AML/CTF Compliance program

First Business Transactions Limited

March 2020

•This AML/CTF Compliance Program shall apply to all branches and subsidiaries of First Business Transactions Limited both in Hong Kong and abroad.

•Implementation of this program will not detract from the obligation to comply with any other local law and is not to be regarded as enabling the implementation of acts that have been prohibited or restricted by local laws.

•First Business Transactions Limited maintains full cooperation with law and regulatory authorities in legislations, investigations and inquiries in Hong Kong and abroad.

•This AML/CTF Compliance Program is a subject to an annual review.

Introduced by:
Mr. Halkin - Compliance Officer/MLRO

MSO Licence No:
17-02-02081

Table of contents

Introduction

First Business Transactions Limited (hereinafter referred to as “First Business Transactions”) adopts appropriate, sufficient measures aimed to preventing its operations from being used as means to conceal, manage, invest or use any form of money – or other assets – due to illicit activities, or to give the appearance of legality to such activities. The company adopts a risk-based approach in the design and implementation of the AML/CTF Policy with a view to managing and mitigating ML/TF risks. A qualified Compliance Officer/Money Laundering Reporting Officer has been appointed to implement appropriate AML/CTF policies and procedures.

First Business Transactions' 5 Key AML/CTF Principles:

- to comply with AML/CTF legislation in the countries in which it operates;
- to strive to fulfil international standards as detailed by the Financial Action Task Force (FATF) recommendations;
- to work in conjunction with the Government of Hong Kong SAR and the governments of the countries First Business Transactions operates in, as well as support their objectives in relation to the prevention, detection and control of ML/TF;
- First Business Transactions may decide not to provide products or services based upon decisions guided by ML/TF risk appetite and corporate social responsibility;
- to comply with primary legislation of Hong Kong on AML/CTF: Anti-Money Laundering and Counter-Terrorist Financing Ordinance (“AMLO”), April 2018 and the Guideline on Anti-Money Laundering and Counter-Terrorist Financing (for MSO), November 2018.

First Business Transactions's AML/CTF Compliance Program:

- forms part of its wider compliance regime, and is designed to meet the requirements of its legislative environment;
- ensures that First Business Transactions is able to detect suspicious activities associated with money laundering, fraud, and terrorist financing, and report them to the appropriate authorities;
- focuses not only on the effectiveness of internal systems and controls developed to detect money laundering, but on the risk posed by the activities of customers with which First Business Transactions does business;
- is built on a strong foundation of regulatory understanding and overseen by personnel who are experienced and knowledgeable enough to create a climate of compliance at every level of their organisation.

Prevention of Money Laundering & Terrorist Financing in Hong Kong

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.

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:
(a) Placement - the physical disposal of cash proceeds derived from illegal activities;
(b) 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; and
(c) 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.

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 organisations 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.
FATF defines *"proliferation of weapons of mass destruction"* as the transfer and export of nuclear, chemical or biological weapons, their means of delivery and related materials.

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 recognised 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.

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.

Guidelines on Anti-Money Laundering and Counter-Terrorist Financing (for Money Service Operators) are issued by the Hong Kong Customs and Excise Department (HKCED), Government of Hong Kong SAR, to offer guidance to money service operators (MSOs). The guidelines are published under section 7 of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance, Cap. 615 (AMLO). The guidelines are intended for use by Financial Institutions (FIs), their officers and their staff.

First Business Transactions has established its AML/CTF Compliance Program to ensure that any money laundering risks identified by First Business Transactions are appropriately managed and mitigated. This means having adequate systems and controls in place to mitigate the risk of the company being used to facilitate any financial crimes. This program is designed to represent the basic standards of Anti-Money Laundering and Combating Terrorism Financing procedures and standards, which will be strictly observed by First Business Transactions.

The AML/CTF Compliance Program is based upon applicable AML/CTF laws, regulations and regulatory guidance from the Government of Hong Kong SAR. This program is further designed to comply with the Financial Action Task Force (FATF) Standards on combating money laundering and the financing of terrorism and proliferation. It also follows the AML principles of the Wolfsberg Group.

Money Service Operators licensed in Hong Kong are supervised by Customs and Excise Department of Hong Kong:

Money Service Supervision Bureau Customs and Excise Department
Nan Fung Commercial Centre
19 Lam Lok Street, Kowloon Bay, Kowloon
Telephone: (852) 2707 7837 Fax: (852) 2707 7838
E-mail: msoenquiry@customs.gov.hk

Chapter 1. AML / CTF SYSTEMS

The Primary Legislation Governing AML/CTF in Hong Kong is as follows:

- Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance ("AMLO"), Cap. 615 (revised April 2018)
- Drug Trafficking (Recovery of Proceeds) Ordinance ("DTROP"), Cap. 405 (revised September 2019)
- Organized and Serious Crimes Ordinance ("OSCO"), Cap. 455 (revised April 2018)
- United Nations (Anti-Terrorism) Measures Ordinance ("UNATMO"), Cap. 575 (revised 2019)
- Weapons of Mass Destruction Ordinance (WMDO), Cap. 526 (2014)

First Business Transactions firmly believes that a reputation for integrity and openness, both in its business model and in its management systems and procedures - are crucial to achievement of its commercial goals and plans, and also to the fulfilment of its corporate responsibilities. The company is, therefore, committed to the highest standards of Money Laundering and Combating Terrorism financing (AML/CTF) measures in its operations, and it adheres to both established and recommended international standards to prevent the use of its services for the above purposes.

Effective Controls

To ensure proper implementation of AML/CTF procedures and controls, First Business Transactions has effective controls covering:

- Effective AML/CTF compliance program
- Senior management oversight
- Appointment of Compliance Officer / Money Laundering Reporting Officer (MLRO)
- Compliance and audit function
- Staff screening and training.

The Director of First Business Transactions is responsible for managing the business effectively and for the oversight of internal AML/CTF controls and systems. Director appoints the Compliance Officer/MLRO who has overall responsibility for the establishment and maintenance of First Business Transactions' AML/CTF systems and is the central reference point for suspicious transaction reporting.

Three Lines of Defence

First Business Transactions follows the three lines of defense framework when managing ML/TF risks. The three lines of defense is an industry model for managing risk. It is used to structure roles, responsibilities and accountabilities for decision making, risk and control management, and independent assurance. The three lines of defense are used as the fundamental guiding principle when performing the AML/CTF review.

Board of Directors' Responsibilities

The Board of Directors' responsibilities include but are not limited to:

- Maintaining compliance with effective laws of Hong Kong
- Monitoring and overseeing the compliance activities of the Company to ensure they are in accordance with the applicable federal and state laws, regulations and internal policies and procedures;

- Reviewing the AML/CTF Compliance Program to ensure it is comprehensive, adequate and viable;
- Approving the AML/CTF Compliance Program;
- Ensuring that the AML/CTF Compliance Program is effectively implemented by the Company's management and Chief Compliance officer/MLRO;
- Designating a qualified employee to serve as the Company's Chief Compliance Officer;
- Reviewing the performance of the Chief Compliance officer/MLRO;
- Ensuring that the Chief Compliance officer/MLRO has sufficient authority and resources (monetary, physical and personnel) to administer an effective AML/CTF Compliance Program based on the Company's risk profile;
- Periodically receiving and reviewing reports presented by the Chief Compliance Officer to ensure that the compliance program is being executed as approved and that it is, in fact, serving its intended purpose of maintaining the integrity, safety and soundness of the Company;
- Annually reviewing changes proposed to be made to AML/CTF Compliance Program, and, if satisfied that the modifications are desirable, approving the modifications/changes;
- Designating and contracting the services of a competent entity to perform independent compliance audits of the Company to test for the Company's level of adherence to the applicable anti-money laundering and anti-terrorist laws and regulations.

The Senior Management of the Company have approved this AML/CTF Compliance Program and the designation of the Chief Compliance Officer/MLRO, and have assigned responsibility to such person to maintain and monitor overall compliance on a day-to-day basis with AML/CTF requirements.

Compliance Officer / MLRO

The Compliance Officer/MLRO acts as the focal point within the company for the oversight of all activities relating to the prevention and detection of ML/TF and providing support and guidance to the senior management to ensure that ML/TF risks are adequately managed.

Compliance Officer /MLRO is sufficiently independent and has a direct reporting line to the company's executive board. Compliance Officer /MLRO has access to sufficient resources and information to be able to ensure company's compliance with effective laws and regulations of Hong Kong.

In particular, the Compliance Officer/MLRO assumes responsibility for:

- developing and/or continuously reviewing the AML/CTF systems to ensure they remain up-to-date and meet current statutory and regulatory requirements;
- the oversight of all aspects of the AML/CTF systems which include monitoring effectiveness and enhancing the controls and procedures where necessary.

The Compliance Officer/MLRO plays an active role in the identification and reporting of suspicious transactions. Principal functions of Compliance Officer/MLRO include in particular:

- reviewing all internal disclosures and exception reports and determining whether or not it is necessary to make a report to the JFIU;
- maintaining all records related to such internal reviews;
- providing guidance on how to avoid "tipping off" if any disclosure is made;
- acting as the main point of contact with the JFIU, law enforcement, and any other competent authorities in relation to ML/TF prevention and detection, investigation or compliance.

In addition, Compliance Officer/MLRO:

- conducts on-going monitoring of First Business Transactions' relationships with it customers;
- on a daily basis conducts monitoring of customers transactions;
- identifies suspicious transactions and activities;
- monitors changes of regulatory requirements with respect to ML/CTF prevention and counteraction;
- communicates all AML/CTF relevant issues to the Directors;
- develops internal training programs and materials.

Audit Function

Audit function shall be established to perform regularly reviews of the AML/CTF systems, e.g. sample testing, (in particular, the system for recognising and reporting suspicious transactions) to ensure effectiveness. The frequency and extent of the review should be commensurate with the risks of ML/TF and the size of First Business Transactions business. Where appropriate, First Business Transactions will seek a review from external auditors.

Independent Audit Functions include:

- Compliance and audit functions are independent in practice
- The regular review is performed at a frequency of once a year
- External party is leveraged to perform the auditing
- Availability of direct communication to senior management through regular committees (compliance committee) or other means of direct communication

Know Your Employee

The best way to reduce insider abuse is to stop it before it starts. It starts during the hiring process, with First Business Transactions exercising the same precautions as it does when opening an account. First Business Transactions performs due diligence on employees verifying any information supplied.

Integrity of Staff

Integrity is one of the fundamental values that First Business Transactions seeks in the employees it is going to hire. Integrity involves moral judgment and character, honesty and leadership values.

Counter-Checking of Work Completed by Staff

First Business Transactions performs occasional spot checks on work done by staff at all levels. Usually, these checks are undertaken by senior management to ensure that First Business Transactions policies and procedures are being followed and everything is in the correct order.

First Business Transactions has a “Zero Tolerance” policy regarding intentional violation of applicable laws prohibiting money laundering, terrorist financing and related financial crimes. First Business Transactions will require the immediate discharge of an employee who commits such violations, and will refer such cases to the appropriate regulatory bodies.

Procedures for Employees engaged in a Suspicious Activity

If an employee is suspected of engaging in any type of unusual or questionable activity, this must be brought to the attention of both Senior Management and the Compliance officer immediately.

Senior Management and/or the Compliance officer will jointly investigate the actions of the employee in the most discreet manner. All actions taken to conduct the investigation must be documented.

Senior Management determines that the employee’s activity was prejudicial to the interests of the Company, it will determine whether disciplinary action is necessary. Senior Management may seek advice from legal counsel in such action. The decision to file a STR is independent of any disciplinary action (e.g., termination, suspension, etc.) that may be taken against the employee.

In order to know its employees First Business Transactions conducts:

- a criminal conviction search in jurisdictions where it is possible;
- credit checks;
- a private investigation, if thought necessary;
- an internet check before they are hired.

AML/CTF Training

First Business Transactions has a clear policy towards staff training with respect to AML/CTF issues. Staff is being made aware of:

- First Business Transactions' and their own personal statutory obligations and the possible consequences for failure to report suspicious transactions under the DTROP, the OSCO and the UNATMO;
- any other statutory and regulatory obligations that concern First Business Transactions and themselves under the DTROP, the OSCO, the UNATMO, the UNSO and the AMLO, and the possible consequences of breaches of these obligations;
- the First Business Transactions' policies and procedures relating to AML/CTF, including suspicious transaction identification and reporting;
- any new and emerging techniques, methods and trends in ML/TF to the extent that such information is needed by the staff to carry out their particular roles in First Business Transactions with respect to AML/CTF.

