – OUR OBLIGATION

Under AML/CTF regulations Senior Management is required to provide adequate resources to establish appropriate risk-sensitive policies and procedures in order to prevent activities related to money laundering and terrorist financing.

The senior management of RizonPay Limited is actively involved in the implementation and oversight of AML program and controls. An Independent Compliance Function/unit is formed by the Board of Directors of RizonPay Limited Ltd and delegated with the responsibilities to:

- To ensure that the firm's control processes and procedures are appropriately designed and implemented, and are effectively operated to reduce the risk of the firm being used in connection with money laundering or terrorist financing

- 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

- To apply proportionate, risk-based policies across different aspects of its business

- Maintain adequate Record keeping of Customer due diligence, supporting evidence. Transactional records for at least 7 years or as per application regulatory limits at the end of business

- Have in place MLRO to take internal suspicious reports and where appropriate submit these reports to external financial Intelligence unit.

- To ensure that Firm have a system in place to highlight those customers who, on criteria established by the firm, may indicate that they present a higher risk of this

- Must be fully engaged in the decision making processes, and must take ownership of the risk-based approach, since they will be held accountable if the approach is inadequate

- Must be aware of the level of money laundering risk the firm is exposed to and take a view whether the firm is equipped to mitigate that risk effectively

7.1 NOMINATED COMPLIANCE & MONEY LAUNDERING REPORTING OFFICER(MLRO)

The MLRO is the focal point within the company for the oversight of all activity related to anti-financial crime issues.

Responsibilities of Compliance Officer/MLRO includes:

- Reviewing all new laws and deciding how they impact on the operational process of the company
- Preparing a written procedures manual and making it available to all staff and other stakeholders
- Making sure appropriate due diligence is carried out on customers and business partners
- Receiving internal Suspicious Activity Reports (SARs) from staff
- Deciding which internal SAR's need to be reported on to local FIU
- Recording all decisions relating to SARs appropriately
- Ensuring staff receive anti-financial crime training when they join and that the receive regular Refresher training
- Monitoring business relationships and recording reviews and decisions taken about continuing or Terminating trading activity with particular customers
- Making sure that all business records are kept for at least five years from the date of the last customer transaction
- Prepare and submit periodic transactional report to the CED
- Be a focal contact point for the CED enquiries

Business Monitoring

It is the responsibility of the MLRO to monitor all the activity of the business with particular reference to the potential financial crime risk. The MLRO will keep a close eye on the following criteria and provide a report to senior management when required.

The report is likely to include commentary on the following issues (in the case that there is no information to report, there should be a 'nil return' should be indicated)

- Confirmation that adequate CDD information is being collected and that on-going monitoring is taking place
- Summary data relating to complex or unusual transactions
- Number of internal consents/SARs received from staff members
- Number of SARs made to JFIU.
- Information on status of staff training within the company
- Confirmation that all business records have been stored
- Changes in the law/operating environment which are or will impact the business
- Changes in risk matrix effecting the business
- Contacts with the regulator

The MLRO should indicate where there is action of the regulator, law enforcement or other agency which raises any potential issues for the business.

The Company's MLRO contact details are given below for your information:

Name	Mr. Fermin, Deliuz M. Jr.
E-mail	mlro@rizonpay.com / b.parnev@rizonpay.com
Tel	+ 852 9288 9296

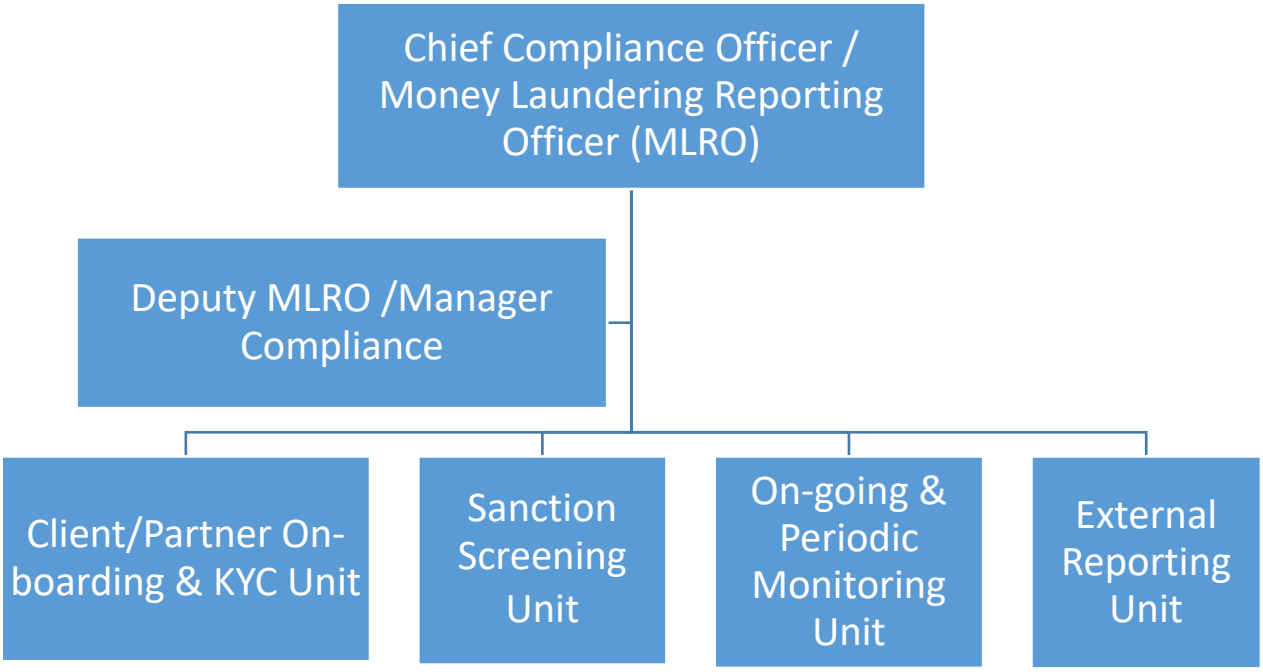
The RizonPay Limited DMLRO (UK/EU Operations) contact details are given below for your information:

Name	Mr. Ahtisham Zaheer
E-mail	a.zaheer@rizonpay.com
Tel	+34-632529760

Every Agent / Partner must appoint a compliance officer who will act directly as contact person for the Supervisory Authorities and the Financial Intelligence Unit (FIU). The officer may be the agent himself (if a sole trader) or a staff with sufficient authority who will be responsible for the following functions:

- Compliance with the relevant provisions of the Anti-Money Laundering Regulations, the directives issued by Regulatory Authorities or other supervising entities and Company's internal policies and procedures.
- Identify and make Suspicious Activity Reports (SAR) to the RizonPay Limited MLRO. Where possible, this could be made directly to the FIU and notifying the Company.
- Coordinate with the Regulatory Authorities and provide any information requested including relevant documentation and audits
- Educate the frontline staff regarding Anti-Money Laundering & Combating Terrorist Financing and 'Know Your Customer' procedures.
- Ensure effective arrangement is in place to comply with record keeping requirement.
- Liaise with the Company appointed MLRO for support and guidance regarding the aforementioned functions.

8.1 COMPLIANCE STRUCTURE


Chief Compliance Officer / Money Laundering Reporting Officer (MLRO)
Deputy MLRO /Manager Compliance
Client/Partner On-boarding & KYC Unit
Sanction Screening Unit
On-going & Periodic Monitoring Unit
External Reporting Unit

9.1 RIZONPAY LIMITED RISK BASED APPROACH – ASSESSMENT & MITIGATION

The risk-based approach is where you assess the risks that your business may be used for money laundering or terrorist financing and put in place appropriate measures to manage and try to mitigate those risks.

By adopting a risk-based approach, organizations are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the most attention in order to prevent operations related to money laundering or terrorist financing.

- Determining 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.
- Applying Enhanced Due Diligence measures, where client is in financial sanction list or is PEP. And if dealing with corporate customers.
- Identifying where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk sensitive basis to verify his identity (including in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure).
- Scrutinizing 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
- Maintaining up to date 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.
- Performing sanction screening and where found seizing and reporting such transactions.
- Creating Policies and procedures that relate to customer due diligence, ongoing Monitoring and internal reporting to MLRO/CO, if any suspicions are identified.
- Establishing internal procedures for investigating any complaint that may be made against us in relation to any transaction.
- Performing initial and on-going Due diligence and enhanced due diligence- (where required) on Agents, intended to use payment service system of the Company. The Company's agents are only allowed to start work once authorization is received from regulator.

RizonPay Limited recognises the various risks its business is exposed to and has made appropriate assessment and evaluation of the risks within their operating context at organizational level.

Please Refer to Appendix I for the detailed Risk Assessment and Mitigation

10.1 CUSTOMER DUE DILIGENCE

CDD comprises the gathering of all relevant information about a client's affairs. This is the information that enables an organization to assess the extent to which that client exposes it to a range of risks, including the risk of involvement in money laundering. CDD is often referred to as Know Your Customer (KYC) information, although the terminology has developed, as KYC was often associated with the client identification process, commonly thought of as the 'passport and utility bills' approach to CDD. CDD is a far more holistic concept than basic client identification measures, and encompasses a wider range of information and processes, which need to be gathered, verified and assessed throughout a client relationship.

This section sets out the standard identification requirements for customers who are private individuals. This is likely to be sufficient for most scenarios. If, however, the customer or transaction is assessed as presenting a higher money laundering or terrorist financing risk (in-line with our identified risk matrix), then we will require further identity information and will increase the level of verification accordingly.

The Company applies an Risk Based Approach (RBA) when conducting CDD measures and the extent of CDD measures should be commensurate with the ML/TF risks associated with a business relationship. Where the ML/TF risks are high, the Company conducts enhanced due diligence (EDD) measures. In low-risk situations, the Company applies simplified due diligence (SDD) measures.

Where the result of a standard verification check gives rise to concern or uncertainty over identity, the number of matches that will be required for the Company to be reasonably satisfied as to the individual's identity will increase. Employees must notify any concerns to the Compliance officer.

Employees may also need to follow this guidance when identifying and verifying the identity of ultimate beneficial owners and any other relevant individuals associated with the relationship or transaction. Employees must notify the Compliance Officer of any issues relating to beneficial owners.

All documentary evidence must be dated within the past 3 months and the date of expiry must be noted on the system. Employees will be prompted by the system when any ID is due to expire and will need to request a new ID document from the customer before the transaction may continue or the account may operate.

In terms of beneficial ownership, we will ask every customer whether they are acting in their own capacity or on behalf of another person. If they are acting for another person, we will require details on the ultimate beneficial owner.

According to the requirements imposed by the AMLO the following CDD measures applicable to the Company:

a) Identify the customer and verify the customer's identity using documents, data or information provided by a reliable and independent source;
b) Where there is a beneficial owner in relation to the customer, identify and take reasonable measures to verify the beneficial owner's identity so that the MSO is satisfied that it knows who the beneficial owner is, including in the case of a legal person or trust, measures to enable the MSO to understand the ownership and control structure of the legal person or trust;
c) obtain information on the purpose and intended nature of the business relationship (if any) established with the Company unless the purpose and intended nature are obvious
d) if a person purports to act on behalf of the customer:

I. identify the person and take reasonable measures to verify the person's identity using documents, data or information provided by a reliable and independent source; and
II. verify the person's authority to act on behalf of the customer

10.2 DUE DILIGENCE MEASURES – INDIVIDUALS

RizonPay Limited and/or you/Agent shall identify the customer and verify the customer's identity on the basis of documents, data or information obtained from a reliable and independent source.

