Contents

1. FIRM POLICY

This Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") Policy is restricted for internal use by the management and employees of Isend Pte. Ltd (the "Company") in respect of their dealings with clients and intermediaries. All employees are required to read, understand and strictly adhere to this Policy.

It is the policy of the Company to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the following legislations and regulations:

- Monetary Authority of Singapore Act (Cap. 186);
- Money-changing and Remittance Businesses Act (Cap. 187);
- Terrorism (Suppression of Financing) Act. (Cap. 325);
- Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap 65A);
- Monetary Authority of Singapore (Anti-Terrorism Measures) Regulations 2002; and
- MAS Notice 3001 and its implementing regulations.

Money Laundering

Money laundering (ML) is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorist Financing

Terrorist financing (TF) may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers,

the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Our AML/CFT policies, procedures and internal controls are designed to ensure compliance with all applicable Monetary Authority of Singapore rules and will be reviewed and updated on annual basis or on material trigger to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

2. AML/CFT PRIMARY AND SECONDARY LEGISLATION IN SINGAPORE

- Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A);
- Monetary Authority of Singapore (Anti-Terrorism Measures) Regulations 2002; and
- Terrorism (Suppression of Financing) Act (Cap. 325).
- MAS Notice 3001: Notice on Prevention of Money Laundering and Countering the Financing of Terrorism – Guidelines to MAS Notice 3001 on Prevention of Money Laundering and Countering the Financing of Terrorism
- Guidelines for Financial Institutions to Safeguard the Integrity of Singapore's Financial System

3. EMPLOYEES' RESPONSIBILTY FOR AML/CFT

This Policy aims to emphasise that whilst the ultimate responsibility and accountability with AML and CFT rest with the board of directors and senior management (appointed managers), every employee of the Company plays a key role in identifying any signs of suspicious transactions and identifying any client and/or trust relevant party that may have been involved in money laundering or terrorist financing.

3.1 The Three Lines of Defence

First line of defence - Front line client serving persons

The Front line (e.g. counter employees and business/marketing personnel) forms part of the first line defence. Their role is to identify and assess the money

laundering and terrorist financing risk by identifying the clients by way of obtaining client due diligence documents during over the counter transactions, on-boarding clients, on-going monitoring and remittance transactions. As the client facing officer, the Front line shall attempt to communicate with the client directly to seek any update of changes in the client's personal information and financial source. When in doubt, the Front line shall not hesitate to obtain more information and follow up on any anomalies. If there is any reason for the officer to believe that the transaction is suspicious in nature, a notification has to be made to Compliance Officer immediately. It is to be noted however, that making any disclosure or providing any tip off to a client that an investigation is underway is an offence and prohibited at all times.

Second line of defence - Compliance

The secondary line of defence lies with the Compliance Officer whose responsibility is to conduct thorough reviews of clients, conduct CDD and monitor transactions on a risk-based approach. This line of defence is also responsible for investigating any exception reports and escalating the matter to the senior management. If there is a reasonable ground for Compliance to suspect money laundering and terrorist financing, a suspicious transaction report (STR) should be submitted to the Commercial Affairs Department (STRO) within 12 working days.

Third line of defence- Internal Audit

As the third line of defence, the role of internal auditor is to independently evaluate the AML and CFT risk management and control within the Company by evaluating the adequacy and effectiveness of the Company's policies and procedures on AML and CFT that have been put in place. Some of the key areas that require evaluation include the following:

- The adequacy of the Company's policies in identifying and managing money laundering and terrorist financing risk.
- The effectiveness of the employee and the officers in implementing the policies and procedures.
- The frequency and the effectiveness of AML/CFT trainings that have provided to the employees.

Finally, the directors and senior management (manager or employee appointed by a Director to have delegated responsibilities) are ultimately responsible and accountable for ensuring the Company's compliance with the laws, regulations and guidelines for the prevention of money laundering and financing terrorism of Singapore and where necessary, take appropriate remedial action if breaches are identified.

4. ENTERPRISE WIDE RISK ASSESSMENT

In addition to assessing the ML/TF risks presented by the client, the Company shall also identify and assess the ML/TF risk at enterprise level.