The training is assigned for all groups of First Business Transactions' staff:

- all new staff, irrespective of seniority;
- to the Compliance Officer/ MLRO;
- back-office staff, depending on their roles;
- managerial staff.

Training program provides staff with an understanding of the process of money laundering, the laws and regulations that make it illegal, and the responsibilities of employees to help detect and prevent it.
The training on AML/CTF issues raises awareness of financial crime risks, global laws and regulations, laws and regulations applicable to First Business Transactions.

Annual AML Seminar

Designed for all operational staff and includes:

- General information: the background and history pertaining to money laundering controls, what money laundering and terrorist financing is;
- Legal framework: how AML/CFT laws and regulations apply to First Business Transactions and its employees;
- Penalties for anti-money laundering violations, including criminal and civil penalties, fines, jail terms, as well as internal sanctions, such as disciplinary action up to and including termination of employment;
- How to react when faced with a suspicious client or activity;
- Internal policies, such as customer identification and verification procedures and CDD policies;
- What the legal record keeping requirements are;
- Suspicious activity reporting requirements;
- Duties and accountability of employees.

Ad-hoc Training
Provided regularly to all employees based on, but not limited to, changes in government regulations, changes/amendments in First Business Transactions' AML/CFT policies and procedures.

First Business Transactions uses mix of training techniques and tools in delivering training, depending on the available resources and learning needs of its staff. These techniques and tools include visiting external seminars of Mastercard academy, on-line learning systems, focused classroom training, relevant videos as well as paper- or intranet-based procedures manuals. First Business Transactions also includes available FATF papers and typologies as part of its the training materials. All materials are kept up-to-date and in line with current requirements and standards.

The effectiveness of training is being monitored by testing the staff's understanding of AML/CTF issues and its ability to recognise suspicious activity. To achieve this First Business Transactions's Compliance Department conducts random testing sessions on a quarterly basis.
All training related records and documents are kept throughout the employment relationship with the employee and for a period of at least five years after the end of the employmen

Chapter 2. RISK-BASED APPROACH (RBA)

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

The inherent risk is assessed in course of identification of the specific products, services, customers, entities, and geographic locations. Depending on the specific characteristics of the particular product, service, or customer, the risks are not always the same. Various factors, such as the number and volume of transactions, geographic locations, and nature of the customer relationships, should be considered.

Risk assessment on the stage of on-boarding of a new customer is an opportunity for the management of First Business Transactions to gain an insight into the type and nature of its potential customers, their geographic locations and business activities.
Verifying identities, making sure they're real, confirming they're not on any prohibited lists, and assessing their risk factors—ensures that First Business Transactions keeps money laundering, terrorism financing, and more run-of-the-mill fraud schemes at bay.

First Business Transactions determines the extent of its CDD measures and ongoing monitoring, using a risk-based approach (RBA) depending upon the background of the customer and the product, transaction or service used by that customer, so that preventive or mitigating measures are commensurate to the risks identified.

The RBA enables First Business Transactions to subject its customers to proportionate controls and oversight by determining:

- the extent of the due diligence to be performed on the direct customer;
- the extent of the measures to be undertaken to verify the identity of any beneficial owner and any person purporting to act on behalf of the customer;
- the level of ongoing monitoring to be applied to the relationship;
- measures to mitigate any risks identified.

An RBA involves identifying and categorising ML/TF risks at the customer level and establishing reasonable measures based on risks identified. An RBA does not refrain First Business Transactions from engaging in transactions with customers or establishing business relationships with potential customers, but rather it assists First Business Transactions to effectively manage potential ML/TF risks.

Risk assessment and risk categories
First Business Transactions assess the ML/TF risks of its customers by assigning a ML/TF risk rating taking into consideration the following risk factors:

Geography risk
Customers with residence in or connection with high-risk jurisdictions:

- those that have been identified by the FATF as jurisdictions with strategic AML/CTF deficiencies;
- countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations;
- countries which are vulnerable to corruption;

- those countries that are believed to have strong links to terrorist activities.

In assessing country risk associated with a customer, consideration may be given to local legislation (United Nations Sanctions Ordinance (UNSO), UNATMO), data available from the United Nations, the International Monetary Fund, the World Bank, the FATF, etc. and the First Business Transactions' own experience.

Customer risk

The customers who might be considered to carry lower ML/TF risks: the reputation of the customer, e.g. a well-known, reputable private company, with a long history that is well documented by independent sources, including information regarding its ownership and control.

However, some customers, by their nature or behaviour might present a higher risk of ML/TF. Factors might include:

- the public profile of the customer indicating involvement with, or connection to PEPs;
- complexity of the relationship, including use of corporate structures, trusts and the use of nominee and bearer shares where there is no legitimate commercial rationale;
- a request to use numbered accounts or undue levels of secrecy with a transaction;
- involvement in cash-intensive businesses;
- nature, scope and location of business activities generating the funds/assets, having regard to sensitive or high-risk activities; and
- where the origin of wealth (for high risk customers and PEPs) or ownership cannot be easily verified.

  Product / service risk

  Factors presenting higher risk might include:
- services that inherently have provided more anonymity;
- ability to pool underlying customers/funds.

Delivery / distribution channel risk

The distribution channel for products may alter the risk profile of a customer. This may include sales through online, postal or telephone channels where a non-face-to-face account opening approach is used.

In addition, following high risk elements/factors should also be considered as per international standards:

Additional factors to be considered in measuring Customer risk will include the following:

- New services provided and new acquisitions made by the Company since the previous risk assessment
- Customer'sCompliance Program, its comprehensiveness and the effectiveness of its application;
- Structure of the compliance staff;
- Adequacy of the staff size;
- Experience level of each staff member;
- Knowledge base of each staff member;
- Level of empowerment the board and senior management gives to the department;
- Volume of STRs filed;

- Quality and effectiveness of functional and Customer -wide training;
- Breadth and depth of the independent audit function;
- Quality of the Customer's data processing system and the effectiveness of the monitoring software;
- Nature/severity/consequences of regulatory sanctions.

The annual risk assessment will be presented by the Compliance Officer and through the Compliance Officer to the Board.

First Business Transactions adjusts its risk assessment of a particular customer from time to time or based upon information received from a competent authority, and review the extent of the CDD and ongoing monitoring to be applied to the customer.

Low Risk – entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorised as low risk, Government Departments and Government owned companies, regulators and statutory bodies etc. Generally consumers with a small number or transfers and small dollar transactions would be considered LOW RISK.

Medium Risk – customers that are likely to pose a higher than average risk to First Business Transactions may be categorised as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds.

High Risk – First Business Transactions applies enhanced due diligence measures based on the risk assessment for higher risk customers, especially those for whom the sources of funds are not clear.

To all customers classified as high risk the procedure of enhanced due diligence is applied. The main criteria to rank the client as high risk are the following:

- the high risk jurisdiction domiciles of customers;
- the high risk or prohibited industries or activities of customers;
- complex shareholder structure with hidden UBOs;
- UBOs, PEPs, US-citizens as shareholders or key management personnel;
- restrictions or sanctions imposed on customers by regulatory authorities;
- customers who are not physically present for identification purposes (non face-to-face customers);
- non resident customers;
- Politically Exposed Persons (PEPs) accounts;
- customers from countries that are considered by the FATF inadequately to apply the FATF Recommendations;
- transactions that are unusual, lack an obvious economic or lawful purpose;
- transactions that are complex or large or might lend themselves to anonymity;
- trusts, charities, NGOs and organisation receiving donations;
- any other customers that their nature entail a higher risk of money laundering or terrorist financing;
- customers with dubious reputation as per public information available.

First Business Transactions categorises the following categories of customers as high-risk customers:

- High Net worth individuals
- Trusts, charities, NGOs and organisations receiving donations
- Companies having close family shareholding or beneficial ownership

- Firms with 'sleeping partners'
- Politically Exposed Persons (PEPs) of foreign origin
- Non-face to face customers
- Companies issuing bearer shares
- Trade of oil products
- Trade of new financial products (e.g. virtual currencies)
- Those with dubious reputation as per public information available
- Organisation and execution of auctions

Account Risk Reviews/Procedure
The Compliance officer/MLRO or Designee will review each customer's account as per the schedule below to determine if the risk rating is still applicable, or should be modified based on any changes of the identity of the customer, the nature of the customer's business, the customer's home country's AML risk, the actual volume in the account, and the actual nature of account activity as outlined above.

Only the Compliance officer/MLRO is permitted to alter a customer's risk rating. The Compliance officer/ MLRO will maintain relationship opening documentation, activity statements, and other necessary documentation to support the risk profiles assigned to accounts.

High Risk:
Due to the high-risk nature of these relationships, the Compliance officer/MLRO or Designee will perform monthly reviews of every High-Risk relationship including a transactional review.
Each High Risk customer will require Enhanced Due Diligence before the relationship and additional facts will be gathered to learn more about the business. For any Non-Individual Customer whose business has been identified as a "high-risk business," the Compliance officer/MLRO or Designee must also verify the existence of the business and purpose of the account.

Medium Risk:
The Compliance officer/MLRO will perform semi-annual reviews of every medium-risk relationships that is no longer a new relationship.

Low Risk:
The Compliance Officer will engage in annual reviews of each low-risk account.

Non-acceptable Customers
First Business Transactions does not accept clients from the industries as stated below:
- Trade /production/mediation in the trade of weapons
- Trade of antiques works of art, numismatic values
- Trade of ferrous, non-ferrous and rare metals and their wares, precocious stones
- Production/recycling of explosive and nuclear fuel
- Unregulated charities and other unregulated organisations
- Dealers of high-value precious goods
- Adult industries
- Wholesale trade of alcohol and tobacco products
- Unlicensed financial institutions / money service businesses

The detailed information on prohibited business types is captured in *Appendix 5* hereto.

Prohibition of Anonymous Accounts
First Business Transactions does not maintain anonymous accounts or accounts in fictitious names for any new or existing customer.

Prohibition of Shell Banks
First Business Transactions does not maintain correspondent relationships with shell banks, which are defined as non-resident banks that have no permanent executive bodies in the countries in which they have been registered, and has not entered into correspondent relationships with banks that allow their accounts to be used by shell banks.

Customer Due Diligence
Customer due diligence (CDD) is central to an effective anti-money laundering and counter-terrorism financing (AML/CTF) regime. First Business Transactions takes measures to identify and verify each of tits customers so it can:

- determine the money laundering and terrorism financing risk posed by each customer;
- decide whether to proceed with a business relationship or transaction;
- assess the level of future monitoring required.

Chapter 3. CUSTOMER DUE DILIGENCE (CDD)

Identification and Verification of the Customer's Identity

First Business Transactions applies the following CDD measures:

- identification of the customer and verification of the customer's identity using reliable, independent source documents, data or information;
- identification and taking reasonable measures to verify the beneficial owner's identity so that First Business Transactions is satisfied that it knows who the beneficial owner is, including in the case of a legal person or trust, measures to enable First Business Transactions to understand the ownership and control structure of the legal person or trust;
- obtaining an information on the purpose and intended nature of the business relationship unless the purpose and intended nature are obvious;

If a person purports to act on behalf of the customer, First Business Transactions take s measures to: identify the person and take reasonable measures to verify the person's

- identity using reliable and independent source documents, data or information;
- iverify the person's authority to act on behalf of the customer.

CDD requirements should apply:

- at the outset of a business relationship;
- before performing any occasional transaction:

i) equal to or exceeding an aggregate value of HKD 120,000, whether carried out in a single operation or several operations that appear to First Business Transactions to be linked;
ii) a wire transfer equal to or exceeding an aggregate value of HKD 8,000, whether carried out in a single operation or several operations that appear to First Business Transactions to be linked;

- when First Business Transactions suspects that the customer or the customer's account is involved in ML/TF irrespective of the amount of transaction;
- when First Business Transactions doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.

Occasional transaction – is a transaction between First Business Transactions and a customer who does not have a business relationship with First Business Transactions. Occasional transactions may include for example, wire transfers, currency exchanges, purchase of cashier orders or gift cheques.

First Business Transactions is vigilant to the possibility that a series of linked occasional transactions could meet or exceed the CDD thresholds of HKD 8,000 for wire transfers and HKD120,000 for other types of transactions. Where First Business Transactions becomes aware that these thresholds are met or exceeded, full CDD procedures are being applied.