RizonPay Limited and/or you/Agent shall bring a customer out of anonymity and give him/her a name, an identity. Identification shall be done by completing in the Company's system, Company's customer form (hereinafter referred to as the "Identification Customer Form") into the IT System.

The Company and/or you shall verify on the other hand the customer's identity to ensure that this identity in fact relates to the person one is dealing with, that this person exists in reality and that the documents, data or information are both trustworthy and conclusive. They may be made available by the customer, although the obligation that they be independent means they cannot be produced by the customer himself. Generally, the identification of natural persons and the verification of their identity are done in one single step on the basis of official documents.

For a customer that is a natural person, an MSO should identify the customer by obtaining at least the following identification information:

a) full name;
b) date of birth;
c) nationality; and
d) unique identification number (e.g. identity card number or passport number) and document type

As a part of the identification and verification following documentation (in original) can be used either alone or jointly with other documentation (which must be scanned in its totality into the Company's system)

EXAMPLES OF RELIABLE AND INDEPENDENT SOURCES OF CUSTOMER IDENTIFICATION	
Identity of an individual physically present in Hong Kong	The identity of an individual physically present in Hong Kong should be verified by reference to their Hong Kong identify card or travel document. RizonPay Limited always identify and/or verify a Hong Kong resident's identity by reference to their Hong Kong identity card or document of identity. The identity of a non-resident should be verified by reference to their valid travel document.

Identity of non-resident individuals	For non-resident individuals who are not physically present in Hong Kong, MSOs may identify and/or verify their identity by reference to the following documents: a) a valid international passport or other travel document; or b) a current national (i.e. Government or State- issued) identity card bearing the photograph of the individual; or c) current valid national (i.e. Government or State- issued) driving license incorporating photographic evidence of the identity of the applicant, issued by a competent national or state authority.
Travel Document	Travel document means a valid 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 following documents constitute travel documents for the purpose of identity verification: a) Permanent Resident Identity Card of Macau Special Administrative Region; b) Mainland Travel Permit for Taiwan Residents; c) Seaman's Identity Document (issued under and in accordance with the International Labor Organization Convention/Seafarers Identity Document Convention 1958); d) Taiwan Travel Permit for Mainland Residents; e) Permit for residents of Macau issued by Director of Immigration; f) Exit-entry Permit for Travelling to and from Hong Kong and Macau for Official Purposes; and g) Exit-entry Permit for Travelling to and from Hong Kong and Macau.

SUITABLE CERTIFICATION OF SUCH DOCUMENTS

Use of an independent and appropriate person to certify verification of identification documents guards against the risk that documentation provided does not correspond to the customer whose identity is being verified. However, for certification to be effective, the certifier will need to have seen the original documentation.

Non-exhaustive examples of appropriate persons to certify verification of identification documents	a. member of the judiciary in an equivalent jurisdiction; b. an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity; c. a Justice of the Peace; and d. other professional person such as certified public accountant, lawyer, notary public and chartered secretary; etc.
Certification Form	Duly certified documents shall contain the following mandatory information: ➢ the certifier's signature; ➢ the date of certification; ➢ the certifier's name to be printed/written clearly in capitals underneath; ➢ the certifier's position or capacity has to be clearly stated. The certifier should state that it is a true copy of the original (or words to similar effect).

SOURCES OF EVIDENCE	
Acceptable photographic ID: ➢ Valid passport; ➢ Valid photo card driving license; ➢ Hong Kong Identity Card or other national identity card; ➢ other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).	Evidence of address or date of birth: ➢ Instrument of a court appointment (such as a grant of probate or bankruptcy); ➢ Bank statements, credit/debit card statements issued by a regulated financial sector firm in Hong Kong or equivalent jurisdiction (but not statements printed off the internet) from within the last 3 months; ➢ A file note of a visit by a member of the Company to the address (i.e. a home visit); ➢ An electoral register search showing residence in the current electoral year or most recent electoral year; ➢ A utility bill or statement of account (i.e. not correspondence) from the last 3 months - includes gas, water, electricity, telephone but not mobile phone; ➢ Valid photo card driving license (full or provisional);

	➢ Evidence of entitlement to a state or a local authority funded benefit (including housing benefit and council tax benefit), tax credit, pension, educational or other grant; ➢ Documents issued by Hong Kong Revenue Departments such as coding notices and statements of an account (n.b. employer-issued documents are not acceptable);

When accepting a customer's evidence of identity, it is important that we make sufficient checks on the evidence to verify the customer's identity and that we keep a record of the checks made, making a scan and uploading it to the customer's file.

CHECKS TO BE UNDERTAKEN	
Evidence of identity: Checks on photographic ID include: ➢ Visual likeness against the customer; ➢ Does the date of birth on the evidence match the apparent age of the customer? ➢ Is the ID valid? ➢ Is the spelling of names the same as other documents customer?	Evidence of address or date of birth: Checks on secondary evidence include: ➢ Do the addresses match the address given on the photographic ID? ➢ Does the name of the customer match with the name on the photographic ID? ➢ Does the DOB match with the one informed by the customer?

NON FACE-TO-FACE CUSTOMERS

Non face-to-face customers present an increased risk of money laundering in addition to other risks such as fraud. We must take account of this in framing our internal policies and procedures. We will apply enhanced due diligence measures on a risk-sensitive basis whenever we don't physically meet our customers, as required by the AMLO.

These additional checks may include:

I. Requiring additional documents, data or information to verify the customer's identity;
II. Applying supplementary measures to verify the documents supplied;
III. Requiring the first transaction to be carried out through an account in the customer's name with a Hong Kong or other regulated bank from a comparable jurisdiction;

IV. Telephone contact with the customer at a home or business number which has already been verified, using it to verify additional aspects of personal identity information provided during the application process;
V. Communicating with the customer at an address which has already been verified (e.g. by letter).
VI. Photocopied identity documents can be accepted as evidence of ID provided that each copy document has an original certification by an appropriate person to confirm the person's identity. An appropriate person is an independent professional person who is not a friend or relative of the applicant, for example: family doctor, accountant, civil servant, teacher, solicitor, notary public, Post Office branch employee, or employer.
VII. As well as providing a written certification on the copy document to confirm the applicant's ID, the certifying individual should also provide their business contact details (address, occupation and telephone number) and a statement that the document is "Certified to be a true copy of the original seen by me", signed and dated.

Electronic verification:

As a secondary proof of identification, we may also screen customers against electronic verification services provided by third party providers.

Electronic verification should meet a standard level of confirmation before it can be relied upon. In circumstances that do not give rise to suspicion or significant risk of impersonation fraud, the standard level of confirmation is:

- One match on an individual's full name and current address; and
- A second match on the full name and either his current address or his date of birth;

Where the customer is not physically present for identification purposes, we must obtain further evidence of identity. This means that we will either ask for further forms of evidence or we will perform further checks on the evidence supplied.

10.3 DUE DILIGENCE MEASURES – CORPORATE CLIENTS

Limited Companies and Sole Traders:

For a customer that is a legal person, the Company identifies the customer by obtaining at least the following identification information:

- full name;
- date of incorporation, establishment or registration;
- place of incorporation, establishment or registration (including address of registered office);
- unique identification number (e.g. incorporation number or business registration number) and document type; and
- principal place of business (if different from the address of registered office).

In verifying the identity of a customer that is a legal person, we normally verify its name, legal form, current existence (at the time of verification) and powers that regulate and bind the legal person by reference to documents, data or information provided by a reliable and independent source, examples of which include:

(a) certificate of incorporation;
(b) record in an independent company registry;
(c) certificate of incumbency;
(d) certificate of good standing;
(e) record of registration;
(f) partnership agreement or deed;
(g) constitutional document; or
(h) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).

We will also verify their identity from:

a) Either a search of the relevant company register;
b) Confirmation of the company's listing on a regulated market (as defined by the FCA); or
c) A copy of the company's certificate of incorporation.
d) Searching on the online platform

This standard evidence is likely to be sufficient to verify the identity of most corporate customers. If, however, any of the circumstances outlined in our risk matrix exist then we require further information to be provided so that we can satisfy ourselves as to the customer's identity. This includes, where appropriate, the nature and purpose of the customer's business activities and the source of funds.

In general, the structure, ownership, purposes and activities of many private companies will be clear and understandable.

We should obtain and verify the standard evidence on corporate customers as well as:

- Names of all directors (or equivalent); and
- Names of beneficial owners/shareholders owning over 25% shares;
- When the person placing the transaction on behalf of the corporate is not one of the Directors, we will request a written authorization from the company giving them authority to act for the company. We will request the identification of the authorized person and verify the information.

Partnership or an Unincorporated Body:

For a customer that is a partnership or an unincorporated body, confirmation of the customer's membership of a relevant professional or trade association is likely to be sufficient to verify the identity of the customer as required by the present Policy provided that:

(a) the customer is a well-known, reputable organization;
(b) the customer has a long history in its industry; and
(c) there is substantial public information about the customer, its partners and controllers.

In the case of associations, clubs, societies, charities, religious bodies, institutes, mutual and friendly societies, co-operative and provident societies, an MSO should satisfy itself as to the legitimate purpose of the organization, e.g. by requesting sight of the constitution.

10.4 DUE DILIGENCE MEASURES– AGENTS

The company when offering any of its services through agent(s) shall adopt the policies within this section.

All agents of the company will be required to complete an application form. The company will adopt the following policy for agents which are offering money transfer services on behalf of our company. We will obtain:

- full name, registered number and registered address
- business address and business activity
- confirmation of the names of all directors and beneficial owners
- letter from the directors confirming which named individuals have authority to act on behalf of the company
- copy of ID and proof of address for all those who are authorized to represent the company
- turnover of the business, its size and number of employees
- length of establishment

The company will confirm the following information for each agent prior to commencing business. This will include:

- Confirmation that all directors/owners/key operational staff are 'fit and proper'
- A check to ensure agent credit worthiness
- Confirmation that a Compliance officer/MLRO has been appointed to supervise the compliance procedures within the agent
- Confirmation that all who offer money transfer business in the agency are identified and receive anti-Money laundering training
- All agency staff must read and sign the company compliance manual and undertake to ensure that procedures set down in the manual are followed in day to day Operations
- Confirmation as to whether or not that agent is not working for any other money transfer company (and, if they are, confirm which company it is) – agents working for multiple money transfer companies are considered high risk, and require a higher level of on-going supervision.

If agents are used, all information on originating agents will be recorded along with baseline information on the volume of transactions expected.