The objective of enterprise-wide ML/TF risk assessment is to enable the company to better understand its overall vulnerability to ML/TF risks. This shall form the basis for the Company's overall risk-based approach. The Company's senior management shall approve the enterprise-wide risk assessment. All employees should give their full support and cooperation for the assessment.

The enterprise-wide risk assessment shall take into account the following ML/TF risk that the Company faced

(a) The clients, intermediaries, and agents (collectively known as Parties);
(b) The countries or jurisdictions its Parties are from or in;
(c) The countries or jurisdictions the Company has operations in;
(d) The products, services, transactions and delivery channels of the Company

In addition, the Company shall incorporate the results of the Singapore National ML/TF Risk Assessment ("NRA") Report during its risk assessment process.

The enterprise-wide risk assessment shall be reviewed at least once on annual basis or when material trigger events occur, whichever is earlier.

Material trigger events include, but are not limited to the following:

(a) The acquisition of new segments of clients from certain industries/jurisdictions
(b) New delivery channels
(c) The launch of new products and services by the Company
(d) Regulatory changes
(e) Additional or changes in Company's operating jurisdictions

If any of the above trigger (a) to (e) events occur, it may be necessary to review the risk assessment and go through a risk assessment process prior to implementation within the Company.

The risk management methodology will incorporate the following steps:

<u>Measure the risk</u>

- Identify the risk and the various risk factors

- Assess the risk factors incorporating the likelihood of the risk occurring and the potential impact if the risk occurs

Manage the risk

- This will involve analysing the Company's current internal control procedures and policies in operation and to assess whether they mitigate or reduce any identified risk factors from the new product, channel etc.
- Evaluate the identified internal control to identify whether the identified risks are adequately managed

Update the enterprise wide ML/TF risk matrix

- The enterprise wide risk assessment is updated to reflect the new product, channel etc. to give the overall enterprise risk assessment
- The overall risk assessment is reviewed by senior management to ensure the risk is within acceptable and defined limits or whether further risk reduction or mitigation measures are required

Risk mitigation

- Assess whether any new or changes to the current internal controls, procedures or policies is needed to address the risks identified
- Implementation of the appropriate or required internal controls, policies or procedures prior to the new product, channel etc.

Risk monitoring and review

- Periodic monitoring of the risks to ensure that the identified risks and managed in a structured and timely manner
- The risks are also reviewed when there is a change in circumstances or a situation is identified (such as a trigger event) that has led to a reassessment of the risks faced by Company.

Senior management consisting of Directors and Compliance Officer are required to sign-off on the assessment prior to the implementation of the relevant new product or channel.

The results of these reviews should be documented and approved by senior management even if there are no significant changes to the Company's enterprise-wide risk assessment.

5. CLIENT RISK ASSESSMENT

In order to allow financial services to focus compliance resources where these are most required, the Company is required take a risk-based approach to risk rate each client by the completion of the relevant CDD & Risk Assessment Form (Form B) and to seek to conduct client due diligence on the basis of the risk. All

risk rating is conducted by the Front line and Compliance by completing the Risk Assessment Forms and tallying the total score for a risk rating and the risk rating will dictate the amount of client due diligence required and the frequency of all on-going monitoring and reviews.

The simple premise is that the greater the risk that the client is engaged in money laundering or the financing of terrorism, the more documentation the financial services institution should obtain in order to verify the client's identity and perform Enhance Due Diligence (EDD) as shall be necessary to manage that risk or make a decision to terminate establishing the relationship or file a Suspicious Transaction Report.

6. CUSTOMER DUE DILIGENCE

Every effort must be made to identify and report illicit funds to relevant authorities in order for necessary corrective action to be taken. The Client Due Diligence (CDD) process has become integral to all financial service providers including remittance businesses, as a means to identify questionable funds and activities. The CDD procedures set in this Policy ensures the Company assist relevant authorities to control money laundering and terrorism financing activities and observes the AML/CFT laws. One of the main objectives of this Policy is to uphold that the Company must "know your customer" by way of the CDD process. This is an ongoing process that continues and is updated over the full life of the customer engagement.