In determining whether the transactions are in fact linked, First Business Transactions considers the following factors and the time frame within which the transactions are conducted:

- where several payments are made to the same recipient from one or more sources over a short period;
- where a customer regularly transfers funds to one or more destinations.

First Business Transactions identifies the customer and verifies the customer's identity by reference to documents, data or information provided by a reliable and independent source:

- a governmental body;
- the relevant authority;
- an authority in a place outside Hong Kong that performs functions similar to those of the relevant authority;
- any other reliable and independent source that is recognised by the relevant authority.

Identification and Verification of a Beneficial Owner
A beneficial owner is normally an individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. First Business Transactions verifies the identity of beneficial owner(s) owning or controlling 25% or more of the voting rights or shares of the legal entity, taking reasonable measures based on ML/ TF risks, so that First Business Transactions knows who the beneficial owner(s) is.
When an individual is identified as a beneficial owner, First Business Transactions obtains the following identification information:

- full name
- date of birth
- nationality
- identity document type and number

First Business Transactions obtains the residential address (and permanent address if different) of the beneficial owners and adopts a risk-based approach to determine the need to verify the address, taking in account the number of beneficial owners, the nature and distribution of the interests in the entity and the nature and extent of any business, contractual or family relationship.

Identification and Verification of a Person who Purports to Act on Behalf of the Customer
If a person purports to act on behalf of the customer, First Business Transactions:

- identifies the person and takes reasonable measures to verify the person's identity on the basis of documents, data or information provided by-
  i) a governmental body;
  ii) the relevant authority or any other relevant authority;
  iii) an authority in a place outside Hong Kong that performs functions similar to those of the relevant authority or any other relevant authority; or
  iv) any other reliable and independent source that is recognised by the relevant authority; and
- verifies the person's authority to act on behalf of the customer.

In general, First Business Transactions identifies and verifies the identity of those authorized to give instructions for the movement of funds or assets.

First Business Transactions obtains written authority in order to verify that the individual purporting to represent the customer is authorised to do so.

Purpose and Intended Nature of Business Relationship
Unless the purpose and intended nature are obvious, First Business Transactions obtains satisfactory information from all new customers as to the intended purpose and reason for opening the account or establishing the business relationship, and records the information on the account opening documentation.

Depending on the First Business Transactions risk assessment of the situation, information required may include:
- nature and details of the business/occupation/employment;

- the anticipated level and nature of the activity that is to be undertaken through the relationship (e.g. what the typical transactions are likely to be);
- location of customer;
- the expected source and origin of the funds to be used in the relationship;
- initial and ongoing source(s) of wealth or income.

Timing of Identification and Verification of Identity

First Business Transactions completes the CDD process before establishing any business relationship or before carrying out a specified occasional transaction.

Customer identification information (and information on any beneficial owners) and information about the purpose and intended nature of the business relationship shall be obtained before the business relationship is entered into.

Where First Business Transactions is unable to comply with relevant CDD requirements and the ongoing due diligence requirements, it must not establish a business relationship or carry out any occasional transaction with that customer, or must terminate business relationship as soon as reasonably practicable (where applicable), and where there is relevant knowledge or suspicion, should make an STR to the JFIU.

All the results of customer due diligence are fixed in First Business Transactions's AML Report. In case of a dispute regarding the onboarding of the new customer the issue is a subject to discussion by AML commission, that consists of First Business Transactions's top management representatives. The collective decision of the commission is final.

Keeping Customer's Information Up-to-Date

First Business Transactions takes steps from time to time to ensure that the customer information that has been obtained is up- to-date and relevant. To achieve this, First Business Transactions undertakes periodic reviews of existing records of customers.

An appropriate time to do so is upon certain trigger events such as:

- when a significant transaction (not only of a big amount, but also unusual) is to take place;
- when a material change occurs in the way the customer's account is operated;
- when the customer's documentation standards change substantially;
- when First Business Transactions is aware that it lacks sufficient information about the customer concerned.

Chapter 4. KNOW YOUR CUSTOMER / CUSTOMER ON-BOARDING

Identification and verification of natural persons

• full name

• date of birth

• nationality

• identity document type and number.

HK residents		Non-residents	
Permanent	Non-permanent	Physically present in HK	Not physically present in HK
Name, date of birth, ID card No.	Name, date of birth, nationality, travel document No. and type	Name, date of birth, nationality, travel document No. and type	Name, date of birth, nationality, travel document No. and type
• HK ID card	• valid travel document with photograph • a relevant national (i.e. government or state-issued) identity card bearing the individual's photograph • any government or state-issued document which certifies nationality	• valid travel document with photograph	• a valid travel document; • a relevant national (i.e. government or state-issued) identity card bearing the individual's photograph; • a valid national driving license bearing the individual's photograph; or • any applicable alternatives mentioned.

• Permanent Resident Identity Card of Macau Special Administrative Region;

• Mainland Travel Permit for Taiwan Residents;

•Seaman's Identity Document (issued under and in accordance with the International Labour Organisation Convention/Seafarers Identity Document Convention 1958);

• Taiwan Travel Permit for Mainland Residents;

• Permit for residents of Macau issued by Director of Immigration;

• Exit-entry Permit for Travelling to and from Hong Kong and Macau for Official Purposes;

• Exit-entry Permit for Travelling to and from Hong Kong and Macau.

Unacceptable forms of identification for completing a transaction:

• Any expired identification

• Birth Certificate

• Club or Association Card

• Marriage License

• Library Card

• Letters of Introduction

• Fishing or Hunting Licenses

• Business Card

• ATM Card

• Bank ID Card

• Insurance Policy or Card

Address identification and verification

First Business Transactions verifies the residential address (and permanent address if different) of a direct customer with whom it establishes a business relationship.

Methods for verifying residential addresses may include obtaining:

• a recent utility bill issued within the last 3 months;

• recent correspondence from a Government department or agency (i.e. issued within the last 3 months);

• a statement, issued by an authorized institution, a licensed corporation or an authorized insurer within the last 3 months;

• a record of a visit to the residential address by BancServices representatives;

• an acknowledgement of receipt duly signed by the customer in response to a letter sent by BancServices to the address provided by the customer;

• a letter from an immediate family member at which the individual resides confirming that the applicant lives at that address in Hong Kong, setting out the relationship between the applicant and the immediate family member, together with evidence that the immediate family member resides at the same address (for persons such as students and housewives who are unable to provide proof of address of their own name);

• mobile phone or pay TV statement (sent to the address provided by the customer) issued within the last 3 months;

• a letter from a Hong Kong nursing or residential home for the elderly or disabled, which BancServices is satisfied that it can place reliance on, confirming the residence of the applicant;

• a letter from a Hong Kong university or college, which BancServices is satisfied that it can place reliance on, that confirms residence at a stated address;

• a Hong Kong tenancy agreement which has been duly stamped by the Inland Revenue Department;

• a current Hong Kong domestic helper employment contract stamped by an appropriate Consulate (the name of the employer should correspond with the applicant's visa endorsement in their passport);

• a letter from a Hong Kong employer together with proof of employment, which BancServices is satisfied that it can place reliance on and that confirms residence at a stated address in Hong Kong;

• a lawyer's confirmation of property purchase, or legal document recognising title to property;

• for non-Hong Kong residents, a government-issued photographic driving license or national identity card containing the current residential address or bank statements issued by a bank in an equivalent jurisdiction where BancServices is satisfied that the address has been verified.

Identification of a Legal Entity

With respect to legal entities, First Business Transactions pays special attention when looking behind the customer to identity those who have ultimate control or ultimate beneficial ownership over the business and the customer's assets. Verifying the identity of the beneficial owner(s) is being carried out using reasonable measures based on a risk-based approach. For a customer other than a natural person, First Business Transactions ensures that it fully understands the customer's legal form, structure and ownership, and additionally obtains information on the nature of its business, and the reasons for seeking the product or service unless the reasons are obvious.

First Business Transactions conducts reviews from time to time to ensure the customer information held is up-to-date and relevant; methods by which a review could be conducted include conducting company searches, seeking copies of resolutions appointing directors, noting the resignation of directors, or by other appropriate means.

First Business Transactions obtains and verifies the following information in relation to a customer which is a legal entity:

- full name
- date and place of incorporation
- registration or incorporation number
- registered office address in the place of incorporation
- web-site requirements

  i) Cross-reference of the web-site and the Company (Merchant's web-site as well as their Terms & Conditions (User Agreement) are to contain the following information about the Company: address, register number, license (if applicable).
  ii) Terms & Conditions (User Agreement),
  iii) Payment&Refund Policy
  iv) Privacy Policy

If the business address of the customer is different from the registered office address in the place of incorporation, First Business Transactions obtains information on the business address and verifies it.

In the course of verifying the customer's identity, First Business Transactions obtains the following data and documents:

- a copy of the certificate of incorporation and business registration (where applicable);
- a copy of the company's memorandum and articles of association which evidence the powers that regulate and bind the company;
- details of the ownership and structure control of the company, e.g. an ownership chart;
- the names of all directors.

First Business Transactions shall also:

- confirm the company is still registered and has not been dissolved, wound up, suspended or struck off;
- independently identify and verify the names of the directors and shareholders recorded in the company registry in the place of incorporation;

- verifiy the company's registered office address in the place of incorporation.

First Business Transactions verifies the above mentioned information from:

For a locally incorporated company:
• a search of file at the Hong Kong Company Registry and obtains a company report.

For a company incorporated overseas:
- a similar company search enquiry of the registry in the place of incorporation and obtains a company report;
- a certificate of incumbency or equivalent issued by the company's registered agent in the place of
  incorporation; or
- a similar or comparable document to a company search report or a certificate of incumbency certified by a professional third party in the relevant jurisdiction.

With respect to aforementioned, First Business Transactions accepts:
- a true copy of a company search report certified by a company registry or professional third party, and issued within the last 6 months;
- a true copy of a certificate of incumbency certified by a professional third party, and issued within the last 6 months.

First Business Transactions does not accept documents which have been self-certified by the customer.

Beneficial Owners

First Business Transactions identifies and records the identity of all beneficial owners, and takes reasonable measures to verify the identity of:
- all shareholders holding 25% of the voting rights or share capital (the threshold shall be lowered to 10% for each high-risk relationship);
- any individual who exercises ultimate control over the management of the corporation;
- any person on whose behalf the customer is acting.

For companies with multiple layers in their ownership structures, First Business Transactions takes measures to ensure that it has an understanding of the ownership and control structure of the company.

The intermediate layers of the company are being fully identified. For this purpose, First Business Transactions obtains a director's declaration incorporating or annexing an ownership chart describing the intermediate layers. The minimum information to be provided includes:

- company name;
- place of incorporation;
- the rationale behind the particular structure employed (where applicable)

Screening Process

Screening constitutes an essential stage of onboarding process and an ongoing monitoring.
Customers and transactions are screened against:

- Sanctions lists
- PEPs lists
- Adverse media

Screening tools used by First Business Transactions:
https://namescan.io/
http://www.fedsfm.ru/documents/terrorists-catalog-portal-act
http://www.fedsfm.ru/documents/terrorists-catalog-portal-act

Partnerships and Unincorporated Bodies

Partnerships and unincorporated bodies, although principally operated by individuals or groups of individuals, are different from individuals, in that there is an underlying business.
The beneficial owner, in relation to a partnership is an individual who:

- is entitled to or controls, directly or indirectly, more than 25% share of the capital or profits of the partnership (the threshold shall be lowered to 10% for each high-risk relationship);
- is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights in the partnership (the threshold shall be lowered to 10% for each high-risk relationship);
- exercises ultimate control over the management of the partnership;
- if the partnership is acting on behalf of another person, means the other person.

The beneficial owner, in relation to an unincorporated body is:

- an individual who ultimately owns or controls the unincorporated body;
- if the unincorporated body is acting on behalf of another person, means the other person.

In relation to the partnership or unincorporated body First Business Transactions obtains:

- the full name;
- the business address;
- the names of all partners and individuals who exercise control over the management of the partnership or unincorporated body, and names of individuals who own or control more than 25% of its capital or profits, or of its voting rights.

In cases where a partnership arrangement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained.
Where partnerships or unincorporated bodies are well-known, reputable organisations, with long histories in their industries, and with substantial public information about them, their partners and controllers, confirmation of the customer's membership of a relevant professional or trade association is likely to be sufficient to provide such reliable and independent evidence of the identity of the customer.