As recommended by the Financial Action Task Force (FATF), the company will undertake a specific risk assessment of all agents both prior to commencing business and on an on-going basis. The risk assessment will be carried out (and recorded) with reference to the following criteria. These are as follows:

- Agents conducting unusually high number of transactions with another agent location, particularly through an agent in a geographic area of concern.
- The transaction volume of the agent, either overall or relative to typical past transaction volume.
- Agents that have been referred by other departments of the MSO
- agents that have been the subject of negative attention from credible media or law Enforcement enquiries.
- Agents that are not in compliance with internal policies and external regulation, such as compliance programmed requirements, monitoring, reporting, or Know Your Customer practices.
- Agents that are unwilling to follow compliance program review recommendations, and therefore subject to probation, suspension or termination.
- Agents who fail to provide required originator information upon request.
- Agents whose data collection is lax, sloppy or inconsistent.
- Agents willing to accept false identification.

- Agents willing to enter identification into records that contain false information, non- existent addresses that would be known to be non-existent to a person in that area, or phone numbers that are used as fillers.
- Agents with a send-to-receive ratio that is not consistent with other agents in the locale or is consistent with participation in a criminal transaction corridor.
- Agents whose seasonal business fluctuation is not consistent with other agents in the locale or is consistent with participation in a criminal transaction corridor.
- Agents whose ratio of questionable or anomalous customers to customers who are not in such groups is out of the norm for comparable locations
- Agents whose ratio of questionable or anomalous transactions to transactions that are not in such sets are out of the norm for comparable locations.

10.5 DUE DILIGENCE MEASURES– CORRESPONDENTS

EU/UK Licensed Money Transfer Operating Correspondents/Partners

Before engaging and/or offering RizonPay Limited (hereinafter refereed to as the "Company") Payout Network services to any EU/UK Licensed Money Transfer Operator, the Company will conduct Complete KYB checks and will ensure that counter party has appropriate AML/CTF Program/Controls in Place. At Minimum following documents will be assessed along with Effectiveness of AML/CTF Program, before entering into services agreement with other EU/UK Authorized Payment institution;

- Copy of Certificate (s) of Registration
- Copy of Remittance/Money Transfer business license - [If the Correspondent operates in multiple geographies, copies of individual licenses issued by the regulator corresponding to the nature of business and jurisdiction shall be attached.]
- Memorandum of Association or Articles of Incorporation
- Copy of the latest AML/CTF policies and Programs duly approved by the Board of Directors -
- Organizational Chart with full name of all Key management personnel, including General directors, CFO, Compliance Officer.
- List of shareholders [only of those shareholders who hold more than 10% of shares] -
- ID Copies of the shareholders [only of those shareholders who hold more than 10% of shares]
- Copy of the list of Authorized Signatories, approved by the Board of Directors
- ID Copy of the Authorized Person who signs the agreement

Compliance Manager/Officer will review and validate the authorization of Payment institution and will run Sanction/PEP Checks on UBOs. Company Details will also be validated against sanction lists, to ensure appropriateness of counter party.

AML/CTF Measures will also be assessed in detail, before entering into Service Level agreement.

Simplified Due Diligence approach will be carried on the transactions, coming from another licensed Money Transfer Operator. Partnered MSO will be solely be responsible for ensuring their respective country AML/CTF obligations and will ensure Customer CDD/EDD as per their own Internally approved AML/CTF Policies.

Payout Correspondents

The company recognizes its obligation to have a full understanding of all partners who are involved in the payment process. The company will keep full information on all pay out partners. This information will be stored in Electronic register. All owners/directors will be verified against appropriate sanctions lists/PEP's lists.

10.6 ON-GOING MONITORING OF BUSINESS RELATIONSHIP

The Company and you/Agent shall conduct on-going monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's and your knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

The Company and you are furthermore required to continuously monitor the customers from the beginning and throughout the entire business relationship. The extent of such measures can be adapted in accordance with the degree of risk of money laundering and terrorist financing associated with the relevant customer. The Company and you shall also, in accordance with the risk assessment and Company's instructions, enquire about the source of the funds of the customer in question.

10.7 MAINTAINING CLIENT'S INFORMATION/DOCUMENTS UP-TO-DATE

At the time of the initial identification of the customer and verification of the identity based on a valid document, the Company and you have checked the customer's identity.

Note that identification (e.g. ID card or passport) is invalidated if it's being used after its expiry date.

The Company and you should rely on the identification and verification measures already performed, unless the Company and you have reason to doubt the veracity of the information obtained in the course of the monitoring of the business relationship.

10.8 SANCTION SCREENING PROCESS

Elements of Terrorist Funding

- The primary objective behind terrorist funding is to intimidate or force a government or population to do or abstain from doing any act. In money laundering the objective is monetary gain.
- The volume of remittances for terrorist funding need not have to be large as compared to money laundering. They will vary according to the strategies and methods adopted by the terrorists.
- Terrorist funds need not be from illegal sources always. In some cases, funds are also sourced from legal income.

What can we do to fight terrorist funding?

Prevention- We have to prevent our products and services from used by terrorists for transferring their money. This can be done by applying appropriate "Know Your Customer" Policies and Procedures.

Pursuit- We have to track down the terrorist transactions by blocking their names. In case you come across any blacklisted names, it has to be immediately reported to the concerned authorities.

Protection- We have to protect our institution, our reputation, customers, our jobs and our communities where we operate. We have to protect by being responsible in our duties. If an agent does a money transfer transaction for a customer and has reasonable cause to suspect that it may be used, in whole or in part for the purpose of terrorism, then it should be immediately reported the concerned Compliance Officer for necessary action.

The fight against money laundering & terrorist financing is an evolving and never-ending process. Money laundering not only harms the public as a whole, but it taints the financial services industry. It clearly is in the best interests of the financial industry to take all feasible action to prevent money laundering. Therefore, we need to work together and co-operate to fight against the challenges posed by this social evil.

All staff, partners and affiliates of the Company are required to maintain the highest level of due diligence when engaging in any aspects of remittance services.

The Company has introduced an IT-based solution to fulfil the screening obligations automatically. All of the Company's relevant Customers & Business Partners' key data is stored in the internal system. The relevant data (such as name, surname, and address) is automatically exported and matched with the sanctions lists on a cloud server solution offered and serviced by an external service provider. These checks are on each transaction/activity.

If during the matching procedure a customer is marked as a potentially Restricted Party, this is defined as a hit. This IT-solution simultaneously generates an alert message including all recorded hits, which is submitted to the respective Compliance Manager/Officer.

All potential hits are investigated properly by the Compliance Manager/Officer. The investigation may result in different outcomes (see below).

Due to various characteristics (such as similarities in names, ages, etc.), customers might be marked as potentially Restricted Parties and hence enter the hit management process even if they are not the actual party registered in the sanctions lists ("False Positives").

The Compliance Manager/Officer manages these hits by clarifying the identity of the Customer/Business Partner. This can be done, e.g., by performing background checks, by enquiries to authorities as well as by interviews with departments who conduct business with the potentially Restricted Party (such as procurement or sales).

The hit management process may result in three outcomes:

1. The Customer/Business Partner is in fact not the person or legal entity included in the sanctions lists: The Compliance Manager/Officer defines the Customer/Business Partner as a safe Customer/Business Partner by defining alert as "False Positive" with a reasoned justification.
2. The Customer/Business Partner is in fact the person or legal entity included in the sanctions lists: The Compliance Manager/Officer takes all measures to immediately terminate the relationship with this Customer/Business Partner and report to FIU in writing
3. It remains unclear, if the Customer/Business Partner is in fact the person or legal entity included in the sanctions lists:

   The Compliance Manager escalates this issue to the Chief Compliance Officer/MLRO, which subsequently takes a decision on whether to terminate or to continue the relationship with the Customer/Business Partner. If the Chief Compliance Officer decides to continue the relationship with

the Business Partner, a full and comprehensive documentation shall be provided by the Compliance Officer to the Shareholders.

11.1 ENHANCED DUE DILIGENCE

Enhanced due diligence' is mandatory for the situations that pose high risk to the company, this means taking additional measures to identify and verify the customer's identity and source of funds and doing additional ongoing monitoring. Enhanced Due diligence is required when:

- Customer is not physically present for identification face-to-face.
- Customer is a "politically exposed person", or an immediate family member or a close associate of a politically exposed person.
- The nature of a particular situation presents a higher risk of money laundering or terrorist financing.
- Customer doing large amount transaction and or
- If there is any suspicion or unusually activity is identified

11.2 UNDERSTANDING/OBTAINING CLIENT SOURCE/PROOF OF FUNDS

RizonPay Limited (hereinafter referred to as the "Company") obliging to the Regulations monitors the ongoing relationship with its clients. The below table shows the process and ID requirements we will ask from our clients.

Company's Enhanced Due Diligence (EDD) policy is designed to obtain as much information as possible in order to ensure the validity of the transaction and that the Company complies with AML&CTF regulations.

The checking is meant to be thorough in its nature to ensure that we record enough information that will help us form a true picture of the client. As follow

- Disclaimer/questionnaire for the origin of funds not being derived from the proceeds of crime
- Source of funds verification in the form of a recent Bank statement showing the movement of funds. - As Per the Company's ID Matrix

If funds have been generated/received via a 3rd party IE: solicitor for a house sale. Then additional correspondence or documentation is to be collected and put on file.

Sr. No	Amount	Duration	Requirement
1	Less than HK$8,000 paid in cash	Single or Calendar month Aggregate Thresholds	No scanned identification documents required for transactions less than HK$8,000, but, cashier must identify customers, complete all mandatory fields in the system and verify the information with original document provided by the customer. **Documents required**

			None. In Payments in cash the original Identification document must be seen by the cashier and details of the identification typed in the customer profile in Internal system.
2	Less than HK$8,000 payment bank transfer or debit card	Single or Calendar month Aggregate Thresholds	No scanned identification documents required for transactions less than HK$8,000 **Documents required** None
3	More than HK$8,000 any payment method	Single or Calendar month Aggregate Thresholds	Copy of ID scanned into Internal System **Documents required** Customer Identification required and identification details typed in the customer profile in Internal system.
4	HK$120,000 or more	Aggregate in a year	Proof of occupation will be retained
5	HK$120,000 or more	Single Transaction	Proof of funds + proof of occupation will be retained

Amounts Aggregate in a Calendar Month (Natural Persons)

Payout Country	Risk	SOF Threshold for Single or Aggregate Paid by Cash Currency EUR equivalent	SOF Threshold for Single or Aggregate Paid by Bank Currency EUR equivalent
Algeria	3	3,000.00	4,500.00
Argentina	4	2,000.00	3,500.00
Benin	5	1,500.00	3,000.00
Brazil	1	4,000.00	6,000.00
Burkina Faso	3	3,000.00	4,500.00
Colombia	2	3,000.00	5,000.00
Cote d'Ivoire	4	2,000.00	3,500.00
DRC	5	1,500.00	3,000.00
Egypt	1	4,000.00	6,000.00
EU & Equivalent	1	4,000.00	6,000.00
Ghana	2	3,000.00	5,000.00
Guinea	5	1,500.00	3,000.00
Hong Kong	2	3,000.00	5,000.00
India	2	3,000.00	5,000.00
Jamaica	3	3,000.00	4,500.00
Kenya	5	1,500.00	3,000.00
Lebanon	2	3,000.00	5,000.00
Madagascar	3	3,000.00	4,500.00
Mali	5	1,500.00	3,000.00
Morocco	2	3,000.00	5,000.00
Mozambique	5	1,500.00	3,000.00

Nigeria	4	2,000.00	3,500.00
Pakistan	3	3,000.00	4,500.00
Russian Federation	2	3,000.00	5,000.00
Senegal	3	3,000.00	4,500.00
South Africa	1	4,000.00	6,000.00
Sri-Lanka	4	2,000.00	3,500.00
Tanzania	4	2,000.00	3,500.00
Togo	4	2,000.00	3,500.00
Ukraine	2	3,000.00	5,000.00

Proof of Funds

Bank statement - in name of the customer and the amount sent cannot be deposited in the same day into customer account. Bank statement will be accepted just for amounts that meet the income of the customer.