6.1 CDD Initiating Procedures

The CDD account opening process for individuals and corporates consist of:
(1) Individual or Corporate Account Opening Forms (Form A and Form C),
(2) Risk Assessment Form (Form B)
(3) Identification documentation and information
(4) verification proofs
(5) screening reports

Whenever possible, prior to any account opening for a new customer, a face to face meeting is necessary.

The Company will be responsible for the conduct of CDD on its clients and complete CDD must also be conducted for foreign paying agents which includes banks, remittance agents.

6.2 Customer Forms

The Company prescribe standards forms for completion and execution whenever the Company accepts a new customer as part of the CDD, identification, verification and risk assessment process. These forms constitute

the initial set of documentation that the Company will include during account onboarding and these forms contain important legal declarations and self-certifications which the client must make prior to being onboarded. The customer must complete:

(1) Individual or Corporate Account Opening Forms
(2) Risk Assessment Forms
(3) For Large Transactions of SGD$1500 the customer must complete a Declaration of Fund Form.
(4) New Beneficiary Form (for existing customer with new beneficiaries)

A copy of these Forms is attached in the Appendices.

Type of Forms	Form Number	Purpose of Form	Parties to Complete Form	Comments
Individual Account Opening Application	FORM A	Every individual customer must complete this Form before remittance services is provided. And to gather required KYC/CDD information on each customer. Customer to declare residing address.	The individual customer	Must complete for each new individual customer
Individual Risk Assessment Form (CDD)	FORM B	To ensure each customer is assessed for ML/TF risk and the rating will indicate the amount of due diligence required and for ongoing periodic reviews	-Front line -Compliance -Manager -Director	For Low and Medium risk rating, Compliance and Manager may approve proposed account opening and transactions. For High rating, only Director may approve.
Declaration of Fund Form (Sender)	FORM D	-For transactions 1500 above -For Large Transaction 5000 - Process for EDD	Customer	Front line to give customer
New Beneficiary Form	FORM A	-Whenever remittance to a new beneficiary -whenever the Company require	Customer	If the Frontline require more information of a new beneficiary from a existing customer this Form should be completed.

Type of Form	Form Number	Purpose of Form	Parties to Complete Form	Comments
Corporate Account Opening Application Form	FORM C	Every corporate customer must complete this Form before remittance services is provided. And to gather required KYC/CDD	The Corporate customer	Must complete for each new corporate customer.

		information on each customer.		
Corporate Risk Assessment Form (CDD)	FORM B	To ensure each corporate customer is assessed for ML/TF risk and the rating will indicate the amount of due diligence required and for ongoing periodic reviews	-Front line -Compliance -Manager -Director	For Low and Medium risk rating, Compliance may approve proposed account opening and transactions. For High risk rating, only Director may approve.
Customer Watch List Register	FORM F	• Internal STR escalated • External STR filed • Frequent large or small remittances • Multiple Senders to same beneficiary • Name hits from screening result (positive and false) must be recorded in this register • Large transactions 5000 and above • Other unusual transactions	-Compliance -Manager -Employees	-For ongoing monitoring -Director to review register annually and sign off
AML/KYC Questionnaire	Wolfsberg AML Questionnaire		-Financial Institutions -Agents	
Suspicious Transaction Report Form (Internal STR)	FORM E	For internal investigation before filling a STR to STROLLS.	-Front line -Compliance -Manager -Director	This Form should be completed before an external STR is filed with STROLLS.
Risk Assessment Form for FIs and Agents	Wolfsberg AML Questionnaire	Before using or providing services to FIs and engaging Agents	-Compliance -Manager; or -Director	Simplified CDD may be considered for Singapore Financial Institutions or foreign FIs regulated my competent authorities and FTAF compliant jurisdictions.

6.3 Customers Who Refuse to Provide Information

If a potential or existing customer either refuses to provide the information requested in the relevant forms without a reasonable explanation, or appears to have intentionally provided misleading information, our firm will not open a new account or refuse transactions and, after considering the risks involved, consider closing any existing account. In either case, our Senior Management will be notified so that we can determine whether we should file a STR.

6.4 Identification and Verification

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. Our Compliance officer will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

We will verify customer identity through documentary means, non-documentary means or both. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, postal code, telephone number, date of birth and identity document number, allow us to determine that we have a reasonable belief that we know the identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

Appropriate identification and verification procedure of customers include the following:

6.5 Identification requirements for individuals

With respect to each individual, the following identification information must be obtained.