Other partnerships and unincorporated bodies have a lower profile, and generally comprise a much smaller number of partners and controllers. In verifying the identity of such customers, First Business Transactions primarily has regard to the number of partners and controllers. Where these are relatively few, the customer should be treated as a collection of individuals; where numbers are larger, First Business Transactions should decide whether it should continue to regard the customer as a collection of individuals, or whether it can be satisfied with evidence of membership of a relevant professional or trade association.
In either case, First Business Transactions obtains the partnership deed (or other evidence in the case of sole traders or other unincorporated bodies), to satisfy itself that the entity exists, unless an entry in an appropriate national register may be checked.

In the case of associations, clubs, societies, charities, religious bodies, institutes, mutual and friendly societies, co- operative and provident societies, First Business Transactions obtains the evidence of the legitimate purpose of the organisation, e.g. by requesting sight of the constitution.

Trusts

A trust does not possess a separate legal personality. It cannot form business relationships or carry out occasional transactions itself. It is the trustee who enters into a business relationship or carries out occasional transactions on behalf of the trust and who is considered to be the customer (i.e. the trustee is acting on behalf of a third party – the trust and the individuals concerned with the trust).
The beneficial owner, in relation to a trust is:

- an individual who is entitled to a vested interest in more than 25% of the capital of the trust property, whether the interest is in possession or in remainder or reversion and whether it is defeasible or not (the threshold shall be lowered to 10% for each high-risk relationship);
- the settlor of the trust;
- a protector or enforcer of the trust;
- an individual who has ultimate control over the trust.

First Business Transactions collects the following identification information in respect of a trust on whose behalf the trustee (i.e. the customer) is acting:

- the name of the trust;
- date of establishment/settlement;
- the jurisdiction whose laws govern the arrangement, as set out in the trust instrument;
- the identification number (if any) granted by any applicable official bodies (e.g. tax identification number or registered charity or non-profit organization number);
- identification information of trustee(s) - in line with guidance for individuals or corporations;
- identification information of settlor(s) and any protector(s) or enforcers in line with the guidance for individuals/corporations;
- identification information of known beneficiaries. (Known beneficiaries mean those persons or that class of persons who can, from the terms of the trust instrument, be identified as having a reasonable expectation of benefiting from the trust capital or income)

First Business Transactions verifies the name and date of establishment of a trust and obtain s appropriate evidence to verify the existence, legal form and parties to it, i.e. trustee, settlor, protector, beneficiary, etc.

Reasonable measures to verify the existence, legal form and parties to a trust, having regard to the ML/TF risk, may include:

- reviewing a copy of the trust instrument and retaining a redacted copy;
- by reference to an appropriate register in the relevant country of establishment;
- a written confirmation from a trustee acting in a professional capacity;
- a written confirmation from a lawyer who has reviewed the relevant instrument;for trusts that are managed by the trust companies which are subsidiaries (or affiliate companies) of First Business Transactions, that First Business Transactions may rely on a written confirmation from its trust subsidiaries (or trust affiliate companies).

For the avoidance of doubt, First Business Transactions takes reasonable measures to verify the actual identity of the individual parties (i.e. trustee, settlor, protector, beneficiary, etc.).

First Business Transactions takes particular care in relation to trusts created in jurisdictions with no money laundering legislation similar to Hong Kong.

Chapter 5. SIMPLIFIED CUSTOMER DUE DILIGENCE (SDD)

SDD foresees that application of full CDD measures is not required, which means that First Business Transactions is not required to identify and verify the beneficial owner. However, other aspects of CDD must be undertaken and it is still necessary to conduct ongoing monitoring of the business relationship. First Business Transactions needs to have reasonable grounds to support the use of SDD in each particular case.

SDD measures shall not be applied if:

- First Business Transactions suspects that the customer, the customer's account or the transaction is involved in ML/TF;
- First Business Transactions doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or verifying the customer's identity.

SDD may be applied to:

- a financial institution as defined in the AMLO;
- an institution that:
  i) is incorporated or established in an equivalent jurisdiction as First Business Transactions;
  ii) carries on a business similar to that carried on by First Business Transactions;
  iii) is established in AML equivalent jurisdiction;
- a corporation listed on any stock exchange ("listed company");
- an investment vehicle where the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle is:
  i) a financial institution;
  ii) an institution incorporated or established in Hong Kong, or in an AML equivalent jurisdiction;
- the Government or any public body in Hong Kong;
- the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions
  similar to those of a public body.

First Business Transactions shall still identify and take reasonable measures to verify the identity of beneficial owners in the ownership chain that are not connected with that entity.

For avoidance of doubt, First Business Transactions:

- identifies the customer and verifies the customer's identity – if a business relationship is to be established and its purpose and intended nature are not obvious, obtains information on the purpose and intended nature of the business relationship with First Business Transactions;
- if a person purports to act on behalf of the customer – identifies the person and takes reasonable measures to verify the person's identity and verify the person's authority to act on behalf of the customer.

Listed Companies

First Business Transactions performs SDD in respect of a corporate customer listed on a stock exchange. This means First Business Transactions need not to identify the beneficial owners of the listed company cases, it will be generally sufficient to obtain proof of listed status on a stock exchange.

Government and Public Body

First Business Transactions may apply SDD to a customer that is the Hong Kong government, any public bodies in Hong Kong, the government of an equivalent jurisdiction or a body in an equivalent

jurisdiction that performs functions similar to those of a public body.

Public body includes:

- any executive, legislative, municipal or urban council;
- any Government department or undertaking;
- any local or public authority or undertaking;
- any board, commission, committee or other body, whether paid or unpaid, appointed by the Chief Executive or the Government;
- any board, commission, committee or other body that has power to act in a public capacity under or for the purposes of any enactment.

Chapter 6. ENHANCED CUSTOMER DUE DILIGENCE (EDD)

First Business Transactions applies an Enhance Due Diligence where the customer and product/service combination is considered to be a greater risk. This higher level of due diligence is required to mitigate the increased risk. A high risk situation generally occurs where there is an increased opportunity from money laundering or terrorist financing through the service and product First Business Transactions provides or from a customer of First Business Transactions.
What the enhanced due diligence actually entails will be dependant on the nature and severity of the risk.

High-Risk Situations

In any situation that by its nature presents a higher risk of ML/TF, First Business Transactions takes additional measures to mitigate the risk of ML/TF.

Additional measures or EDD may include:

- obtaining additional information on the customer (e.g. connected parties, accounts or relationships) and updating more regularly the customer profile including the identification data;
- obtaining additional information on the intended nature of the business relationship (e.g. anticipated account activity), the source of wealth and source of funds;
- obtaining the approval of senior management to commence or continue the relationship; and
- conducting enhanced monitoring of the business relationship, by increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination.

Customers not Physically Present for Identification Purposes

First Business Transactions applies equally effective customer identification procedures and ongoing monitoring standards for customers not physically present for identification purposes as for those where the customer is available for interview. Nevertheless, the face-to-face meeting can take place outside Hong Kong as well. Alternatively, First Business Transactionss streams online interview of the client.

If a customer has not been physically present for identification purposes, First Business Transactions takes the following measures to mitigate the risks posed:

- obtains additional information on the customer;
- obtains additional information on the intended nature of the business relationship;
- obtains information on the source of funds or source of wealth of the customer;
- obtains information about the reasons for the intended or performed transactions;
- obtains approval from senior management for establishing / continuing the relationship;
- conducts enhanced monitoring of the relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further explanation;
- requires first payment to be carried out through an account in the customer’s name with a bank subject to similar CDD standards.

First Business Transactions accepts copies of documents that have been certified by a suitable certifier. Use of an independent suitable certifier 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. The certifier must sign and date the copy document (printing his/her name clearly in capitals underneath) and clearly indicate his/her position or capacity on it. The certifier must state that it is a true copy of the original (or words to similar effect).

In course of conducting EDD measures, First Business Transactions also takes into consideration all relevant adverse information. Whether an official document or something posted publicly on the Internet, any information that pertains to money laundering or corruption is thoroughly considered. When clients or transactions are large enough to warrant EDD, there is no room for leniency and no risks should be taken.

Bearer shares

Bearer shares are an equity security that is wholly owned by whoever holds the physical stock certificate. The issuing corporate does not register the owner of the stock or track transfers of ownership. Transferring the ownership of the stock involves only delivering the physical document. Bearer shares therefore lack the regulation and control of common shares because ownership is never recorded. Due to the higher ML/TF risks associated with bearer shares the FATF requires countries that have legal persons able to issue bearer shares should take appropriate measures to ensure that they are not misused for money laundering.

First Business Transactions takes additional measures in case of possible cooperation with companies with bearer shares capital, as it is often difficult to identify the beneficial owner(s). First Business Transactions adopts procedures to establish the identities of the holders and beneficial owners of such shares and ensures that it is notified whenever there is a change of holder or beneficial owner.

Where bearer shares have been deposited with an authorized/registered custodian, First Business Transactions seeks an independent evidence of this, for example:

- confirmation from the registered agent that an authorized/registered custodian holds the bearer shares;
- the identity of the authorized/registered custodian;
- the name and address of the person who has the right to those entitlements carried by the share.

As part of an ongoing periodic review, First Business Transactions obtains evidence to confirm the authorized/registered custodian of the bearer shares.

Where the shares are not deposited with an authorized/registered custodian, First Business Transactions:

- obtains declarations prior to account opening and annually thereafter from each beneficial owner of such shares;
- requires the customer to notify it immediately of any changes in the ownership of the shares.

Politically Exposed Persons (PEPs)

Foreign PEPs

- an individual who is or has been entrusted with a prominent public function in a place outside the People's Republic of China and 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;
- a spouse, a partner, a child or a parent of an individual falling within paragraph above, or a spouse or a partner of a child of such an individual;
- a close associate of an individual falling within paragraph above.

A PEP's close associate is:

- an individual who has close business relations with a person falling under the definition of PEP, including an individual who is a beneficial owner of a legal person or trust;

- 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 the definition of PEP.

In order to reduce possible risks First Business Transactions conducts EDD at the outset of the business relationship and ongoing monitoring where it knows or suspects that it has business relationship with a PEP.

For that purpose First Business Transactions:
- makes reference to publicly available information;
- screens against commercially available databases for determining whether a customer or a beneficial owner of a customer is a PEP;
- uses publicly available information or refer to relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations to assess which countries are most vulnerable to corruption.

In relation to PEPs, First Business Transactions applies the following EDD measures:
- obtaining approval from First Business Transactions' senior management;
- taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds;
- applying enhanced monitoring to the relationship in accordance with the assessed risks.

Domestic PEPs
A domestic PEP is defined as:
- an individual who is or has been entrusted with a prominent public function in a place within the People's Republic of China and 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;
- a spouse, a partner, a child or a parent of an individual falling within paragraph above, or a spouse or a partner of a child of such an individual;
- a close associate of an individual falling within paragraph above.

If an individual is known to be a domestic PEP, First Business Transactions performs a risk assessment to determine whether the individual poses a higher risk of ML/TF. Domestic PEPs status in itself does not automatically confer higher risk. In any PEP related situation that First Business Transactions assess to present a higher risk of ML/TF, it applies EDD measures.

Foreign PEPs and domestic PEPs which have been assessed to present a higher risk, are subject to a minimum annual review. First Business Transactions reviews CDD information to ensure that it remains up-to-date and relevant.

Source of Wealth vs Source of Funds

Establishing the customer's source of wealth or source of funds is a core requirement of EDD.

Source of wealth refers to the origin of an individual's entire body of wealth (i.e. total assets). This information will usually give an indication as to the size of wealth the customer would be expected to have, and a picture of how the individual acquired such wealth. Although First Business Transactions may not have specific information about assets not deposited with or processed by it, it may be possible to gather general information from the individual, commercial databases or other open sources.

Source of funds refers to the origin of the particular funds or other assets which are the subject of the business relationship between an individual and First Business Transactions (e.g. the amounts being invested, deposited, or wired as part of the business relationship). Source of funds information should not simply be limited to knowing from which the funds may have been transferred, but also the activity that generates the funds. The information obtained should be substantive and establish a provenance or reason for the funds having been acquired.

First Business Transactions collects information relating to the source of wealth or source of funds of its customers and, according to the level of risk involved, takes reasonable steps to verify that information.
The types of data and documents that can be used for verification will vary depending on the circumstances and the information that the customer provides to First Business Transactions.