- Saving account
- Loan agreement - note that with loan agreement customers shall demonstrate the amount come into their account.
- Funds from other person: Beneficial owner need to be identified and proof of funds should apply for the beneficial owner instead of the customer.
- Proof of address (domicile): Utility bill (gas, electricity, landline, bank statement), Hong Kong driving license (if it is not use as proof of ID).

IMPORTANT NOTES:

Please note that currently we are not requesting proof of address, however it might be requested if the information provided is mismatch or incomplete.

The thresholds listed above is just a reference and the amounts are set up in our operational system. However, compliance department can stop any transaction and request further documents regardless the amount. Transactions placed with amount right below the limit set up above will be treated as unusual transactions and further action will be taken.

Deposits in cash into our account will be considered "non-face to face" transactions in cash and ID will be required for any amount. The thresholds applied will be the same applied to cash transactions.

Aggregate in a year HK$120,000 - proof of occupation will be required. In some cases, if it's a single transaction more than HK$120,000, proof of funds + proof of occupation will be required.

Compliance form is available in Appendix III.

11.3 LINKED TRANSACTIONS

Linked transactions may be a series of transactions by a legitimate customer, or they may be transactions that appear to be independent, but are in fact split into two or more transactions to avoid detection.

Simply put, a client may attempt to disguise a remittance payment by breaking it into several smaller sums and utilizing his/her friends or family to send the funds usually to a single beneficiary.

In anticipation that a client will avoid requiring proof of funds and have structured his/her transactions in reaching the limit amount, the client may divide the amount among his/her friends and send the money at the same time to a single beneficiary. In this case, our remittance front-end IT system is a valuable asset as it will assist towards detecting linked transactions.

Staff must exercise personal judgment and consider the following:

- Are a number of transactions carried out by the same customer within a short space of time?
- Could a number of customers be carrying out transactions on behalf of the same individual or group of individuals?
- In the case of money transmission, are a number of customers sending payments to the same individual?

In the event that 'linked' transactions are identified, they should be notified to the MLRO who will determine whether or not there are any suspicious circumstances and whether the transaction should be reported to JFIU.

11.4 POLITICAL EXPOSED PERSONS - PEPs

One of the most prominent risks to the financial services sector is the risk posed by public officials, their associates and family members. There have been a number of damaging high-profile money laundering scandals within the private banking sector that have involved PEPs

A domestic PEP is defined as:

a) an individual who is or has been entrusted with a prominent public function in a place within the People's Republic of China and

   I. includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official;
   II. but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph

b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or

c) a close associate of an individual falling within paragraph (a).

A (foreign) PEP is defined in the AMLO as:

a) an individual who is or has been entrusted with a prominent public function in a place outside the People's Republic of China and

   I. includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official;
   II. but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph

b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or
c) a close associate of an individual falling within paragraph (a).

The AMLO defines a close associate as:

a) an individual who has close business relations with a person falling under previous paragraph above, including an individual who is a beneficial owner of a legal person or trust of which the person falling under paragraph above is also a beneficial owner; or

b) an individual who is the beneficial owner of a legal person or trust that is set up for the benefit of a person falling under paragraph above.

EDD in respect of PEPs shall be:

Having appropriate risk-sensitive procedures, known to all Employees and agents, to determine whether the customer or the ultimate beneficial owner is a PEP residing in a foreign country. Such procedures involve assessing the information provided by the customer, publicly available information, or information contained on commercial databases relating to PEPs.

Obtaining prior approval from the Compliance Officer before entering into a business relationship with a PEP or executing an occasional transaction for a PEP.

Taking adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction. Employees should also, on a risk-sensitive basis, verify the source of funds and require documentary evidence; and

Conducting enhanced ongoing monitoring of the business relationship.

When dealing with clients with a more sophisticated financial profile, we should search about the provenance of their wealth such as: where their net worth was originally earned or acquired and the origins of their income;

The usual origins of wealth and income for PEPs might include:

- Business activity including business disposals, to determine whether the magnitude of their business activity is consistent with the wealth and income claimed.

- Employment: inquiries about salary, bonuses, share options to determine whether their employment is capable of generating the accumulated wealth.

- Investments: we will ask about the origin of the funds that purchased the investments in the first place. We will search for the magnitude and nature of the investments, annual income and capital growth, to determine whether the client's holdings are consistent with the wealth and income declared.

- Family money: we will search about the original source of the wealth, who transferred it to the client, when and in what form, and how that person earned or acquired the wealth, to determine whether inheritance provides a satisfactory explanation for the wealth and income claimed.

The requirement to identify close associates of prominent public functionaries as PEPs only applies to the extent that the relationship is publicly known or that the Company has reasons to believe that such a relationship exists. Thus it does not presuppose active research on the Company's part.

PEPs do not normally include public functionaries at regional or local levels of government. However, where their political exposure is comparable to that of similar positions at national level, the Company will assess, on a risk-sensitive basis, whether those persons should be considered PEPs.

The Company, its Employees and, in particular, the Compliance Officer must closely monitor all ongoing business relationships with PEPs.

All transactions will be screened against PEP lists, and any transactions with possible PEP matches will be stopped by our system for further analysis. Confirming PEP status or otherwise may require us to gather more information about the customer. The information that we will request is date of birth (DOB), place of birth and proof of occupation. This information will be used to compare and confirm if the client is a PEP or not.

If we confirm that the customer is a PEP, we will make sure that the correct profession is allocated in our system to meet the customer risk criteria.

12.1 TRANSACTION MONITORING

The Company monitors all transactions generated on its system to ensure compliance with the AML Manual, applicable legal and regulatory requirements by way of a two-level approach:

First Level

The Company adopts a hybrid model for monitoring its transactions. This includes a combination of automated and manual processes. All transactions undergo a stringent compliance process that includes:

- Sanctions & PEP Screening: The Company performs sanctions screening against the sanctions and PEP database maintained in in-house system. Alerts are investigated and closed as per the procedures set in this regard.

- Real Time Transaction Monitoring: Based on various rules, and defined thresholds and velocity controls, transactions undergo automated surveillance. The Company has an in- house developed surveillance system that has embedded the required rules. The compliance department undertakes the initial review and investigation. Transactions are assessed for (among other things) conformity with the Company's policy, data quality, structuring effort and restrictions on high-risk country involvement and, where applicable thresholds are met, the provision of supporting evidence (e.g. of the source of funds). The Company's MLRO conducts further investigation of any transaction that is flagged on the basis of this screening and determines whether any further action is required including, for example an SAR submission.

- Specific Post Facto Analysis: The compliance department of the Company along with assistance of a dedicated back office unit, conducts periodic analysis on agents and their transactions. The reports and the findings are submitted to the MLRO so that appropriate actions are undertaken. The analysis looks for specific patterns, unusual patterns, data quality standards, and similar warning flags.

Second Level

This monitoring is a more detailed risk-based assessment of agents' activities. This is carried out by the compliance department of the Company along with the assistance of a dedicated back office unit. Sample data sets for agents (selected on the basis of risk) are extracted from the Company's system and a shadow CDD exercise is undertaken. In the event of any concerns as to the adequacy of process followed by an agent, the Company's MLRO approaches the agent for clarification. Periodic compliance visits to agents will be carried out in person to discuss any major or recurrent issues that have arisen through the monitoring process, as well as to check record keeping, training and to discuss the overall risk and compliance environment. The frequency of visits to an agent is determined by Agent's risk classification.

13.1 SUSPICIOUS ACTIVITY REPORTING

What is Suspicious Activity:

"Suspicious activity" is a difficult concept to define because it can vary from one transaction to another based upon on all of the circumstances surrounding the transaction, or group of transactions. However in general suspicious Activities/transactions refers to any transaction or group of transactions about which doubts arise with the registered person concerning their link to money laundering and terrorist financing through their unusual size, repetition, nature, conditions and circumstances surrounding them, their unusual pattern that does not involve a clear economic objective or an obvious legal purpose, if the activities of the persons involved in the transaction(s) do not conform with their normal activities. For example, transactions by one customer may be normal because of your knowledge of that customer, while similar transactions by another customer may be suspicious.

In brief, the factors involved in determining whether transactions are suspicious, including the amount, the location of your business, comments made by your customer, the customer's behavior etc. A good rule to follow is that if a transaction is inconsistent with the business or personal circumstances of a customer and there is no reasonable explanation for the inconsistency, then it may be suspicious. Just because a customer appears on the suspect list it does not mean that he/she is involved in illegal activity. It only means that such transaction requires closer scrutiny.

What is Suspicious Activity Reporting:

The Suspicious Activity Report is a tool for identifying and reporting transactions that could be related to money laundering or terrorist financing. You need to refer any transactions you consider suspicious to the Company by:

- Completing a Suspicious Activity Report Manual/Electronic form for any transaction or pattern of transactions – completed or attempted – that is suspicious.

- Faxing the completed Manual form to the Company or to your local Regulator if required by law as soon as the suspicious activity is discovered

13.2 RECEIVING & REPORTING SAR – CORE OBLIGATIONS

The AMLO guidance explains the core obligations of receiving and reporting of suspicious activity

- All staff must raise an internal report where they have knowledge or suspicion, or where there are reasonable grounds for having knowledge or suspicion, that another person is engaged in money laundering, or that terrorist property exists
- The firm's nominated officer (or their appointed alternate) must consider all internal reports
- The firm's nominated officer (or their appointed alternate) must make an external report to the Joint Financial Intelligence Unit (JFIU) as soon as is practicable if he considers that there is knowledge, suspicion, or reasonable grounds for knowledge or suspicion, that another person is engaged in money laundering, or that terrorist property exists
- The firm must seek consent from the JFIU before proceeding with a suspicious Activity/transaction or entering into arrangements
- Firms must freeze funds if a customer is identified as being on the Sanction List of suspected terrorists or sanctioned individuals and entities, and make an external report to JFIU
- It is a criminal offence for anyone, following a disclosure to a nominated officer or to the JFIU, to do or say anything that might either 'tip off' another person that a disclosure has been made or prejudice an investigation
- The firm's nominated officer (or their appointed alternate) must report suspicious approaches, even if no transaction takes place
- Actions required, to be kept under regular review
- Enquiries made in respect of disclosures must be documented
- The reasons why a Suspicious Activity Report (SAR) was, or was not, submitted should be recorded
- Any communications made with or received from the authorities, including the JFIU, in relation to a SAR should be maintained on file
- In cases where advance notice of a transaction or of arrangements is given, the need for prior consent before it is allowed to proceed should be considered

Persons in the regulated sector are required to make a report in respect of information that comes to them within the course of a business in the regulated sector:

- where they know or
- where they suspect or
- where they have reasonable grounds for knowing or suspecting

That a person is engaged in, or attempting, money laundering or terrorist financing. Within this guidance, the above obligations are collectively referred to as "grounds for knowledge or suspicion".