(i) full name (including any former name and any aliases);
(ii) gender;
(iii) government-issued personal identification number;
(iv) principal residential addresses (residential address where the person is working, if applicable);
(v) contact telephone number;

(vi) nationality;
(vii) occupation;
(viii) employer;
(ix) place of birth; and
(x) date of birth.

6.6 Verification procedure for individuals

With respect to each individual, the following verification procedures must be carried out:

- For an individual. Sight an original valid government issued photo identification document evidencing residential address and take a photocopy. The employee who sighted and photocopied the original document must clearly indicate on the photocopy that the original has been sighted, employee name, designation, and signature. Alternatively, without having to sighted the original document, obtain a certified copy. Examples of a government issued document are national identity card, work permit or its equivalent, driving license and valid passport (at least 6 months before expiry), and various Singapore issued foreigner work passes, which includes employment pass, s-pass, long-term pass and work permit.

- Alternatively, for over the counter transactions verification will be to sight the identification documents as described above and scan a copy of the identification documents into the Company's computerized system.

  Note that in cases where the photograph of the primary identity document was taken at a younger age (as is often the case with citizen's identity card) and therefore may not allow verification of a person's identity with absolute certainty, secondary identity document bearing recent photograph (such as driving licence) will be requested as supplementary document. Both the primary and secondary identity document will be verified and sighted as required in this Policy for record retention.

  Note: All photocopied or scanned identification document must be a clear copy of the photograph of the holder and all information readable. Blurred copies are unacceptable.

- If the government issued document does not evidence residing address, Frontline must sight an original document evidencing the individual's permanent address (home country) or current address (the country where the individual is currently working and residing), such as a utility/telephone bill or a bank statement (issued within the prior 3 months) and take a photocopy or for over the counter transactions scan

a copy of the proof of address document into the Company's system. The employee who sighted and photocopied the original document must clearly indicate on the photocopy that the original has been sighted, employee name, designation, and signature. Alternatively, without having to sighted the original document, obtain a certified copy.

In some situations, when foreign workers are unable to produce a document evidencing a proof of residence, therefore the Company should obtain and sight a dormitory pass indicating the dormitory address of the workers. The Company may at its discretion carry out dormitory on-site inspection to authenticate dormitory address.

Note: In the event, conflicting information is discovered (example: address in identification document is different from document evidencing residing address), the employee must verify the discrepancies with the individual and confirm the appropriate information and this verification and confirmation must be documented by a file note or written on the respective account opening forms.

6.7 Specific types of Customers

Certain class of foreign workers in specific industries may not have the required documents for verifying certain information (their work permit may not indicate residing address), therefore collecting identification information and conducting verification procedures as required in this Policy may not be possible. It is acceptable to adopt alternative identification and verification procedures for the following situations:

a. Crewmen working on a ship

In shipping industries, there are situations when crewmen's identification information and verification documents mentioned above cannot be obtained. The Company can accept a crewmen list issued by Singapore Immigration and Custom Authority as a substitute or a copy of the immigration stamp indicating the vessel's name, or a letter signed by the vessel's Captain or First Officer confirming the crewmen's identity.

b. Foreign workers

The Front-line employee should obtain identification information and conduct verification procedures on the representative foreign worker by obtaining their national identity document, or passport, or a letter issued by the Ministry of Manpower or a dormitory pass and sign the declaration in Individual Account Opening Application Form, Form A.

c. Foreign worker sending money on behalf of another domestic/foreign worker

For amount of below SGD$5000
The Front-line employee should obtain identification information and conduct verification procedures on the representative foreign worker. Front line should ask for the actual sender's (a) Name (b) Contact Number.

For amount of SGD$5000 and above
The Front-line employee should obtain identification information and conduct verification procedures on the representative foreign worker. Front line should ask for the actual sender's (a) Name (b) FIN (c) Contact Number and in addition conduct CDD, identification and verification procedures on the beneficiary.

6.8 Individual Account Opening Procedures

This serves to document the customer due diligence procedures that must be conducted on a person applying to open an account with the Company to facilitate remittance transaction. It is important to note that what is detailed here pertains to account opening only.