The following documents, data, or information could be considered reliable and independent:

- government-issued or registered documents or data;
- full bank and other investment statements;
- full payslip or wage slip or other documents confirming salary;
- inheritance (stamped grant of probate, stamped grant of letters of administration);
- audited financial accounts from a chartered accountant or Charities Services;
- letter from an agent of the customer confirming they have knowledge of and established business relationships with the customer;
- a copy of a will;
- sales and purchase agreements.

For customers who conduct their business with First Business Transactions there is a range of documents that First Business Transactions can use to verify how funds have been acquired.

High-risk jurisdictions

- Countries-subject to OFAC sanctions;
- Countries identified as supporting international terrorism;
- Jurisdictions, determined to be of primary money laundering concern and subject to special measures;
- Offshore financial centres;
- Jurisdictions with deficiencies in combating money laundering and terrorist financing identified by FATF.

First Business Transactions gives particular attention to, and exercises extra care in respect of:

- business relationships and transactions with persons (including legal persons and other financial institutions) from or in jurisdictions that do not or insufficiently apply the FATF Recommendations;
- transactions and business connected with jurisdictions assessed as higher risk.

The Financial Action Task Force (“FATF”) has published a list of countries/jurisdictions classified as being “non-cooperative in the international fight against money laundering”. The list may be modified and updated as needed. The FATF list is kept current by theCompliance officer/MLRO.

In addition to ascertaining and documenting the business rationale for establishing a relationship, First Business Transactions takes reasonable measures to establish the source of funds of such customers.

In determining which jurisdictions do not apply, or insufficiently apply the FATF Recommendations, or may otherwise pose a higher risk, First Business Transactions considers, among other things:

- circulars issued by relevant authorities (e.g. by HKCED);
- whether the jurisdiction is subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN);
- whether the jurisdiction is identified by credible sources as lacking appropriate AML/CTF laws, regulations and other measures;
- whether the jurisdiction is identified by credible sources as providing funding or support for terrorist activities and has designated terrorist organisations operating within it;
- whether the jurisdiction is identified by credible sources as having significant levels of corruption, or other criminal activity.

In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra- national or international bodies such as the International Monetary Fund, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-government organisations. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

First Business Transactions will make a reference to publicly available information or relevant reports and data bases on corruption risk, e.g. Transparency International Corruption Perceptions Index.

Money Transmitting Business

First Business Transactions will not do business with MSBs that are not appropriately licensed and registered. As part of the Account Opening Procedures, theCompliance officer/MLRO will conduct appropriate due diligence to identify those customers of the Company engaged in a money transmitting business, and verify that such customers are not engaged in unlicensed money transmitting business. The Compliance officer/MLRO will maintain a file to alert the Company when licenses/registrations are due to be renewed. This file will be facilitated by the system that will automatically flag dates. Sixty (60) days prior to the expiration date of an MSB registration or license, the Compliance Department will send the MSB a request for proof of appropriate registration or license renewal.

MSBs' AML/CTF Policies and Procedures

All entities offering money services will be required to have appropriate AML Compliance Programs with written AML/CTF procedures. Before approving a new relationship, First Business Transactions will document and review for effectiveness, the MSB’s AML compliance procedures.

Chapter 7. ON-GOING MONITORING

Effective ongoing monitoring is vital for understanding of customers' activities and an integral part of effective AML/CTF systems.

First Business Transactions continuously monitors its business relationship with a customer by:

- reviewing from time to time web-site, documents, data and information relating to the customer and obtained for the purposes of customer's identification and verification to ensure that they are up-to-date and relevant;
- monitoring the activities of the customer to ensure that they are consistent with the nature of business, the risk profile and source of funds. An unusual transaction may be in the form of activity that is inconsistent with the expected pattern for that customer, or with the normal business activities for the type of product or service that is being delivered;
- identifying transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose and which may indicate ML/TF.

Risk-Based Approach to Monitoring

The extent of monitoring is linked to the risk profile of the customer which has been determined through the risk assessment procedures. First Business Transactions takes additional measures when monitoring business relationships that pose a higher risk. High-risk relationships, for example those involving PEPs, will require more frequent and intensive monitoring.

First Business Transactions conducts an on-going monitoring on a risk-based approach and considers:

- the nature and type of transactions (e.g. abnormal size or frequency);
- the nature of a series of transactions (e.g. a number of cash deposits);
- the amount of any transactions, paying particular attention to particularly substantial transactions;
- the geographical origin/destination of a payment or receipt;
- the customer's normal activity or turnover.

First Business Transactions is vigilant for changes on the basis of the business relationship with the customer over time, which may include:

- new products or services that pose higher risk are entered into;
- new corporate or trust structures are created;
- the stated activity or turnover of a customer changes or increases;
- the nature of transactions changes or their volume or size increases etc.

Where the basis of the business relationship changes significantly, First Business Transactions carries out further CDD procedures to ensure that the ML/TF risk involved and basis of the relationship are fully understood. Ongoing monitoring procedures take account of the above changes.

Methods and Procedures

When considering how best to monitor customer transactions and activities, First Business Transactions takes into account the following factors:

- the size and complexity of its business;
- its assessment of the ML/TF risks arising from its business;
- the nature of its systems and controls;
- the monitoring procedures that already exist to satisfy other business needs;
- the nature of the products and services (which includes the means of delivery or communication).

Where transactions that are complex, large or unusual, or patterns of transactions which have no apparent economic or lawful purpose are noted, First Business Transactions examines the background

and purpose, including where appropriate, the circumstances of the transactions. The findings and outcomes of these examinations shall be properly documented in writing and be available to assist the relevant authorities, other competent authorities and auditors.

First Business Transactions takes the four steps systemic approach to suspicious activity identification:

Screening
The recognition of an indicator of suspicious activity is the first step in the suspicious activity identification system.
The following are some of the suspicious activity indicators most commonly associated with money laundering in Hong Kong.

1. Large or frequent cash transaction, either deposits or withdrawals.
2. Suspicious activity based on transaction pattern, i.e.
   - account used as a temporary repository for funds;
   - a period of significantly increased activity amid relatively dormant periods;
   - “structuring" or "smurfing" i.e. many lower value transactions conducted when one, or a few, large transactions could be used;"
   - U-turn" transactions, i.e. money passes from one person or company to another, and then back to the original person or company;
   - increased level of account activity on the first banking day after Hong Kong horse racing, normally Mondays and Thursdays, indicating illegal bookmaking;
3. Involvement of one or more of the following entities which are commonly involved in money laundering:
   - shelf or shell companies;
   - company registered in a known "tax haven" or “off-shore” financial centre;
   - company formation agent, or secretarial company, as the authorized signatory of the bank account;
   - money service operator;
   - casino.
4. Currencies, countries or national of countries, commonly associated with international crime or drug trafficking or identified as having serious deficiencies in their anti-money laundering regimes;
5. Customer refuses, or is unwilling, to provide explanation of financial activity, or provides explanation assessed to be untrue;
6. Activity is incommensurate with that expected from the customer considering the information already known to you about the customer and the customers previous financial activity.
7. Countries or nationals of countries, commonly associated with terrorist activities or the persons or organizations designated as terrorists or their associates. International and Politically Exposed Persons (PEPs)

Asking
In case a transaction or transactions of a customer bear one or more suspicious activity indicators, First Business Transactions shall ask the customer questions on the reason for conducting the transaction and the identity of the source and ultimate beneficiary of the money being transacted. First Business Transactions also consider s whether the customer's story amounts to a reasonable and

legitimate explanation of the activity observed. If not, then the customer's activity is regarded to be suspicious and a suspicious transaction report should be made to JFIU.

Finding out
Appropriate questions to ask in order to obtain an explanation of the reason for conducting a transaction bearing suspicious activity indicators will depend upon the circumstances of the financial activity observed. For example, when a customer receives "structured" remittances from overseas. First Business Transactions can question the customer on the reason for receiving numerous remittances within a short period of time on the grounds that one larger remittance would be quicker, cheaper for the sender to send, and less time consuming for the recipient to handle.
Persons engaged in legitimate business generally have no objection to, or hesitation in answering such questions. Persons involved in illegal activity are more likely to refuse to answer, give only a partial explanation or give an explanation which is unlikely to be true.
If a customer is unwilling, or refuses, to answer questions or gives replies which First Business Transactions suspects are incorrect or untrue, this may be taken as a further indication of the suspicious nature of the financial activity.

Evaluating
The final step in the suspicious activity identification system is the decision whether or not to make an suspicious transaction report (STR). Due to the fact that suspicion is difficult to quantify, it is not possible to give exact guidelines on the circumstances in which an STR should, or should not, be made. However, such a decision will be of the highest quality when all the relevant circumstances are known to, and considered by, the decision maker, i.e. when all three of the preceding steps in the suspicious transaction identification system have been completed and are considered. If, having considered all the circumstances, First Business Transactions finds the activity genuinely suspicious then an STR should be made.

Black List Procedures
A Black List is the method by which the company restricts transactions to known, suspected or representative advised individuals, business or others who may be conducting activities that are believed to be illegal, suspicious, etc. First Business Transactions has established the Black List as a method to further reduce the probability of remitting to criminal elements beyond sanctions lists (OFAC, UN, EU etc).

Determination has to be made and articulated before a client can be placed in the Black List. Common Reasons for inclusion:

- suspect illegal activities;
- providing false IDs or other documents required for the purposes of customer’s identification and verification;
- exclude someone as not being the person on OFAC, etc.

Black List shall be administered by the Compliance Officer/MLRO. Additions/deletions to the Black List shall be done solely by the Compliance Officer/MLRO or his/her designee. As a general rule, if a STR is filed on a customer, so too will they be added to the Black List.

Chapter 8. SANCTIONS POLICIES

With a view to ensure that there are no payments to or from a person on a sanctions list issued by an overseas jurisdiction, First Business Transactions conducts screening against lists of FATF not-compliant countries, in addition to the lists of sanctioned countries, entities and persons.

First Business Transactions takes measures to thoroughly screen its customers and gather as much information as possible about them and their accounts. This helps to ensure that the customers are not involved in financial crimes.

Many transactions that are completed in order to send money to terrorist organisations are small and innocuous. Terrorist financiers purposefully do not send large amounts of money at once, as they wish to avoid the attention of both governments and financial institutions. Additionally, individuals who finance terrorism also use trade-based money laundering schemes in order to get their money across borders. This is becoming much more common, and it is a difficult problem to track down.

First Business Transactions takes measures to ensure compliance with the relevant regulations and legislation on terrorist financing. It is particularly vital that First Business Transactions is able to identify and report transactions with terrorist suspects and designated parties.

First Business Transactions maintains a database of names and particulars of terrorist suspects and designated parties which consolidates the various lists that have been made known to it. Alternatively, First Business Transactions makes arrangements to access to such a database maintained by third party service providers.

First Business Transactions screens customers and transactions against following lists:

- Consolidated United Nations Security Council Sanctions List
- OFAC Specially Designated Nationals And Blocked Persons List (SDN)
- Other OFAC sanctions lists
- EEAS-consolidated list of persons, groups and entities subject to EU financial sanctions.

To avoid establishing business relationship or conducting transactions with any terrorist suspects and possible designated parties, First Business Transactions implements an effective screening mechanism, which includes:

- screening its customers and any beneficial owners of the customers against current database at the establishment of the relationship;
- screening its customers and any beneficial owners of the customers against all new and any updated designations to the database as soon as practicable;
- screening all relevant parties in a cross-border wire transfer against current database before executing the transfer.

When possible name matches are identified during screening, First Business Transactions conducts enhanced checks to determine whether the possible matches are genuine hits. In case of any suspicions of TF, PF or sanctions violations, First Business Transactions will make a report to the JFIU. Records of enhanced checking results, together with all screening records, should be documented, or recorded electronically.

If First Business Transactions suspects that a transaction is terrorist-related, it should make a report to the JFIU. Even if there is no evidence of a direct terrorist connection, the transaction should still be reported to the JFIU if it looks suspicious for other reasons, as it may emerge subsequently that there is a terrorist link.