13.3 SUSPICIOUS INDICATORS

The following lists are provided for staff as an aid to whether a particular transaction may be suspicious. The list is not limited to and staff & Agents should consider all the circumstances of a particular transaction before deciding whether to report any issues to the MLRO.

New customers and occasional or "one-off" transactions:

- Checking identity is proving difficult.
- The customer is reluctant to provide details of their identity.

- There is no genuine reason for the customer using the services of an MSO
- A cash transaction is unusually large.
- The cash is in used notes and/or small denominations.
- The customer requests currency in large denomination notes.
- The customer will not disclose the source of cash.
- The explanation for the business and/or the amounts involved is not credible.
- A series of transactions are structured just below the regulatory threshold for due diligence identity checks.
- The customer has made an unusual request for collection or delivery.
- Transactions having no apparent purpose or which make no obvious financial sense, or which seem to involve unnecessary complexity.
- Unnecessary routing of funds through third parties.

For Regular and established customers.

- The transaction is different from the normal business of the customer.
- The size of frequency of the transaction is not consistent with the normal activities of the customer.
- The pattern of transactions has changed since the business relationship was established.
- Money transfers to high-risk jurisdictions without reasonable explanation, which are not consistent with the customer's usual foreign business dealings.
- Sudden increases in the frequency/value of transactions of a particular customer without reasonable explanation.
- Examples where customer identification issues have potential to indicate suspicious activity.
- The customer refuses or appears reluctant to provide information requested.
- There appears to be inconsistencies in the information provided by the customer.
- The customer's area of residence is inconsistent with other profile details such as employment.
- An address appears vague or unusual.
- The supporting documentation does not add validity to the other information provided by the customer.
- The customer is in a hurry to rush a transaction through, with promises to provide the information later.

Examples of activity that might suggest to staff that there could be potential terrorist activity:

- The customer is unable to satisfactorily explain the source of income.
- Frequent address changes.
- Media reports on suspected or arrested terrorists or groups.

13.4 PROCEDURE FOR REPORTING SUSPICIOUS CIRCUMSTANCES

Any member of staff or agent, who is suspicious that a transaction may involve money laundering or who becomes aware in the course of their work that someone else is involved in money laundering, must make a disclosure to the MLRO using the report form, by mean of email or using system.

Upon receipt of the Internal SAR by the MLRO, he will then decide what is to be done as a result of the report, e.g., whether the matter must be reported to the JFIU or not, or further enquiries made and record its decision and the reason for it on the report form on the Database. The member of staff concerned must be informed of the decision and the reasons for it.

If the matter is referred to the JFIU the MLRO or his deputy will be responsible for completing the JFIU report form and discussing with the reporting member of staff how matters with the client/transaction are to be conducted from that stage.

In accordance with the tipping off provisions, the report must not be discussed with the customer.

Suspicious Activity/transaction reports can be made to JFIU in one of the following ways:

- by e-reporting system, STREAMS
- by email to jfiu@police.gov.hk
- by fax to: (852) 2529 4013
- by mail, addressed to Joint Financial Intelligence Unit, GPO Box 6555 Hong Kong
- by telephone (852) 2866 3366 (for urgent reports during office hours)

The JFIU will acknowledge receipt of an SAR made by an MSO under section 25A of both the DTROP and the OSCO, and section 12 of the UNATMO. If there is no need for imminent action, e.g. the issue of a restraint order on an account, consent will usually be given for the MSO to operate the account under the provisions of section 25A(2)(a) of both the DTROP and the OSCO, and section 12(2B)(a) of the UNATMO. If a no-consent letter is issued, the MSO should act according to the contents of the letter and seek legal advice where necessary.

An MSO should ensure SARs filed to the JFIU are of high quality taking into account feedback and guidance provided by the JFIU in its quarterly report and the CCE from time to time. The purpose of the quarterly report, which is relevant to all financial sectors, is to raise AML/CFT awareness. It consists of two parts, (i) analysis of SARs and (ii) matters of interest and feedback. The report is available at a secure area of the JFIU's website at www.jfiu.gov.hk. MSOs can apply for a login name and password by completing the registration form available on the JFIU's website or by contacting the JFIU directly.

Providing an MLRO acts in good faith in deciding not to file an SAR with the JFIU, it is unlikely that there will be any criminal liability for failing to report if the MLRO concludes that there is no suspicion after taking into account all available information. It is however vital for the MLRO to keep proper records of the deliberations and actions taken to demonstrate he has acted in reasonable manner.

However, the statutory defense does not absolve an MSO from the legal, reputational or regulatory risks associated with the account's continued operation. An MSO should also be aware that a "consent" response from the JFIU to a pre-transaction report should not be construed as a "clean bill of health" for the continued operation of the account or an indication that the account does not pose a risk to the MSO.

The report must not be discussed with the customer, in accordance with the tipping off provisions of the AMLO. We must not proceed with a transaction to which we await consent from the JFIU.

There must be no record on the customer file or on the computer system which refers in any way to suspicious circumstances reporting, money laundering, etc. to avoid the risk of tipping off under the AMLO. It is a criminal offence to inform a customer that a SAR has been submitted or to inform them of an investigation into their affairs. All records of SARs will be kept in the central reporting file, which is kept in the nominated officer's office.

We should conduct an appropriate review of a business relationship upon the filing of an SAR to the JFIU, irrespective of any subsequent feedback provided by the JFIU, and apply appropriate risk mitigating measures. Filing a report with the JFIU and continuing to operate the relationship without any further consideration of the risks and the imposition of appropriate controls to mitigate the risks identified is not acceptable. If necessary, the issue should be escalated to the MSO's senior management to determine how to handle the relationship concerned to mitigate any potential legal or reputational risks posed by the relationship in line with Company's business objectives, and its capacity to mitigate the risks identified.

Reporting of a suspicion in respect of a transaction or event does not remove the need to report further suspicious Activities/transactions or events in respect of the same customer. Further suspicious Activities or transactions, whether of the same nature or different to the previous suspicion, must continue to be reported to the MLRO who should make further reports to the JFIU if appropriate.

13.5 TIPPING OFF

Any staff member needs to make a judgment as to whether any delay to the transaction ('Consent request') would have the effect of 'tipping off' the customer.

Tipping Off is another offence under the DTROP, the OSCO and the UNATMO. 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 any investigation which might be conducted following that first-mentioned disclosure. The maximum penalty for the offence upon conviction is imprisonment for 3 years and a fine.

You should never disclose to the customer"

- that a transaction was/is being delayed because consent from JFIU has been requested;
- that details of their transactions or activities will be/have been reported to JFIU;
- that they are being investigated by law enforcement.

14.1 AML/CTF TRAINING OF STAFF/AGENT

Training is given to all staff members and compliance delegate at agent location upon commencement of taking on the money transfer service and on regular occasions afterwards (at least once a year). Training covers the following issues:

- The law relating to financial crime
- Risks associated with the financial crime threat to the company
- Identity and responsibilities of the MLRO
- Internal policies and procedures put in place
- Customer Due Diligence/Enhanced due diligence monitoring measures
- Suspicious activity – what to look out for
- How to submit an internal Suspicious Activity Report to the MLRO
- Record-keeping requirement

The MLRO will take appropriate measures to keep a log of all training which is provided to staff members – a sample of the training log is attached in the appendix.

All staff will be required to sign the training log where required to confirm that they have received training.

The MLRO will circulate to all staff other material to heighten awareness of anti-financial crime issues. This must be placed on the company notice board which should be available in all branch/agent locations.

Where possible, MLRO will arrange for external trainings for the staff and a record will be kept of the training material and results.

All agents must take AML/CFT training before they are permitted to create customer transactions. All agents must receive refresher training annually or on need basis.

15.1 RETENTION OF RECORDS

General Legal Requirements

We will only be successful in demonstrating our compliance with the requirements of the regulations through keeping evidence and records of:

- Due diligence checks made and
- Information held on customers and transactions.

These records are crucial in any subsequent investigation by FIU, the police or other Supervisory Authority in other host state. They will enable the business to produce a sound defense against any suspicion of involvement in money laundering or terrorist financing, or charges of failure to comply with the Regulations.

The records that must be kept are:

- A copy of, or the references to, the evidence of the customer's identity obtained under the customer due diligence requirements in the Regulations. Clear copies of the forms of identification presented by customers, or a record of where they can be obtained, should be retained.

- The supporting evidence and records in respect of the business relationships and occasional transactions which are the subject of customer due diligence measures or on-going monitoring. Records must be kept and should include the name and address of the customer.

In relation to the evidence of a customer's due diligence of the Company and its Agents must keep the following records:

- All copies of documents accepted and verified as evidence for conduct of due diligence and
- all other References to the evidence of customer's identity
- Transaction and business relationship records including evidence of the customers' source of fund (including account files, relevant business correspondence, daily log books, receipts, cheques etc.) should be maintained in a form from which a satisfactory audit trail may be compiled, and which may establish a financial profile of any suspect account or customer.

How long the customer due diligence records must be kept?

Evidence of customer's identity records must be kept for minimum of Seven years beginning from the end of the year during which the date of completion of the transaction or the termination of the business relationship occurred.

The same retention period applies to records of transactions (whether undertaken as occasional transactions or part of a business relationship).

In what format must the records be kept?

Records may therefore be kept:

- By way of original documents
- By way of good photocopies of original documents
- In scanned form

- In computerized or electronic form.

It must be ensured, however, that the data stored electronically is consistent with the original document.

16.1 INDEPENDENT REVIEW OF RizonPay Limited ANTI-MONEY LAUNDERING PROGRAM

At least once in every two years, the Company will appoint an internal or external reviewer to conduct independent review of its AML program, first review will be carried by the end of 2023. The review will cover the testing of the following area:

- Documented AML and Sanctions Screening Policies and Procedures
- Enterprise Wide AML Risk Assessments
- Senior Management/Board Approval of AML Program
- How the business ensures that it holds the appropriate authorizations and abides by local laws both where it has an on the ground presence and where it conducts business on a reach-in basis?
- Customer KYC/CDD and EDD Onboarding and Refresh Processes – Test Customer Files. If company adopts Machine Learning KYC ID&V, test escalation process for clients who do not pass ID&V.
- Customer Risk Scoring – Review of Methodology and Risk Matrices
- Transaction Monitoring System – Review of Methodology
- Transaction Monitoring – Alert Process – Testing of Actions on Alerts
- Transaction Monitoring - Review of QA process relating to discounting of Alerts
- Suspicious Activity monitoring, escalation and reporting (SAR)
- Sanction and PEP Screening and Escalation Process
- Sanctions Screening System – Testing of Fuzzy Logic and List Maintenance
- Ongoing Monitoring Process – (Sanctions and Negative News) Testing
- AML system controls and data integrity
- Third Part Payment Process Policy Review and Testing
- Suspicious Activity Reporting Process - Testing
- AML Training – Program and Oversight Process
- Record keeping/retention

Management and key officers to be interviewed, including:

- Accountable Executives for awareness and responsibilities in the AML control Process
- AML Officer
- Compliance Team Leaders
- Business Leads and Support Unit Heads
- Front office management for AML Procedures and Customer Onboarding
- Operational Heads responsible for AML/Sanctions Screening controls
- IT Head for AML/Sanctions Screening operational system controls (transaction monitoring, customer information)
- Quality and Assurance Teams

Scoping must ensure:

- Coverage of the entire AML/Sanctions Screening Program; while also being

- Risk based to allocate the independent reviewer's time and staff resources to areas of greater risk and heavier testing of internal controls

APPENDIX I – RISK ASSESSMENT & MITIGATION

RISK MATRIX/RISK SCORE

LIKELIHOOD	IMPACT		
High likelihood	Medium - 2	High - 3	Extreme - 4
Medium likelihood	Low - 1	Medium - 2	High - 3
Low likelihood	Low - 1	Low - 1	N/A
	Minor	Moderate	Major

Likelihood: the potential of an ML/TF risk occurring in your business for the particular risk being assessed.