Individual account opening refers to request by an individual person in his/her own capacity, for the setting up of a customer account with the Company for remitting funds.

6.8.1 The "Individual Account Opening Application Form" Form A

The first step for establishing the relationship between an individual and the Company is the completion of the "Individual Account Opening Application Form A". A copy of the Form A is attached in the Appendices.

Form A is designed to allow us to gather information that is required for CDD, identification and verification procedures, profiling and risk assessment of the individual in relation to ML/TF.

Therefore, all fields in this form MUST be completed. Where certain fields are not applicable (for example, if the applicant does not have Alias), it must be filled with the abbreviation "NA" which stands for Not Applicable.

6.8.2 Front line account opening CDD procedures for Individual Customer

Applicant 's Identity Verification:

- Applicant complete "Individual Account Opening Application" Form A & submit form together with original identity document and proof of residential address to our staff. In the event where potential customer is obtained through marketing cold-calling or other marketing strategies, our staff will make physical visitation to meet customer(s) to complete the necessary CDD procedures and collect all required documents for CDD purposes.

- Completed Form A will be signed by Applicant in the presence of our staff

- Front line verify that Applicant is the same person as the photograph in **Original Identity Document** and also check to ensure that document has not expired.

- Front line must perform a check against the client database to make sure the individual does not have an existing account with the Company. No second account is to be opened for existing account holders (individual or corporate) unless approved by the Director and such the reason for approval must be documented on the new account opening form.

Copies must be made for all identification documents, digital signature and each copy must be verified and sighted as prescribed in this Policy or for over the counter transactions all identification and proof of address documents/ photo must be scanned and uploaded into the system.

If the applicant is unable to produce identification documents and the Company is unable to verify the applicant's identity to its satisfaction, Account Opening Application must be rejected.

- Front line or the Compliance Officer or the Manager should complete the "Individual Risk Assessment Form" Form B using that as the tool to systematically conduct CDD and risk assessment.

As applicant is currently not a customer, he/she does not have a customer reference number. Therefore, for the purpose of tracking the account opening application, the applicant is assigned a unique "Application Ref No", which is used to track this application and shall appear on all documents and forms related to this application. This facilitates tracking and cross-referencing.

"Application Ref No" is assigned sequentially, with the next applicant being assigned the next number in the sequence.

- Front line to check the completed Form A to ensure that all fields are completed. Fields that are not relevant /applicable to the applicant should be filled with “NA”.

If Applicant is unable to complete the form because he/she does not understand what is required, Front line employee may explain and guide applicant in its completion.

- Using the original documents provided by Applicant as the basis of documentary evidence, Front line employee completes the “Individual Risk Assessment Form” Form B within 24 hours, going through the check list step-by-step & signing next to each step to indicate that staff has indeed diligently processed each of these steps.

Whenever necessary, Front line will have made note on discoveries and observations in the remark column of Form B.

- Upon completion of Form B, staff will submit the Form B, Form A and the verified/sighted CDD documents to the Compliance Officer or Manager

- Compliance officer will validate that Form B has been diligently processed by staff, and also assess the level of money laundering / terrorist financing risk that the Applicant by adding up the points and provide a risk rating of low, medium or high.

- If the risk rating is low or medium the Compliance Officer or Manager will sign off on the Form B.

- If Compliance Officer or the Manager is not satisfied that the application warrant an outright approval, he can either decline/reject the application (in which case he will tick in the box “Application Declined” and sign below it. For all applications with risk rating of high, the case must be referred to a Director for approval.) Compliance Officer or the Manager will then approach Director and senior management for advice and review of the matter. The outcome of this is either rejected or approved by the Director and such approval or rejection should be signed by Director on Form B.

- If application is rejected, the Compliance officer must consider filing a STR.

- If application is approved, Front line employee will enter data into our computerised system to create a new customer account.

The computer system auto-assigned "Customer Number" will be filled into the required field of the Form B "Assigned Customer No.".

- The applicant has successfully completed all application processes and his/her customer account is now setup and ready to be used for remittance transaction.

- Scanned images of all applicant's documents such as identity document, proof of address are uploaded to and linked to the customer record in our computer system.