UNATMO is an ordinance to further implement a decision under UNSCR 1373 (2001) relating to measures for prevention of terrorist acts and a decision under UNSCR 2178 (2014) relating to the prevention of travel for the purpose of terrorist acts or terrorist training; as well as to implement certain terrorism-related multilateral conventions and certain FATF Recommendations. All UN member states are required to freeze any funds, or other financial assets, or economic resources of any person(s) named in these lists and to report any suspected name matches to the relevant authorities.
Where a person or property is designated by a Committee of the UNSC as a terrorist/terrorist associate or terrorist property respectively, the Chief Executive may publish a notice in the Gazette specifying the name of the person or the property. Besides, the Chief Executive may make an application to the Court of First Instance for an order to specify a person or property as a terrorist/terrorist associate or terrorist property respectively, and if the order is made, it will also be published in the Gazette.

A number of provisions in the UNATMO are of particular relevance to First Business Transactions, and are listed below:

- section 6 empowers the Secretary for Security (S for S) to freeze suspected terrorist property;
- section 7 prohibits the provision or collection of property for use to commit terrorist acts;
- section 8 prohibits any person from making available or collecting or soliciting property or financial (or related) services for terrorists and terrorist associates;
- section 8A prohibits any person from dealing with any property knowing that, or being reckless as to whether, the property is specified terrorist property or property of a specified terrorist or terrorist associate;
- section 11L prohibits any person from providing or collecting any property to finance the travel of a person between states with the intention or knowing that the travel will be for a specified purpose, i.e. the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs); or the provision or receiving of training that is in connection with the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs as a result of the training).

The Secretary for Security can licence exceptions to the prohibitions to enable frozen property to be unfrozen and to allow payments to be made to or for the benefit of a designated party under the UNATMO (e.g. reasonable living/ legal expenses and payments liable to be made under the Employment Ordinance). For seeking such a licence First Business Transactions should write to the Security Bureau.

The UNSO empowers the Chief Executive to make regulations to implement sanctions decided by the UNSC, including targeted financial sanctions 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. For seeking such a licence First Business Transactions should write to the Commerce and Economic Development Bureau.

The counter proliferation (PF) 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.

First Business Transactions, being an MSO operating internationally is aware of the scope and focus of relevant sanctions regimes in those jurisdictions. Where these sanctions regimes may affect its operations, First Business Transactions considers what implications exist for its procedures and takes appropriate measures, such as including relevant overseas designations in its database for screening purpose, where applicable.

OFAC Compliance

It is the policy of First Business Transactions to comply with all OFAC requirements and directives that restrict providing services, conducting business with, maintaining accounts for, or handling transactions or monetary transfers for foreign countries or foreign nationals listed on the Office of Foreign Assets Control (OFAC) list of Specially Designated Nationals (SDNs) and Blocked Entities.

First Business Transactions shall not open a relationship for, handle a transaction or monetary transfer for, or do business with any person, government or other entity on the OFAC list of Specially Designated Nationals and Blocked Entities. Through screening and monitoring, the Company will identify such customers or transactions, and if it is found, contact OFAC immediately and all directives as to rejecting, restricting, blocking or seizing will be followed.

As per new relationship opening procedure, no new relationship will be established without passing through the steps indicated and obtain the necessary approvals. As part of the relationship opening procedure, the Compliance Department will check the names of all, business owners, and authorized signers against OFAC's master list of "Specially Designated Nationals and Blocked Persons" (SDN list), and check the prospective customer's geographical location for embargoed countries and cities by putting the information through the system prior to opening the relationship.

The system will check names against the OFAC list and prior to approving the relationship. The system checks the entered name for matching spelling, close matches, name variations and phonetically. If the name of the prospective customer is a match or possible match to a name in the OFAC list, the system will displays the potential match, and maintain an electronic record of such a match to be included in the documentation.

The Company's staff is trained to recognize false positive matches and can continue with the transaction in the event a false positive match is displayed. The system will prompt the Compliance Staff to document the reason for the false positive, and will maintain that record in an electronic file. Any close matches that cannot be easily categorized as a false positive must be immediately brought to the attention of the Compliance Officer for validation.

First Business Transactions includes in its database:

- the lists published in the Gazette or on the website of the Commerce and Economic Development Bureau;
- the lists that the CCE draws to the attention of MSOs from time to time;
- any relevant designations by overseas authorities which may affect its operations.

- The database is a subject to timely update whenever there are changes.

Chapter 9. SUSPICIOUS TRANSACTIONS REPORTING

It is a statutory obligation under the DTROP and the OSCO, as well as the UNATMO, that where a person knows or suspects that any property:

- in whole or in part directly or indirectly represents any person's proceeds of was used in connection with, or is intended to be used in connection with drug trafficking or an indictable offence; or
- that any property is terrorist property, the person shall as soon as it is reasonable for him to do so, file an STR with the JFIU. The STR should be made together with any matter on which the knowledge or suspicion is based. Under the DTROP, the OSCO and the UNATMO, failure to report knowledge or suspicion carries a maximum penalty of imprisonment for three months and a fine of HKD 50,000.

First Business Transactions provides sufficient guidance to its staff to enable them to form suspicion or to recognise when ML/ TF is taking place, taking account of the nature of the transactions and instructions that staff is likely to encounter, the type of product or service and the means of delivery, i.e. whether face to face or remote. This will also enable staff to identify and assess the information that is relevant for judging whether a transaction or instruction is suspicious in the circumstances.

The key is knowing enough about the customer's business to recognise that a transaction, or a series of transactions, is unusual and, from an examination of the unusual, whether there is a suspicion of ML/TF. Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, etc., the transaction is considered as unusual and is put on alert.

Where First Business Transactions conducts enquiries and obtains what it considers to be a satisfactory explanation of the activity or transaction, it may conclude that there are no grounds for suspicion, and therefore take no further action. However, where First Business Transactions' enquiries do not provide a satisfactory explanation of the activity or transaction, it may conclude that there are grounds for suspicion, and must make a disclosure to JFIU.

The following examples of situations might give rise to suspicion in certain circumstances:

- transactions or instructions which have no apparent legitimate purpose and/or appear not to have a commercial rationale;
- transactions, instructions or activity that involve apparently unnecessary complexity or which do not constitute the most logical, convenient or secure way to do business;
- where the transaction being requested by the customer, without reasonable explanation, is out of the ordinary range of services normally requested, or is outside the experience of the financial services business in relation to the particular customer;
- where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that has previously emerged; where the customer refuses to provide the information requested without reasonable explanation or who otherwise refuses to cooperate with the CDD and/or ongoing monitoring process;
- where a customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation;
- the extensive use of trusts or offshore structures in circumstances where the customer's needs are inconsistent with the use of such services;
- transfers to and from high risk jurisdictions without reasonable explanation, which are not consistent with the customer's declared business dealings or interests;
- unnecessary routing of funds or other property from/to third parties or through third party accounts.

Timing and Manner of Reporting

When First Business Transactions knows or suspects that property represents the proceeds of crime or terrorist property, a disclosure must be made to the JFIU as soon as it is reasonable to do so. Dependent on when knowledge or suspicion arises, disclosures may be made either before a suspicious transaction or activity occurs (whether the intended transaction ultimately takes place or not), or after a transaction or activity has been completed.

The disclosure shall be made together with any matter on which the knowledge or suspicion is based. Once knowledge or suspicion has been formed, First Business Transactions should:

- file an STR even where no transaction has been conducted by or through First Business Transactions;
- the STR must be made as soon as reasonably practical after the suspicion was first identified.

Tipping-Off

It is an offence ("tipping off") to reveal to any person any information which might prejudice an investigation; if a customer is told that a report has been made, this would prejudice the investigation and an offence would be committed. The tipping-off provision includes circumstances where a suspicion has been raised internally within the company, but has not yet been reported to the JFIU.

The need for prompt disclosures is especially important in cases where the customer instructed First Business Transactions:

- to move funds or other property;
- to close the account;
- to make cash available for collection;
- to carry out significant changes to the business relationship.

In such circumstances, First Business Transactions contacts the JFIU urgently.
In the event that an urgent reporting is required (e.g. where a customer has instructed First Business Transactions to move funds or other property, close the account, make cash available for collection, or carry out significant changes to the business relationship etc.), particularly when the account is part of an ongoing investigation by law enforcement agency, First Business Transactions should indicate this in the STR. Where exceptional circumstances exist in relation to an urgent reporting, an initial notification by telephone to the JFIU should be considered.

The JFIU will acknowledge receipt of an STR made by First Business Transactions. 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 company to operate the account under the provisions of both the DTROP and the OSCO, and the UNATMO. If a no-consent letter is issued, First Business Transactions should act according to the contents of the letter and seek legal advice where necessary.

Filing an STR to the JFIU provides First Business Transactions with a statutory defence to the offence of ML/TF in respect of the acts disclosed in the report, provided:

- the report is made before First Business Transactions undertakes the disclosed acts and the acts (transaction(s)) are undertaken with the consent of the JFIU; or
- the report is made after First Business Transactions has performed the disclosed acts (transaction(s)) and the report is made on the First Business Transactions's own initiative and as soon as it is reasonable for First Business Transactions to do so.

Suspicious transaction reports can be made 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)

Internal Reporting

An effective Anti-Money Laundering Compliance program recognizes that certain client transactions may be suspicious in nature. First Business Transactions must make an informed decision as to the suspicious nature of a particular transaction or pattern of transactions and determine whether to file a Suspicious Transaction Report (STR). In this regard, the company must know its clients and the nature of their businesses and respective account activities. The following lists provide examples of potentially suspicious activities that could raise red flags for further investigation. Upon closer inspection, the company may find that the transactions or activities reflect legitimate business activity rather than illicit activities.

Compliance Officer / MLRO plays an active role in the identification and reporting of suspicious transactions. This also involves regular review of exception reports or large or irregular transaction reports as well as ad hoc reports made by staff. To fulfil these functions First Business Transactions ensures that the MLRO receives full co-operation from all staff and full access to all relevant documentation to be able to decide whether attempted or actual ML/TF is suspected or known.

In particular, First Business Transactions ensures that:

- all staff are made aware of the identity of the Compliance Officer / MLRO and of the procedures to follow when making an internal disclosure report;
- all disclosure reports must reach the Compliance Officer /MLRO without undue delay.

The legal obligation is to report as soon as it is reasonable to do so, so reporting lines should be as short as possible with the minimum number of people between the staff with the suspicion and the Compliance Officer / MLRO. This ensures speed, confidentiality and accessibility to the Compliance Officer/MLRO.

All suspicious activity reported to the Compliance Officer / MLRO shall be documented (in urgent cases this may follow an initial discussion by telephone). The report shell include the full details of the customer and as full a statement as possible of the information giving rise to the suspicion.

Should an employee detect unusual or questionable activity, the employee will immediately notify the Compliance officer/MLRO in writing of the unusual activity through a Unusual Activity Report (UAR) attached as Appendix 2.

The Company employee must complete all of the required information on the UAR and must sign it prior to submitting it to theCompliance officer/MLRO.

All employees shall be trained to understand it is their responsibility to look for “unusual” activity, but it is the responsibility of the Compliance officer/MLRO to determine if that activity is unusual enough to be “suspicious.”

In the event that the activity/transaction being reported to the Compliance officer/MLRO involves a possible insider (any employee, officer, director, or other related party) of the company, the company employee may write “Anonymous” instead of providing their name and signature. If the Compliance

officer/MLRO is the subject of the UAR, the form should be delivered directly to the Company's CEO instead of the Compliance officer/ MLRO.

The Compliance officer/MLRO shall evaluate the information set forth in theUAR regarding the transaction or activity in question and shall either:

- indicate on the UAR that the activity/transaction is being logged on the Active Investigations Log attached as Appendix 3 and proceed with a due diligence investigation of the activity/transaction; or
- indicate on the UAR that the activity or transaction is not being logged on the Active Investigations Log and provide a detailed written explanation regarding such decision.

The Compliance officer/MLRO shall ensure that proper records are maintained for any such action.

The Compliance officer/MLRO shall conduct such further investigation as is deemed necessary and, if deemed appropriate, shall consult with legal counsel to determine whether such transaction or activity is suspicious and therefore reportable. The investigation may include, but is not limited to discussing the activity with the Company Officer, or other Company employees; reviewing the account/customer file; reviewing the customer account activity; and reviewing the specific transaction under consideration.

The Compliance officer/MLRO will present all relevant findings of the investigation to the Compliance Committee, along with his/her determination whether the data/information collected provides a satisfactory explanation for the unusual activity/transaction in question. The Compliance officer/MLRO will make the final decision concerning filing or not filing a STR in connection with the UAR.