Impact (consequence): the seriousness of the loss or damage which could occur should the event (risk) happen

High Likelihood:	Almost certain that risk event will occur several times a year
Medium Likelihood:	High probability that risk event will occur once a year
Low Likelihood:	Unlikely, if not impossible

Major Impact:	Huge consequences – major damage or effect. Serious terrorist act or large scale money laundering
Moderate Impact:	Moderate level of money laundering or terrorism financing
Minor Impact:	Minor or negligible consequences or effects

The risk that RizonPay Limited services will be used for ML/TF. Risk group – Customers

Customer Risk

Customer Risk Factors	Risk Indicator	Likelihood	Impact	Risk Score	RizonPay Limited Action/ Control(refer Control Library)	Hard wire control which effectively mitigates risk
New customer carrying out large (cash) transaction	Transactions are almost always paid in by cash to agent	Medium / High	Moderate	Medium 2	• Cash transactions maximum threshold • Enhanced Customer Due Diligence • Systems controls (transaction screens) • Monitoring • AML/Compliance awareness training • Assurance processes • Prohibited customers and transactions	1. An absolute ceiling of HKD equivalent of EURO 5,000 prevents any transaction above this amount from being processed. Reduced limits apply to particular countries; 2. Multiple transactions by common sender or to common beneficiary to circumvent max threshold limits are tracked by phone number and ID details. System will automatically block second and following transactions – as well as first transaction if payout is still pending.
Non-resident Customer	Possibility for remittance transactions sent overseas by non-residents.	Low	Minor/ Moderate	Low 1	• Customer acceptance • Systems controls (transaction screens) • Enhanced customer due diligence • AML/Compliance awareness training	
Entities that are opaque, personal asset holding	Transactions by legal, non-individual entities.	Low	Minor	Low 1	• Customer acceptance • Systems controls (transaction screens) • Enhanced	Only individual to individual transactions are permitted - RizonPay Limited system requires

vehicles (e.g. trust, company)					customer due diligence	completion of fields including: name/surname, DOB, ID information. No transaction is permitted by a non-individual.
PEP (Politically Exposed Person)	Person whose stated occupation or ID document details or screening results indicate likelihood of PEP status.	Low	Minor	Low 1	• Sanction List screening • Monitoring • Customer acceptance • Systems controls (transaction screens) • AML/Compliance awareness training	
Customer or group of customers making numerous Transactions to same individual/ group	Multiple transactions just below threshold; Multiple transactions to common beneficiary; Multiple transactions from common sender.	Medium	Moderate	Medium 2	• Cash transactions Threshold of Zero • Monitoring • Customer acceptance • Enhanced customer due diligence • Systems controls (transaction screens) • AML/Compliance awareness training • Unusual Transaction reporting • Suspicious Activity Reporting	1. An absolute ceiling of HKD equivalent of EURO 5,000 prevents any transaction above this amount from being processed. Reduced limits apply to particular countries; 2. Multiple transactions by common sender or to common beneficiary to circumvent max threshold limits are tracked by phone number and ID details. System will automatically block second and following transactions – as well as first transaction if payout is still pending.
Customer who has a business/ occupation which is cash-intensive	Customer performs large volume of transactions which are inconsistent with	Low/Medium	Minor/ Moderate	Low 1	• Cash transactions maximum threshold • Customer acceptance • Systems controls (transaction screens) • Enhanced	An absolute ceiling of HKD equivalent of EURO 5,000 prevents any transaction above this amount from being processed. Reduced limits apply to particular countries.

	customer's profile as individual and stated source of income.				customer due diligence • AML/Compliance awareness training • Monitoring	
Customer who presents unusual or invalid ID	Customers do not always possess common acceptable ID types such as: EU National ID passport or Age proof card.	Low	Moderate/ Major	Medium 2	• Customer acceptance • Enhanced customer due diligence • Monitoring • Assurance processes • AML/Compliance awareness training	Foreign driver licenses and non-photographic ID documents are not acceptable for customer ID verification or transaction identity verification purposes.
Customer ID verifications not done properly	Incomplete or inaccurate customer data provided by customer and accepted by agent; The Company has lower level of control over customer due diligence verification as this is performed by agents*)	Low	Moderate/ Major	Medium 2	• Systems controls (transaction screens) • Enhanced customer due diligence • Monitoring • AML/Compliance awareness training • Assurance processes	Agent must provide confirmation/declaration for each and every transaction that customer verification processes have been performed correctly.
Affiliate agents are typically small businesses (<5 persons); Agents operate in a different industry environment with different business priorities. The knowledge and experience of KYC compliance procedures is of a lesser standard resulting in a lower level understanding of AML/CTF obligations including significance and ramifications of ML offences – and what constitutes particular ML offences. Remittance services often represent a low proportion of the affiliate agent's business revenue. Therefore, there is a higher risk for inadequate verification processes occurring						

Product Risk

Product Risk Factors	Risk Indicator	Likelihood	Impact	Risk Score	RizonPay Limited Action/ Control(refer	Hard wire control which effectively mitigates risk

					Control Library)	
Door Delivery Service		Low	Moderate	Low 1	• Customer acceptance • Enhanced customer due diligence • Assurance processes	N/A
Account Credit		Low/Medium	Minor/ Moderate	Medium 2	• Customer acceptance • Enhanced customer due diligence • Assurance processes • Monitoring	
E-services: cash to card		Low	Minor	Low 1	• Customer acceptance • Enhanced customer due diligence • Assurance processes • Monitoring	N/A
E-services: cash to mobile		Low	Minor	Low 1	• Customer acceptance • Enhanced customer due diligence • Assurance processes • Monitoring	N/A
Cash to Cash		Medium	Moderate	Medium 2	• Cash transactions maximum threshold • Monitoring • Customer acceptance • Enhanced customer due diligence • Systems controls (transaction screens) • AML/Compliance awareness training • Assurance processes • List screening • Suspicious Activity Reporting	1. An absolute ceiling of HKD equivalent of EURO 5,000prevents any transaction above this amount from being processed. Reduced limits apply to particular countries; 2. Multiple transactions by common sender or to common beneficiary to circumvent max threshold limits are tracked by phone number and ID details. System will automatically block second and following

						transactions – as well as first transaction if payout is still pending.

Business Practice Risk Factors	Risk Indicator	Likelihood	Impact	Risk Score	RizonPay LimitedAction/ Control(refer Control Library)	Hard wire control which effectively mitigates risk
Face to face transactions – paid out via bank partners (cash to cash; account credit; cash to card; cash to mobile)		Low/Medium	Minor/Moderate	Medium 2	• Customer acceptance • Enhanced customer due diligence • Assurance processes • Monitoring • List screening	
Face to face transactions – paid out via direct agent partners (Cash to cash; cheque payment; door delivery)		Medium	Moderate	Medium 2	• Customer acceptance • Enhanced customer due diligence • Assurance processes • Monitoring • List screening	
Online/internet (currently not available)		Zero	N/A	N/A 0	No action required	

Likelihood: the potential of an ML/TF risk occurring in your business for the particular risk being assessed.
Impact (consequence): the seriousness of the loss or damage which could occur should the event (risk) happen
Explanatory notes:

'FATF has recognized that specific products, services, transactions or delivery channels may pose a greater risk of money laundering. Examples include private banking, anonymous transactions (which may include cash), non-face-to-face business relationships or transactions, and payment received from unknown or un-associated third parties.'

Geographic Risk

Country Risk Factors	Risk Indicator	Likelihood	Impact	Risk Score	RizonPay Limited Action/ Control(refer Control Library)	Hard wire control which effectively mitigates risk
Countries identified by credible	Transactions to countries identified as	Medium	Moderate	Medium 2	• Country ML/TF risk index	1. An absolute ceiling of HKD equivalent of

sources as not having adequate AML/ CTF systems1	having deficient AML/CTF systems according to RizonPay Limited country risk indicators. Transactions with any country ranked 7.0 or above on Basel AML Index Country Risk Rating presents this risk.				• Monitoring • Red flags • Enhanced customer due diligence • List screening • Suspicious Matter Reporting	EURO 5,000 prevents any transaction above this amount from being processed. Note: Reduced limits apply to particular countries 2. For country corridors where this risk is categorized as High-Extreme, RizonPay Limited makes a determination to exit operations/ distribution network from that country (e.g. Iran, North Korea, Cuba, Somalia etc.).
Countries which are subject to EU trade sanctions1	Country is listed as being subject to sanctions by EU/UN/FATF	Low	Moderate	Low 1	• Country ML/TF risk index • Monitoring • Red flags • Enhanced customer due diligence • List screening • Suspicious Matter Reporting	Most countries which have UN sanctions in place are categorized as High to Extreme risk, and RizonPay Limited consequently does not have business in place.
Countries – or geographic areas identified by credible sources as being known to be a significant source of criminal activity*2	Transactions to countries identified as being known to be source of criminal activity according to RizonPay Limited	Medium	Moderate	Medium 2	• Country ML/TF risk index • Customer acceptance • Enhanced customer due diligence • Agent due diligence processes • Systems	For country corridors where this risk is categorised as High- Extreme, RizonPay Limited makes a determination to exit operations/ distribution network

	country risk indicators.				controls (transaction screens) • Monitoring from that country • Red flags • List screening • Suspicious Matter Reporting	
Countries – or geographic areas identified by credible sources as being linked to terrorism activity*3	Transactions to countries identified as being known to be source of terrorism activity according to RizonPay Limited country risk indicators.	Low	Major	Medium 2	• Country ML/TF risk index • Monitoring • Red flags • Enhanced customer due diligence • List screening • Suspicious Matter Reporting	1. All countries on US State Dept blacklist (Cuba, Iran, Sudan and Syria) are excluded from RizonPay Limited country network;
Explanatory notes: *Criminal activity to include: tax haven activity; source of narcotics; corruption; people smuggling; or other significant criminal activity. **Terrorism activity to include: funding or support provided for terrorist activities or designated terrorist organizations operating within the country.						