- Paper copy of applicant CDD documents, as well as Form A & Form B are also filed in paper folder for record keeping.

6.8.3 Additionally procedure for "Politically Exposed Person" (PEP)

The Company has taken a risk based approach for ascertaining PEPs. Most of our business markets are focused on foreign migrant workers as our main clientele. Therefore, it is very unlikely that a domestic worker and the beneficiary receiving the sender's wages would be classified as a PEPs.
Therefore, in the following situations screening [UN sanction list, OFAC, Dfat, MAS list] should be performed to ascertain PEP status:

- an individual requesting for transaction $5000 and above
- an individual informs the Frontline employee that he is a government official
- an individual provides an embassy or consulate identification card

For PEPs applicants and transactions, the risk assess classification will automatically be rated as High Risk which require EDD and Senior Management approval for each transaction.

- Upon applicant's indication or employee determination (through screening) that this is a case of "PEP", the application shall be referred to the compliance officer for further action.

- Compliance officer may interview the applicant to gather further information to better determine if this is indeed a "PEP" case and include among his investigation, position & seniority in the organ of public service, research on the hierarchical structure of such service (as depending on the country involved, title can be misleading)

- Compliance officer will also interview "PEP" case to determine source of fund. As such interview and investigation are delicate, Compliance officer has to exercise care and discretion. Compliance officer may further request proof of source of fund from applicant.

- Compliance officer shall forward the investigation findings to the Director for final approval of account opening.

- Even if senior management is to approve of the account opening, the applicant will be immediately and permanently placed on "(Isend's) Customer Watch List". This customer will be closely monitored. Each transaction will be scrutinised. In particular, the size of transaction, beneficiaries & pattern of transaction will be closely tracked and monitored. Additionally, each transaction will require senior management approval. A copy of the ***Customer Watch List*** *is attached is the appendices*.

6.9 Identification requirements for Corporate business entities

With respect to each corporate entity, the following information must be obtained.

(i) The name of the company and the name of the client, if a company representative;
(ii) The jurisdiction in which it was incorporated;
(iii) The date on which it was incorporated;
(iv) The government-issued identification number;
(v) The purpose of incorporation;
(vi) The name of all shareholders holding more than 10% of the shares (or major shareholder), name of beneficial owners if their names are not listed as shareholders and names of effective controllers;
(vii) The names of the director(s);
(viii) The name of the company secretary(s) (if any have been appointed);
(ix) The location of the registered office;
(x) The primary mailing address;
(xi) The primary trading address (if applicable) and the location where its trading activities are generally carried out;
(xii) Whether the company is subject to regulation and, if so, the name of the regulator (this applies to agents and financial institutions acting as an intermediary)
(xiii) The name and address of the registered agent (if applicable);

6.9.1 Verification procedure for corporate entities

With respect to each corporate entity, the following verification procedures must be carried out by obtaining:

(i) Memorandum & Articles of Association (or equivalent constitutional documentation, i.e. by-laws);
(ii) Certificate of Incorporation;

(iii) Copy of registers of members, directors and company secretary; (Point (i) to (iii) can be addressed by obtaining a business search report issued by a government authority, example: ACRA or Bizfile Report for Singapore entities)
(iv) Identification documentation for each:
  (a) director, and
  (b) shareholder holding 10% or more of the shares of the company or from a majority shareholder and for each beneficial owner and controller;
(v) a resolution showing the specimen signatures of each of the directors;
(vi) a signed director's statement as to the nature of the company's business, if applicable;
(vii) If, and only where, the company is the client, an authorization document to enter the business relationship with the Company, i.e. Power of Attorney or board resolution;
(viii) Only where the company is the client, identification documents of the person authorised to represent the company in its dealing with the Company;
(ix) For complex structures with multiple layers of beneficial ownership, an Organization Structure Chart should be provided.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity. We may use the following non-documentary methods of verifying identity (for individuals and corporates):

- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source.

- Checking references with other financial institutions; or

- Obtaining a financial statement.