If the Compliance officer/MLRO deems that the transaction/activity does not require the filing of a STR, the Compliance officer/MLRO shall note in the Investigations Log that the investigation is concluded and that no further action is required. The Compliance officer/MLRO shall also prepare a memorandum describing the investigative steps and the final outcome of the investigation resulting in the decision not to file a STR. The Compliance officer/MLRO shall place the memorandum in a specific file maintained for all transactions/activities investigated for which a STR has not been filed.

In the event that the Compliance officer/MLRO determines that a transaction or activity is suspicious and thus reportable through a STR, the Compliance officer/MLRO shall log the suspicious activity on the STR Log (sample attached as Appendix 4) as of the date the activity is deemed suspicious, and shall proceed to prepare the STR, consulting with legal counsel, if appropriate. Only the Compliance officer/MLRO is authorized to prepare and/or file a STR.

The Compliance officer/MLRO shall ensure that the STR form is properly completed and filed.
The Compliance officer/MLRO shall create and maintain a separate supporting documentation file for each STR filed which shall contain all documentation upon which the Company based its decision used to prepare to file the STR.
When evaluating an internal disclosure, the Compliance Officer / MLRO takes reasonable steps to consider all relevant information, including CDD and ongoing monitoring information available within or to First Business Transactions concerning the entities to which the report relates.

This may include:

- making a review of other transaction patterns and volumes through connected accounts;
- any previous patterns of instructions, the length of the business relationship and reference to CDD and ongoing monitoring information and documentation;
- appropriate questioning of the customer per the systematic approach to identifying suspicious transactions recommended by the JFIU. Compliance Officer / MLRO decides that there are grounds for knowledge or suspicion, to be disclosed to the JFIU.

Management Information Reports

A reporting process is implemented and an ongoing monthly trend analysis established to help facilitate governance, but further qualitative and quantitative information to ensure all higher risk factors are discussed and taken into consideration, in particular:

- number of high risk customers onboarded/rejected;
- number of high risk transactions escalated and closed;
- number of internal and/or external suspicious transaction reports.

Through MI reports the management is able to understand what's going on among different functions in compliance team such as:

- client on-boarding & screening (new on boarded clients that fall into categories such as higher risk customers on boarded, PEP Identified, positive adverse news matches, sanctioned country exposure, corruption/bribery, enforcement action/penalty/conviction, etc.)
- new product classification
- new country risk classification
- transactions alert and investigation process conducted upon

transactions monitoring and STR (transactions rejected, external STRs filed)

- risk rating methodology
- compliance Training.

Chapter 10. RECORD KEEPING

In compliance with its obligations with respect to records keeping under the effective law of Hong Kong, First Business Transactions ensures that:

- the audit trail for funds moving through First Business Transactions that relate to any customer and, where appropriate, the beneficial owner of the customer, account or transaction is clear and complete;
- all CDD information and transaction records are available swiftly to the CCE, other authorities and auditors upon appropriate authority;
- it can demonstrate compliance with any relevant requirements specified in guidelines issued by the CCE.

First Business Transactions maintains customer, transaction and other records that are necessary and sufficient to meet the record-keeping requirements:

- the original or a copy of the documents, and a record of the data and information, obtained in the course of identifying and verifying the identity of the customer and/or beneficial owner of the customer and/or beneficiary and/or persons who purports to act on behalf of the customer and/or other connected parties to the customer;
- any additional information in respect of a customer and /or beneficial owner of the customer that may be obtained for the purposes of EDD or ongoing monitoring;
- where applicable, the original or a copy of the documents, and a record of the data and information, on the purpose and intended nature of the business relationship;
- the original or a copy of the records and documents relating to the customer's account (e.g. account opening form; insurance application form);
- risk assessment form and business correspondence with the customer and any beneficial owner of the customer (which at a minimum should include business correspondence material to CDD measures or significant changes to the operation of the account).

Similarly, for occasional transaction equal to or exceeding the CDD threshold (HKD 8,000 for wire transfers and HKD 120,000 for other types of transactions), First Business Transactions keeps all documents and records mentioned above for a period of at least five years after the date of the occasional transaction.

All documents and records mentioned above are kept throughout the business relationship with the customer and for a period of at least five years after the end of the business relationship.

First Business Transactions also maintains the original or a copy of the documents, and a record of the data and information, obtained in connection with the transaction, which should be sufficient to permit reconstruction of individual transactions and establish a financial profile of any suspect account or customer. These records include the following:

- the identity of the parties to the transaction;
- the nature and date of the transaction;
- the type and amount of currency involved;
- the origin of the funds (if known);

- the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc;
- the destination of the funds;
- the form of instruction and authority;
- the type and identifying number of any account involved in the transaction (where applicable).

All documents and records mentioned above are kept for a period of at least five years after the completion of a transaction, regardless of whether the business relationship ends during the period.

The records of First Business Transactions are stored in First Business Transactions's computer database.

Chapter 11. WIRE TRANSFERS

A wire transfer is a transaction carried out by an institution (the ordering institution) on behalf of a person (the originator) by electronic means with a view to making an amount of money available to that person or another person (the recipient) at an institution (the beneficiary institution), which may be the ordering institution or another institution, whether or not one or more other institutions (intermediary institutions) participate in completion of the transfer of the money.

First Business Transactions as an ordering money service operator in an outward wire transfer transaction does not regard the beneficiary who has no relationship with First Business Transactions as its customer. As according to p. 4.1.5. of Hong-Kong Customs& Excise Department Guideline on

Anti-Money Laundering and Counter-Financing of Terrorism the term "customer" refers to the party, or parties, with whom a business relationship is established, or for whom a transaction is carried out by an MSO. This generally excludes the third parties of a transaction.

However, First Business Transactions ensures that the messages it sends to the cover intermediary bank contain originator and beneficiary information. The information on the beneficiary should at least include its name or an identifier code as well as the other beneficiary information sent directly to the bank of the beneficiary, if any.

Ordering Institutions

As an ordering institution, First Business Transactions ensures that a wire transfer of amount equal to or above HKD 8,000 (or an equivalent amount in any other currency) is accompanied by the following originator and recipient information:

- the originator's name;
- the number of the originator's account maintained with First Business Transactions and from which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned by First Business Transactions;
- the originator's address, the originator's customer identification number or identification document number or, if the originator is an individual, the originator's date and place of birth;
- the recipient's name;
- the number of the recipient's account maintained with the beneficiary institution and to which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned to the wire transfer by the beneficiary institution.

First Business Transactions ensures that a wire transfer of amount below HKD 8,000 (or an equivalent amount in any other currency) is accompanied by the following originator and recipient information:

- the originator's name;
- the number of the originator's account maintained with First Business Transactions and from which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned by the ordering institution;
- the recipient's name;
- the number of the recipient's account maintained with the beneficiary institution and to which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned to the wire transfer by the beneficiary institution.

For a wire transfer of amount equal to or above HKD 8,000 (or an equivalent amount in any other currency), First Business Transactions ensures that the required originator information accompanying the wire transfer is accurate.

For an occasional wire transfer involving an amount equal to or above HKD 8,000 (or an equivalent amount in any other currency), First Business Transactions shall verify the identity of the originator.

For an occasional wire transfer below HKD 8,000 (or an equivalent amount in any other currency), First Business Transactions is in general not required to verify the originator's identity, except when several transactions are carried out which appear to First Business Transactions to be linked and are equal to or above HKD 8,000 (or an equivalent amount in any other currency), or when there is a suspicion of ML/TF.

For a domestic wire transfer, First Business Transactions may choose not to include the complete required originator information in the wire transfer but only include the originator's account number or, in the absence of an account, a unique reference number, provided that the number permits traceability of the wire transfer.

Beneficiary Institution

As a beneficiary institution, First Business Transactions establishes and maintains effective procedures for identifying and handling incoming wire transfers that do not comply with the relevant originator or recipient information requirements, which include:

- taking reasonable measures (e.g. post-event monitoring) to identify domestic or cross-border wire transfers that lack required originator information or required recipient information;
- having risk-based policies and procedures for determining when to execute, reject, or suspend a wire transfer lacking required originator information or required recipient information;
- the appropriate follow-up action.

Intermediary Institution

As an intermediary institution, First Business Transactions ensures that all originator and recipient information which accompanies the wire transfer is retained with the transfer and is transmitted to the institution to which it passes on the transfer instruction.

First Business Transactions establishes and maintains effective procedures for identifying and handling incoming wire transfers that have not been complied with the relevant originator or recipient information requirements, which include:

- taking reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or required recipient information;
- having risk-based policies and procedures for determining when to execute, reject, or suspend a wire transfer lacking required originator information or required recipient information and the appropriate follow-up action;
- if a cross-border wire transfer is not accompanied by the required originator information or required recipient information, First Business Transactions shall as soon as reasonably practicable, obtain the missing information from the institution from which it receives the transfer instruction. If the missing information cannot be obtained, First Business Transactions shall either consider restricting or terminating its business relationship with that institution, or take reasonable measures to mitigate the risk of ML/TF involved.

Chapter 12. REMITTANCES

The AMLO defines a remittance transaction as a transaction for sending, or arranging for the sending of, money to a place outside Hong Kong and prescribes the special requirements that must be completed by an MSO before carrying out such a remittance transaction. Essentially, these special requirements amount to the identification and verification of the originator as defined below and various record keeping requirements.

Identification and verification of originator

Before carrying out a remittance transaction, other than a wire transfer, of HKD 8,000 or above or of an equivalent amount in any other currency, First Business Transactions takes measures to identify the originator and verify the identity of the originator and records:

- the originator's name;
- the originator's identification document number and, if the originator's identification document is a travel document, the place of issue of the travel document;
- the originator's address;
- the currency and amount involved;
- the date and time of receipt of the instruction, the recipient's name and address and the method of delivery.

Appendix 1. Onboarding Form

	Name of the Company:			
	❑ Full name			
	❑ Abbreviate name			
	❑ Foreign languages name (if applicable)			
	Legal form			
	State registration information			
	❑ Date			
	❑ Registration number			
	❑ Name of the registration authority			
	❑ Place of registration			
	Legal address			
	Postal address			
	E-mail, URL		**Test login**	**Test password**
	License information (if applicable)			
	☐ Type of activity			
	☐ License No			
	☐ Date of issue			
	☐ Issuing authority			
	☐ Validity (date of issue and date of expiration)			
	Country of Tax Residency		**TAX number**	
	Share capital			
	☐ Amount of the registered share capital			
	☐ Amount of the paid share capital			
	Actual number of personnel			
	Are there any insolvency (bankruptcy) legal proceedings against the Company? Are there any legally effective court decision on insolvency (bankruptcy) in respect of the Company?	**Yes** ☐ **No** ☐ If Yes, please specify:		
	Are there any fact of your financial obligations default due to lack of funds in bank accounts?	**Yes** ☐ **No** ☐ If Yes, please specify:		

	Administrative bodies of the Company (list of the Board of Directors (if applicable), CEO or representative)	1.			Is the Director acting as a nominee? Yes ” No ”
		2.			Is the Director acting as a nominee? Yes ” No ”
		3.			Is the Director acting as a nominee? Yes ” No ”
		4.			Is the Director acting as a nominee? Yes ” No ”
		5.			Is the Director acting as a nominee? Yes ” No ”
	Name of the CFO (or equivalent)				
	Information about the person (s), who is the Company’s ultimate beneficial owner (s), with an indication of the share of equity (full details of the beneficial owner specified in the application in the form prescribed in Appendix 3)				
	Details of Shareholders (participants) holding 5% or more of the authorized capital with an indication of percentage of shares held *In case where the shareholder is a nominee/nominee company please provide all corporate document up to the physical persons (including trust deeds/trust declarations)	1.	Percentage of shares held		Is the Shareholder acting as a nominee? Yes ” No ”
		2.	Percentage of shares held		Is the Shareholder acting as a nominee? Yes ” No ”
		3.	Percentage of shares held		Is the Shareholder acting as a nominee? Yes ” No ”
		4.	Percentage of shares held		Is the Shareholder acting as a nominee? Yes ” No ”
	Types of activity (goods, services)				
	Region (countries) of the business activity?				
	Does your Company have an obligation for the preparation of financial statement to comply with applicable legislation framework?	**Yes** ☐ **No** ☐ If No, please specify the reason:			
	How long the Company carries on business activity in this area?				