Regulatory Risk Factors	Risk Indicator	Likelihood	Impact	Risk Score	RizonPay Limited Action/ Control(refer Control Library)	Hard wire control which effectively mitigates risk
Agent conducting transactions while not registered with location jurisdictional regulatory body as the Company's affiliate		Low	Moderate	Low 1	• Agent due diligence processes • Robust Agent f & p assessment • Separation of duties – Employees	Agents are only activated in the Company's system by the Company's Operations Specialists to be able to conduct transactions, once confirmation has been received by the Company's. Compliance department.
Key Personnel not adequately	Agents with opaque business	Medium	Moderate	Medium 2	Agent due diligence processes	Applications for registration are not approved by the

confirmed	structure such as company or trust;				Agent ID Verification and Authentication Certified copies of ID documents Operational support by the Company Robust Agent f & p	Company's compliance without full documentation and approval.
Customer ID verifications not done properly	Incomplete or inaccurate customer data entered into the Company's transaction system creating data quality errors for reporting purposes	Low/Medium	Moderate	Medium 2	• Systems controls (transaction screens) • Enhanced customer due diligence • Monitoring • AML/Compliance awareness training • Assurance processes	Agent must provide confirmation/declaration for each and every transaction that customer verification processes have been performed correctly.
Failure to train the Company's staff adequately	Inadequate training records	Medium	Moderate	Medium 2	• AML/Compliance awareness training • Record-keeping • Operational support by the Company	Quarterly Board Meeting Review program for oversight
Not having an AML/CTF Program	No program in place.	Low	Moderate	Low 1	• AML/CTF Program	Quarterly Board Meeting Review program for oversight
Failure to generate reports for monitoring and providing support to Agents for regulatory reporting within required time		Low	Minor/ Moderate	Low 1	• Scheduled reports for various parameters (e.g. monthly / half yearly Analysis report) • Employee roles – RizonPay Limited	IT generated reports are scheduled on a monthly basis. Reports generated are cross-checked with an alternative system query to identify transactions that are not captured in IT generation process.
The Company's failure to		Low/Medium	Moderate	Medium 2	• Monitoring • List screening • Suspicious	Quarterly Board Meeting Review program for oversight

report suspicious matters					Matter Reporting • Contract with Affiliate Agents	
Not having an AML/CTF Compliance Report		Low	Moderate	Low 1	• Compliance reporting • Employee roles – RizonPay Limited	Quarterly Board Meeting Review program for oversight
Not having an AML/CTF Compliance Officer		Low	Moderate/ Major	Medium 2	• AML/CTF Compliance Officer role • Employee roles • Board oversight	Quarterly Board Meeting Review program for oversight
Explanatory notes: • 'A jurisdiction compliant with the FATF Recommendations poses a far lower risk of money laundering generally – including corruption-related money laundering – than a jurisdiction that does not' • Countries which are determined to represent an unacceptable risk to RizonPay Limited are withdrawn from distribution network (e.g. Iran, Somalia, Afghanistan, Sudan)						

Regulatory Risk Factors	Risk Indicator	Likelihood	Impact	Risk Score	RizonPay Limited Action/ Control(refer Control Library)	Hard wire control which effectively mitigates risk
Agent conducting transactions while not registered with local regulatory body as the Company's affiliate		Low	Moderate	Low 1	• Agent due diligence processes • Reporting Entity Roll • Agent f&P Assessment Separation of duties - Employees	Agents are only activated in the Company system by the Company Operations Specialists to be able to conduct transactions, once confirmation has been received by the Company Compliance department.
Agent personnel who meet the criteria of Key Personnel are not declared to the Company	Documentation and observation of agent indicates additional key personnel may be in existence.	Medium	Moderate	Medium 2	• Agent due diligence processes • Agent ID Verification and Authentication • Certified copies of ID documents	Applications for registration is verified and/or not submitted to local regulator where the Company is a registered entity without full documentation and declarations received by the Company's

					• Operational support by the Company • Agent f&P Assessment	Compliance department.
Agent verification not done properly (and subsequent data quality errors in regulatory reporting)	Incomplete or inaccurate customer data provided by customer and accepted by agent leading to data quality errors in regulatory reporting by the Company in applicable jurisdictions.	Low/Medium	Moderate	Medium 2	• Systems controls (transaction screens) • Enhanced customer due diligence • Monitoring • AML/Compliance awareness training • Assurance processes	Agent must provide confirmation/declaration for each and every transaction that customer verification processes have been performed correctly.
Failure by affiliate agent to train staff adequately	Inadequate training records; Systemic errors in customer acceptance and transactions.	Medium	Moderate	Medium 2	• AML/Compliance awareness training • Record-keeping • Operational support by the Company	Regular on-site and off site compliance checks by Compliance Team
Not having an AML/CTF Program	No program in place.	Low	Moderate	Low 1	• AML/CTF program • Assurance processes	• Company on-boarding procedure
Failure to report unusual matters to the Company which may constitute a suspicious matter		Low/Medium	Moderate	Medium 2	• Unusual matter reporting • Monitoring • List screening • Contract with Affiliate Agents	Regular on-site and off site compliance checks by Compliance Team
Not having an AML/CTF Compliance Report		Low	Moderate		• Compliance reporting • Employee roles	Regular on-site and off site compliance checks by Compliance Team

APPENDIX II – SAR SUBMISSION FORM

SAR Submission Form

SAR No: _____

Agent Name & Prefix: _____

To: Money Laundering Reporting Officer

From: _____Job Title:_____

I consider the following transaction suspicious and report to you under the internal reporting procedure:

SAR Submission Date: _____/_____ /_____

This SAR is:

☐ A request for consent for a transaction which has not yet completed
☐ A report on a transaction which has taken place which I consider suspicious
☐ Report on other business related activities which I consider suspicious

Transaction Details:			
Sender Name:		Receiver Name:	
Transaction Pin:		Transaction Amount	
Transaction Date:		Transaction Hold Date:	
Reason of Suspiciousness: **Action Taken:** Signed: (Please attach ids and supportive documents)			

Remarks by MLRO: _____

Dated: _____ Signed: _____

NOTE* Following submission of this SAR, the submitter should not discuss the matter with anyone. The MLRO will directly respond with further instructions.

APPENDIX III – SOURCE OF FUNDS DECELERATION FORM

COMPLIANCE FORM – ORIGIN AND PURPOSE OF FUNDS

Date (dd/mm/aa)_____No of transaction_____Transaction No._____ Current Amount_____Total Amount:_____

IDENTIFICACION
Remittent information:

Name(First Name + Last Name) _____
Address_____
TEL_____
City_____Country_____Resident _____
ID document - resident card, passport etc._____
ID Number_____Expiry date_____
Date of birth_____

Job activity_____Country of job activity_____
Place of working_____Job position_____
Employer's TEL._____Employer's address_____
Relationship with beneficiary_____

Origin and purpose of the transfer:

Origin of funds (*)_____

Purpose of the transfer, funds will be used for_____

Beneficiary information:

First Name + Last Name_____Date of birth_____
Address_____TEL_____
City_____Country_____Resident _____No_____
Job activity_____

Sender's undertaking:

I hereby declare that i am not involved in any criminal or money laundering activity and the funds for the above transaction were obtained by me are clear and are not derived from any illegal activities. These funds are derived from the following source.

Agent undertaking:

I/we have examined the photo id/documents of the sender listed above and certify that the sender information recorded matches the information in the ID presented to me/us.

Signature of sender_____

Signature of Agent _____

APPENDIX IV – AML/CTF TRAINING ACKNOWLEDGMENT

Date: 01.08.2023 Ref: RPLNo. 21/08/2023-1

Type: Initial/Refresher Training Conducted by: _____

AML/CTF - TRAINING ACKNOWLEDGMENT

Dear Sir,

I acknowledge the receipt of a copy of RizonPay Limited "Compliance Manual" and confirm that I have read, understood and will comply with the procedures outlined in this manual. I have also undergone the basic AML-training provided by RizonPay Limited. I will likewise give similar training to any of my employees who will conduct transactions on my behalf, or otherwise contact RizonPay Limited to have them trained, before they operate the RizonPay Limited transaction system. I agree to refer any compliance-related questions or difficulties to yourself or to whomever you nominate to act in your absence.

I confirm that compliance at all times with the procedures set out in the manual is a term of our contract with RizonPay Limited. Any breaches to these terms may result in termination of the RizonPay Limited Agreement.

Name: _____

Signature: _____

Date: 01.08.2023

APPENDIX V – LAWS AND REGULATIONS

Legislation concerned with ML, TF, financing of proliferation of weapons of mass destruction (PF) and financial sanctions

Role of the Financial Action Task Force (the FATF)

The Financial Action Task Force (the FATF) is an inter-governmental body formed in 1989. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating of ML, TF, PF, and other related threats to the integrity of the international financial system.

The FATF has developed a series of Recommendations that are recognized as the international standard for combating of ML, TF and PF. They form the basis for a co-ordinated response to these threats to the integrity of the financial system and help ensure a level playing field. In order to ensure full and effective implementation of its standards at the global level, the FATF monitors compliance by conducting evaluations on jurisdictions and undertakes stringent follow- up after the evaluations, including identifying high-risk and other monitored jurisdictions which could be subject to enhanced scrutiny by the FATF or counter-measures by the FATF members and the international community at large.

Many major economies have joined the FATF which has developed into a global network for international cooperation that facilitates exchanges between member jurisdictions. As a member of the FATF, **Hong Kong is obliged to implement the latest FATF Recommendations and it is important that Hong Kong complies with the international AML/CFT standards in order to maintain its status as an international financial centre.**

Main legislation pieces regulating AML and CFT

The main pieces of legislation in Hong Kong that are concerned with ML, TF, PF and financial sanctions are:

- the AMLO,
- the Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405 (DTROP),
- the Organized and Serious Crimes Ordinance, Cap. 455 (OSCO),
- the United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575 (UNATMO),
- the United Nations Sanctions Ordinance, Cap. 537 (UNSO), and
- the Weapons of Mass Destruction (Control of Provision of Services) Ordinance, Cap. 526 (WMD(CPS)O).

It is very important that MSOs and their officers and staff fully understand their respective responsibilities under the different legislation.

Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap. 615 (AMLO):

The AMLO imposes requirements relating to customer due diligence (CDD) and record-keeping on MSOs and provides the Hong Kong Customs and Exercise Department with the powers to supervise compliance with these requirements and other requirements under the AMLO.

In addition, MSOs to take all reasonable measures (a) to ensure that proper safeguards exist to prevent a contravention of any requirement under RBA and AML and CTF Systems; and (b) to mitigate ML/TF risks.

The AMLO makes it a criminal offence if an MSO (1) knowingly; or (2) with the intent to defraud the Hong Kong Customs and Exercise Department, contravenes a specified provision of the AMLO.

The "specified provisions" are listed in Section 5(11) of the AMLO which are related to CDD requirements and Record-Keeping. If the MSO knowingly contravenes a specified provision, it is liable to a maximum term of imprisonment of 2 years and a fine of $1 million upon conviction. **If the MSO contravenes a specified provision with the intent to defraud the CCE, it is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.**

The AMLO also makes it a criminal offence if a person who is an employee of an MSO or is employed to work for an MSO or is concerned in the management of an MSO (1) knowingly; or (2) with the intent to defraud the MSO or the Hong Kong Customs and Exercise Department, causes or permits the MSO to contravene a specified provision in the AMLO. **If the person who is an employee of an MSO or is employed to work for an MSO or is concerned in the management of an MSO knowingly contravenes a specified provision he is liable to a maximum term of imprisonment of 2 years and a fine of $1 million upon conviction. If that person does so with the intent to defraud the MSO or the Hong Kong Customs and Exercise Department he is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.**

The Hong Kong Customs and Exercise Department may take disciplinary actions against MSOs for any contravention of a specified provision in the AMLO. The disciplinary actions that can be taken include publicly reprimanding the MSO; ordering the MSO to take any action for the purpose of remedying the contravention; and ordering the MSO to pay a pecuniary penalty not exceeding the greater of $10 million or 3 times the amount of profit gained, or costs avoided, by the MSO as a result of the contravention.

Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405 (DTROP):

The DTROP contains provisions for the investigation of assets that are suspected to be derived from drug trafficking activities, the freezing of assets on arrest and the confiscation of the proceeds from drug trafficking activities upon conviction.

Organized and Serious Crimes Ordinance, Cap. 455 (OSCO):

The OSCO, among other things:

a) gives officers of the Hong Kong Police and the Customs and Excise Department powers to investigate organized crime and triad activities;
b) gives the Courts jurisdiction to confiscate the proceeds of organized and serious crimes, to issue restraint orders and charging orders in relation to the property of a defendant of an offence specified in the OSCO;

c) creates an offence of money laundering in relation to the proceeds of indictable offences; and
d) enables the Courts, under appropriate circumstances, to receive information about an offender and an offence in order to determine whether the imposition of a greater sentence is appropriate where the offence amounts to an organised crime/triad related offence or other serious offences.

United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575 (UNATMO):

The UNATMO is principally directed towards implementing decisions contained in relevant United Nations Security Council Resolutions (UNSCRs) aimed at preventing the financing of terrorist acts and combating the threats posed by foreign terrorist fighters. Besides the mandatory elements of the relevant UNSCRs, the UNATMO also implements the more pressing elements of the FATF Recommendations specifically related to TF.

Under the DTROP and the OSCO, a person commits an offence if he deals with any property knowing or having reasonable grounds to believe it to represent any person's proceeds of drug trafficking or of an indictable offence respectively. The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine of $5 million.

The UNATMO, among other things, criminalizes the provision or collection of property and making any property or financial (or related) services available to terrorists or terrorist associates. The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine. The UNATMO also permits terrorist property to be frozen and subsequently forfeited.

The DTROP, the OSCO and the UNATMO also make it an offence if a person fails to disclose, as soon as it is reasonable for him to do so, his knowledge or suspicion of any property that directly or indirectly, represents a person's proceeds of, was used in connection with, or is intended to be used in connection with, drug trafficking, an indictable offence or is terrorist property respectively. This offence carries a maximum term of imprisonment of 3 months and a fine of $50,000 upon conviction.

"Tipping off" is another offence under the DTROP, the OSCO and the UNATMO. 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 any investigation which might be conducted following that first-mentioned disclosure. The maximum penalty for the offence upon conviction is imprisonment for 3 years and a fine.

United Nations Sanctions Ordinance, Cap. 537 (UNSO):

The UNSO provides for the imposition of sanctions against persons and against places outside the People's Republic of China arising from Chapter 7 of the Charter of the United Nations. Most UNSCRs are implemented in Hong Kong under the UNSO.

Weapons of Mass Destruction (Control of Provision of Services) Ordinance, Cap. 526 (WMD(CPS)O):

The WMD(CPS)O controls the provision of services that will or may assist the development, production, acquisition or stockpiling of weapons capable of causing mass destruction or that will or may assist the means of delivery of such weapons. Section 4 of WMD(CPS)O prohibits a person from providing any services where he believes or suspects, on reasonable grounds, that those services may be connected to PF. The provision of services is widely defined and includes the lending of money or other provision of financial assistance.

Financial Sanctions & Proliferation Financing:

The UNSO empowers the Chief Executive to make regulations to implement sanctions decided by the UNSC, including targeted financial sanctions44 against individuals and entities designated by the UNSC or its Committees. Designated persons and entities are specified by notice published in the Gazette or on the website of the Commerce and Economic Development Bureau. It is an offence to make available, directly or indirectly, any funds, or other financial assets, or economic resources, to, or for the benefit of, a designated person or entity, as well as those acting on their behalf, at their direction, or owned or controlled by them; or to deal with any funds, other financial assets or economic resources belonging to, or owned or controlled by, such persons and entities, except under the authority of a licence granted by the Chief Executive.

The Chief Executive may grant licence for making available or dealing with any funds, or other financial assets, and economic resources to or belonging to a designated person or entity under specified circumstances in accordance with the provisions of the relevant regulation made under the UNSO. An MSO seeking such a licence should write to the Commerce and Economic Development Bureau.

To combat PF, the UNSC adopts a two-tiered approach through resolutions made under Chapter VII of the UN Charter imposing mandatory obligations on UN member states:

a) global approach under UNSCR 1540 (2004) and its successor resolutions; and
b) country-specific approach under UNSCR 1718 (2006) against the Democratic People's Republic of Korea (DPRK) and
c) UNSCR 2231 (2015) against the Islamic Republic of Iran (Iran) and their successor resolutions.

The counter proliferation financing regime in Hong Kong is implemented through legislation, including the regulations made under the UNSO which are specific to DPRK and Iran, and the WMD(CPS)O. Section 4 of WMD(CPS)O prohibits a person from providing any services where he believes or suspects, on reasonable grounds, that those services may be connected to PF. The provision of services is widely defined and includes the lending of money or other provision of financial assistance.

Sanctions imposed by other Jurisdictions:

While, MSOs do not normally have any obligation under Hong Kong laws to have regard to unilateral sanctions imposed by other organisations or authorities in other jurisdictions, an MSO operating internationally will need to be aware of the scope and focus of relevant sanctions regimes in those jurisdictions. Where these sanctions regimes may affect its operations, the MSO should consider what implications exist for its procedures and take appropriate measures, such as including relevant overseas designations in its database for screening purpose, where applicable.

APPENDIX VI – DATA PROTECTION REQUIREMENTS IN RELATION TO AML

Background to the PDPO:

Hong Kong is one of Asia's earliest adopters of comprehensive data privacy regulation. The Personal Data (Privacy) Ordinance (the PDPO) came into force in 1996.Enforcement activity had been marginal for a number of years, but recent data privacy incidents, including a direct marketing scandal that became front page news in the summer of 2010, led to an overhaul of the regulatory regime in 2012 and a subsequent stepping up of enforcement action. Reforms brought into force in 2013 have made Hong Kong's regulation of direct marketing amongst the most stringent in the world.

Hong Kong's Privacy Commissioner for Personal Data (the Commissioner) is now very

active and regularly publishes official guidance on a wide range of topics. Guidance issued in February, 2014 calls for businesses to adopt comprehensive Privacy Management Programmes directed at achieving compliance in all aspects of business. With increased fines, an activist regulator, a policy of "naming and shaming" those who fail to comply and a growing public interest in data privacy issues, it is clear that PDPO compliance has to be a priority for Hong Kong businesses.

The Commissioner and his Powers:

The Commissioner can investigate complaints of breaches of the PDPO, as well as initiate investigations. The approach to enforcement is generally administrative and consultative in nature, but the scope for criminal enforcement has recently been broadened and the penalties for non-compliance have been increased.

At the conclusion of an investigation, the Commissioner can issue an enforcement notice against the "data user" (ie the business controlling the data processing), requiring it to take remedial action.

The Commissioner can institute civil or criminal proceedings against any data user that fails to comply with an enforcement notice, depending on the nature of the breach. Maximum penalties for breaches under the PDPO are fines of up to HK$1m (US$130,000) and imprisonment for up to five years.

Quite apart from the criminal sanctions, there are reputational risks for an organization that is subject to an investigation. The Commissioner has the right to publish the results of any investigation, name the organisation involved and give details of the breaches committed.

What is Personal Data?

The PDPO draws from the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the guidelines which are the cornerstone for Europe's Data Protection Directive EC95/46.

The PDPO defines "personal data" very broadly and includes any data relating directly or indirectly to a living individual from which it is practicable for the identity of the individual to be directly or indirectly ascertained.

Does the PDPO have Extraterritorial Effect?

The PDPO does not include any express limitation on its territorial scope. However, some limitation may be implied from the discretion the Commissioner has to refuse to investigate a complaint which does not meet one of the following requirements:

I. The investigation relates to the personal data of Hong Kong residents or persons who were in Hong Kong at the relevant time; or
II. The investigation relates to data users that are able to control the collection, holding, processing or use of the relevant personal data from Hong Kong.

On What basis can Personal Data be Processed?

"Processing" in relation to personal data, is defined to include amending, augmenting, deleting or rearranging data, by automated or other means. Subject to specific exemptions, personal data can only be processed for the purposes notified to the data subject on or before the collection of the data and any directly related purpose. Data subjects must consent to any new or additional purpose.

The PDPO contains a number of exemptions to these requirements, including an exemption for national security interests and exemptions for matters such as disclosures to law enforcement officials and processing in connection with legal proceedings.

Do Data owners need to Register with or notify any Authorities, or Appoint an Official Compliance Officer?

There is no need to register with or notify any authorities of data processing, nor is there any requirement to appoint an official compliance officer. However, data users must provide data subjects with the name or job title and address of the individual who will be responsible for handling data access requests.

In practical terms, it is becoming increasingly important to have senior internal roles that include responsibility for PDPO compliance. The Commissioner's February, 2014 guidance dealing with Privacy Management Programmes makes clear that significant organisational measures are the expected standard for compliance.

What Rights do Data Subjects have to Access and Correct their Data?

Data subjects have the right to know whether or not a business holds personal data about them. They have the right to access and make corrections to that data. Data users may refuse to comply with a request for access or a correction, but must be prepared to give reasons for doing so within 40 days of receipt of a proper request. They may charge a fee for producing the personal data.

Are there any Restrictions on Transfers of Personal Data to third Parties? Or within a Group of Companies?

Personal data cannot be transferred to another data user without the data subject's consent. Where transfers are made for direct marketing purposes, the special requirements set out in the section below entitled "How is direct marketing regulated?" apply.

The PDPO draws no distinction between related and unrelated entities, meaning that transfers within groups of companies are in principle regulated to the same standards. There is no requirement under the PDPO to obtain a data subject's consent to transfer personal data to a data processor (i.e., a person or entity which processes personal data on behalf of a data user). As a matter of practice, however, data users often notify data subjects that third party processing will be taking place.

Eight Principles of Data Protection:

a) It must be processed fairly and lawfully. We must inform individuals about how the Company uses their personal data;
b) It must be obtained only for specific lawful purposes;

c) It must be adequate, relevant and not excessive. We must only collect the minimum amount of personal data to support the Company's business activities;
d) It must be accurate and kept to date;
e) It must be processed in accordance with the rights of data subjects. We must be receptive to queries or requests made by individuals in connection with their personal data and where required by law, we must provide individuals with ability to access, correct and delete their personal data;
f) It must not have held for any longer than necessary;
g) It must be protected in appropriate ways, we need to prevent the misuse or loss of personal data and to prevent unauthorized access;
h) It must not be transferred outside Hong Kong, unless that country or territory also ensures an adequate level of protection, or other laws required us to (e.g. Wire Transfer Regulation 2).