7. CORPORATE ACCOUNT OPENING PROCEDURE

This serves to document the CDD procedures that have to be conducted on a business entity or organisation applying to open an account with the Company so as to facilitates remittance transaction. It is important to note that what is

detailed here pertains to account opening only. Corporate account opening refers to request by a business entity (be it publicly listed, limited liability, partnership, limited partnership, limited liability partnership), organisation (such as government agencies) or financial institutions, for the setting up of a customer account with the Company for the purpose of remitting funds.

7.1. The "Corporate Account Opening Application Form" Form C

The first step to establishment of this relationship between a customer and the Company is the completion of the Account opening application **Form C**.

Form C is designed to allow us to gather information that is required for CDD, identification and verification procedures, profiling and risk assessment of the individual in relation to ML/TF.

Therefore, all fields of this form MUST be completed. Where certain fields are not applicable (for example, if a personnel does not have Alias), it must be filled with the abbreviation "NA" which stands for Not Applicable.

7.2 Front line account opening CDD procedures for Corporate Customer

<u>Applicant 's Identity Verification</u>

- Applicant complete "Corporate Account Opening Application Form" Form C & prepared original ACRA company profile or equivalent, original letter of authorisation, verified/sighted photocopy of identity document of directors, shareholders/partners, authorised persons, or sole-proprietor as prescribed in this Policy.

- Part 1 of the Form C to fill in the Applicant's name and Business Registration Number and the required customer's information.

- Front line employee to make an appointment & visit applicant's business office (also remind customer that original identity document be made available for verification against photocopy. Additionally, a person with executive authority that will be signing the application form as well as appointed authorised personnel must be present in-person (if the authorised persons are not present, the authorized person's identification and proof of address documents must be certified and verified by a recognized professional such as a lawyer, notary, commissioner of oath or chartered accountant).

- Front line employee prepares a copy of "Corporate Risk Assessment Form" Form B using that as the tool to systematically perform CDD and Risk Assessment on the Applicant.

- Front line employee must fill in the "Application Ref No." in Form C.

As applicant is currently not a customer, he/she does not have a customer number. Therefore, for the purpose of tracking the account opening application, the applicant is assigned a unique "Application Ref No", which is used to track this application and shall appear on all documents and forms related to this application. This facilitates tracking and cross-referencing.

"Application Ref No" is assigned sequentially, with the next applicant being assigned the next number in the sequence.

- Front line employee must ensure that all fields are completed in the Form C. Fields that are not relevant /applicable to the applicant should be filled with "NA".

  If Applicant is unable to complete the form because he/she does not understand what is required, staff is to explain and guide applicant in its completion.

- Using the original documents provided by Applicant as the basis of documentary evidence, Front line employee must work through the "Corporate Risk Assessment Form" Form B, going through the check list step-by-step & signing next to each step to indicate that staff has indeed diligently processed each of these steps. A copy of the Corporate Risk Assessment Form is attached in the Appendices.

  Whenever necessary, Front line employee will make note on discoveries and observations in the remark column of Form B.

- Completed form Form C will be signed by Applicant's corporate officers vested with executive authority in the presence of our Front-line employee.

- Front line employee will identify and verify that a) corporate officer with executive authority signing the application form b) authorised persons; looks the same as the photograph in their **Original Identity Document** and also check to ensure that document has not expired.

If Front line employee is unable to perform identification and verification as required in this Policy, the Account Opening Application will be rejected.

- Front line employee verify that signature on original copy of letter of appointment of “authorised persons” is the same as that of the corporate officer signing the application form

- Authorised persons must sign Form C in the presence of our employees. This will be the specimen signature that will be used to validate remittance transaction that are handled by authorised persons.(if the authorised persons are not present, the authorized person’s identification and proof of address documents must be certified and verified by a recognized professional such as a lawyer, notary, commissioner of oath or chartered accountant and the authorized persons must sign on the verified identification documents to be used as specimen signatures for validating transactions)

- Front line employee verify photocopy against original of identity document and other documents required such as phone bills etc.

- Front line employee leaves customer premise with all forms and risk assessment checklist as well as original ACRA company profile, original Letter of appointment of authorised persons and verified photocopy of identity documents.

- Front line employee submits all documents and completed Form C & Form B to Compliance Officer or Manager.

- Compliance officer will validate that Form B had been diligently processed by staff, and also provide a score and risk rating in relation to money laundering / terrorist financing risk that the Applicant may pose.