	Please specify the planning turnover of the Company (monthly/yearly), average amount of transactions	
	Please specify the WEB site of the Company or other sources of information about the Company	
	History, reputation, segment of the market and competitors of the Company	

GENERAL AML POLICIES, PRACTICES AND PROCEDURES **Yes** **No** **N/A**

1 (a) Is your institution subject to the supervision of any regulatory authority?

1(b) If yes, please provide the name of the supervisory/regulatory authority, including the one responsible for supervising and controlling money laundering prevention:

1 (c) Please provide your registration / operating license number

2 Does your country adhere to the 40+9 anti-money laundering and counter terrorism financing recommendations developed by the Financial Action Task Force (FATF)?

3 (a) Does your institution have a designated Compliance Officer responsible for the overall AML/CTF program?

3 (b) If "yes," please provide:

- Complete Name:
- Position Title:
- Mailing Address:
- Telephone Number:

4 Does your institution have a written legal and regulatory compliance program that includes a designated Compliance Officer that is responsible for coordinating and overseeing the AML program on a day to day basis?

5 (a) Does your institution's AML program require approval of the Board of Directors?

5 (b) Please specify the most recent date the AML program was last updated:

6 Are your institution's AML policies and procedures being applied to all your branches/subsidiaries both in the home country and in locations outside that jurisdiction?

7 Does your institution have written policies documenting the processes that you have in place to prevent and detect any suspicious transactions/terrorist financing activities?

8 Does your institution have policies and procedures to prohibit any accounts/relationships with shell banks/organizations?

9 (a) Was your institution subject to any investigation related to ML/CTF?

9 (b) If 'Yes' please specify when:

10 (a) Has your institution received any regulatory enforcement action currently or within the past three years?

10 (b) If 'Yes', has the regulatory enforcement action resulted in fines or penalties being assessed?

11 (a) Was your institution ever got fined for ML/CTF crimes?

11 (b) If 'Yes' please specify when and provide additional details regarding the fine:

12 Does your Company have procedures in place to monitor accounts and transactions in order to prevent and detect suspicious activity?

II. PROTECTION OF PERSONAL DATA

The personal data requested above may be recorded in one or several databases in accordance with applicable legislation. _____ may outsource the processing and storage of this data. You expressly authorize _____ to collect and process this personal data. You may make a written request to consult the data concerning yourself and to rectify any inaccuracies in this data. _____ may record or process your personal data for the purpose of managing its contractual relationships with you, including transfer of personal data to our partners in order to provide services to you.

III. FOREIGN ACCOUNT TAX COMPLIANCE ACT (FATCA)

We would like to draw your attention to the USA's Foreign Account Tax Compliance Act (a.k.a FATCA) and its possible implications*. Please indicate if you or any of your beneficial owners are a U.S citizen or resident or are otherwise to be considered as a 'US Person' as per FATCA:

o NO. I/We hereby declare that we are familiar with the FATCA guidelines and possible implications on the parties and that I am/we and any of our beneficial owners are NOT a U.S citizen or resident or are otherwise to be considered as a 'US Person' as per FATCA

o YES. I/We hereby declare that we are familiar with the FATCA guidelines and possible implications on the parties and that I am/we or any of our beneficial owners ARE a U.S citizen or resident or are otherwise to be considered as a 'US Person' as per FATCA and will provide us as soon as possible with the relevant documents, information, W-9 forms and other materials as requested by us.

I/We agree to indemnify _____in respect of any false or misleading information regarding my/our "U.S. person" status for U.S. federal income tax purposes. I/We agree to notify _____30 days of any change in the aforementioned statement.

* For more information see also: http://www.irs.gov/Businesses/Corporations/Foreign-Account-Tax-Compliance-Act-FATCA.

IV. REQUESTED DOCUMENTATION

The following documents (certified copies) shall be attached to the Questionnaire:

1. **Memorandum and Articles of Association;**
2. **Certificate of Incorporation / Registration;**
3. **Certificate of Directors/;**
4. **Certificate of good standing (in the event that the company is older than one year old);**
5. **Certificate of Incumbency;**
6. **Certificate of Shareholders, Register of shareholders or other equivalent document;**
7. **Legal ownership structure certified by the UBO or the person who effectively controls the company**
8. **Operating license and\or authorization;**
9. **Declaration of Trust (if applicable)**
10. **Trust Deeds/ Trust Settlement Agreement (if applicable)**
11. **Onboarding Form followed by you duly completed**
12. **Annual financial (accounting) statements;**
13. **Audited financial (accounting) statements for the last accounting period;**
14. **In the absence of the documents referred to in paragraphs 12-13, an official letter, containing the reasons for the absence of these documents, shall be submitted;**
15. **Identity Card or Passport of representative/s (director/s) and Utility Bill of representative/s (director/s);**
16. **Details of the Company's UBO's including certified copy of passport, and proof of permanent address.**
17. **Account opening confirmation**

***All documents shall be less than 6 months old from the date this questionnaire is signed, presented in hard copies duly certified before any operational activities.**

V. DECLARATIONS AND SIGNATURE

We hereby declare that :

- we are acting on our own account and not on behalf of any other person;
- any funds that are received by us in the future will not be used for the financing of terrorism or with any fraudulent activities; and
- we have not in the past committed any irregularities or fraud in breach of anti-money laundering and financing of terrorism applicable legislation.

In addition, we hereby declare that the details and declarations provided in this Onboarding Form and any documents provided together with this form are, to the best of our knowledge and belief, true, accurate, correct, complete and not misleading and we undertake to immediately inform you about any changes. If any such details, declarations or documents cease to be true, accurate, correct, complete or not misleading, we are aware that we may be held liable for this.

I have answered all questions and understand that my application is subject to verification and approval by _____, reserves the right to decline the application, if it is found to be incomplete or ineligible, and further requests the right to request additional information/documentation as part of the Know Your Customer principles and best banking practices, or even deny processing to any merchant at its own discretion.

Date	
Stamp	_____ (Name, director/representative signature)

Appendix 1
to the Onboarding form

Questionnaire for Shareholders
(legal entity)

	Name of the legal entity:			
	❑ Full name			
	❑ Abbreviate name			
	❑ Foreign languages name (if applicable)			
	Legal form			
	State registration information			
	❑ Data			
	❑ Registration number			
	❑ Name of the registration authority			
	❑ Place of registration			
	Legal address			
	Postal address			
	E-mail, URL			
	Information on the presence (or absence) of Company's director(s) at the legal address of the Company.			
	Country of Tax Residency		**TAX number**	
	Percentage and number of shares in the share capital of the Company			
	Is the Shareholder acting as a nominee?		Yes " No "	
	Date			
	Stamp		_____ (Name, director/representative signature)	

Appendix 2
to the Onboarding form

Questionnaire for Shareholders and Administrative bodies (individuals)

	Name, Surname			
	Date of birth			
	Place of birth			
	Citizenship			
	Actual address			
	Domicile			
	ID or Passport information			
	a. Name of the document			
	b. Number			
	c. Issuing body			
	d. Validity (date of issue and date of expiration)			
	Place of work, title			
	Share in the share capital of the Company (for shareholders only)			
	Country of Tax Residency		Tax identification number (if applicable)	
	Source of wealth			
	Are you a foreign public official/ Politically Exposed Person?		Yes " No " If Yes, please specify:	
	Is any of your close family members/associates a foreign public official/ Politically Exposed Person? * A Politically Exposed Person is defined 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 (i); (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).		Yes " No " If Yes, please specify: Position held Period Relationship with you	
	Is the Shareholder acting as a nominee?		Yes " No "	
	Contact phone number or faximile			
	Email			
	Date			
	Signature			

Appendix 3
to the Onboarding form

Ultimate beneficial owner (UBO) Information

(Beneficial owner means any natural person who ultimately owns or controls the legal entity through direct or indirect ownership or control over 10 % plus 1 (one) share or more of the shares or voting rights in that legal entity or any natural person who otherwise exercises control over the management of the legal entity)

_____

(*Name of the Company for which the listed below individual is the UBO*)

Name			
Last name			
Patronymic (if applicable)			
Date of birth			
Place of birth			
Citizenship			
Share in the share capital of the Company			
Domicile			
Actual address			
Source of wealth			
Country of Tax Residency		TAX number (if applicable)	
Are you a foreign public official/ Politically Exposed Person?		Yes " No " If Yes, please specify:	
Is any of your close family members/associates a foreign public official/ Politically Exposed Person? * A Politically Exposed Person is defined 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 (i); (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).		Yes " No " If Yes, please specify: Position held Period Relationship with you	
Contact phone number or faximile/e-mail			
ID or Passport information			
a. Name of the document			
b. Number			
c. Issuing body			
d. Validity (date of issue and date of expiration)			

Type of business activity	

_____/_____/ «____»_____ 20___

Full name **Signature**

Appendix 2. Unusual Activity Report (UAR)

Report Date:		
Submitted by:		Title:
Customer Name:		Account Number:
Transaction ID:		
Linked Transactions IDs:		
Activity Prompting Report:		
Structuring	High Activity	Number of Transactions
Transaction Amount	Numerous Transactions	Other Activity
Other person/entity involved:		
Details of Activity Prompting Report:		

Appendix 3. Active Investigations Log

Date	Reported/ Submitted by	Nature of Unusual Activity	Investigative Steps Taken	Current Status (Open/Closed)	Final Disposition

Appendix 4. Suspicious Transactions Reports Log (STR Log)

STR LOG

Date last updated: DD/MM/YYYY

Date	Date Filed	ACC(s)	Internal Tracking No.	Reason for Filing	Open / Closed	Amount	Summary of Activity	Suspect Info	Monetary Loss	Electronic Reference No.

Appendix 5. Prohibited Business Types

Merchant Category Code	General Business Services	Description of Prohibited Activity Types
Various	Adult Content	Any merchant connected with visual content, such as pornography or violence, that is not generally thought to be appropriate for viewing by children.
Various	Alcohol sales via Internet	Merchants selling alcohol products via internet, even if the sale of those items is NOT restricted to the merchant own country of domicile.
5169	Chemicals and Allied Products – not elsewhere classified	Wholesale distributors of chemicals and allied products not elsewhere classified. Products for sale are typically used for industrial purposes. Examples include industrial acids, ammonia and alcohol, heavy, aromatic and other chemicals, chlorine, compressed and liquefied gases, detergents, fuel and oil additives, resins, salts, turpentine, sealants, rust proofing chemicals, coal tar products, dry ice, dyestuffs, glue, gelatin, and explosives.
Various	Child Pornography	Any merchant who provides products or services associated with actual or suggested child pornography. Includes any merchant or website who uses the following terminology to promote their product: "lolita," "pedo," "pre-teen," or any other terminology that suggests child pornography.
5993	Cigarette/electronic cigarette/ Tobacco/ Vape Sales	Merchants that sell cigarettes/electronic cigarette/tobacco/vape via Internet even if the sale of those items is NOT restricted to the merchants own country of domicile.
Various	Counterfeit goods	Merchants selling counterfeit merchandise (well-known brands) or goods where merchants are infringing on intellectual property rights of trade mark owners (including illegal use of games, game keys e.t.c.)
5122, 5912, 5999	Non-prescription drugs such as pharmaceutical wonder drugs e.g. Steroids, diet pills & all Internet drug stores.	Outlets offering nonprescription drugs such as: pharmaceutical wonder drugs e.g. steroids, diets pills, and all Internet drug stores.

Merchant Category Code	General Business Services	Description of Prohibited Activity Types
5122	Drug Paraphernalia	Any business whose products are solely intended for aiding the consumption of illegal drugs.
7996	Fortune tellers	Includes fortune-tellers, tarot card readers, and mystics.
5099, 5941	Guns, firearms, munitions sale & distribution	Any sale of firearms by any method
Various	Financial and other Pyramid Sales	Includes sales structures where multiple levels of sales people are making money off one another with no real product or a questionable product to sell: income of the first participants of pyramid is paid at the expense of new participants.
7297	Sexual Encounter/Escort Firms	Any merchant connected with sexual encounter, including escort services, massage parlors, spas, etc., where sexual encounters are permitted.
8651	Political Organizations and parties	Merchants representing the membership organizations that promote the interests of a national, state, or local political party or candidate, including political groups organized specifically to raise funds for a political party or individual candidate.
8661	Religious Organizations (excluding nationally recognized religious organizations/faiths)	Religious organizations that provide worship services, religious training or study, and religious activities, including collection of donations.