- If the applicant risk assessment is low or medium risk, Compliance Officer and Manager will then sign off on the Form B.

- If the applicant risk assessment is high risk the application should be reviewed by the Director, the Compliance Officer or Manager will then tick the box “escalated to Senior Management” and sign below it. He will then approach the Director for advice and review of the matter. The outcome of this is either rejected or approved by the Director.

- If application is rejected, Front line employee will inform applicant, and file the rejected applicant’s Form C & Form B in the “Account Application Declined” folder Folder ID: Y

- If application is approved, an employee will enter data into our computerised system to create a new customer account.

The computer system auto-assigned "Customer Number" will be filled into "Customer ID No." field in From C.

- The applicant has successfully completed all application processes and its customer account is now setup and ready to be used for remittance transaction.

- Verified scanned images of all applicant's documents such as identity document, proof of address are uploaded to and linked to the customer record in our computer system.

- Paper copy of applicant document as well as Form C & Form B are also filed in paper folder Z as part of our record keeping practices.

7.3 Additionally procedure for case of "Politically Exposed Person" (PEP)

Same as above "Account Opening for Individual" please refer paragraph 6.8.3.

7.4 When applicant is a Government entity

Upon applicant's indication that they are a Singapore government entity, the application shall be referred to the compliance officer for further action

- Applicant is requested to provide document to confirm that it is a government entity

- Upon compliance officer satisfaction that the applicant is indeed a government entity, the applicant shall be permitted to omit some of the fields in the Application form, example: Beneficial Owner details , but fields omitted shall be marked "NA" (Not Applicable). If the Company is satisfied that the applicant is a government entity posing low risk, simplified CDD may be applied in such circumstances.

- Notwithstanding the above, letter of authorisation and appointment is still required to establish that the person is an authorised person(s) of the government establishment.

- Applicant who are Singapore government entities may choose not to divulge information. But this relaxation of procedure refers to information gathering, but not measures necessary for positive identification and verification of its personnel involved in the application and transaction.

- Therefore the identity of the authorised person(s) as well as the person with executive authority to authorise the application and the appointment of authorised person(s) must still be determined. Identity document and specimen signature of them must be kept on file.

7.5 Waiver of the need to furnish information on Beneficial owner (simplified CDD)

When applicant is a Singapore or foreign government entity; an Entity listed on Singapore or foreign stock exchange; Financial Institution (other than a holder of a money changer's licence or a holder of a remittance licence); Investment vehicles managed by Financial Institution; the case shall be referred to a compliance officer for further processing.

- Applicant that are any of the above may be granted waiver of the need to furnish beneficial owners information provided that;

a) An entity listed on a foreign stock exchange is subjected to regulatory disclosure requirement that meet internationally accepted standards;

b) The financial institution is supervised by Monetary Authority of Singapore (MAS);

c) The financial institution is NOT a holder of a money changer's licence or a holder of a remittance licence granted by MAS (unless otherwise notified by MAS);

d) A foreign registered and regulated financial institution that is subject to and supervised for AML/CTF compliance that meet FATF standard;

e) An investment vehicle managed by Singapore registered financial institution that are supervised Monetary Authority of Singapore;

f) An investment vehicle managed by foreign registered financial institution that is subject to and supervised for AML/CTF compliance that meet FATF standard.

- For the case of a) and f), compliance officer must complete Form B (Risk Assessment Form for corporate entity) and is satisfied that the risk assessment is low risk as such allow simplified CDD.

Conversely, notwithstanding the meeting of the above condition of waiver, if Compliance officer has reason to suspect that the applicant may pose AML/CTF risk, compliance officer is required to document the basis of withdrawal of waiver and the company must conduct full CDD or EDD on the applicant.

7.6 Confidentiality

Form A, B, C and D are highly-confidential. This confidentiality applies to both the blank form and the completed form. It should not be shown or shared with customer or staff that are not supposed to be handling such Forms.

With the exception of government agencies involved in AML/CTF, such Forms must not be shared or made accessible to outside parties without senior management consent.

8. CDD DOCUMENTATION IN FOREIGN LANGUAGE

In the event that CDD documents provided are in a foreign language, they are to be translated to English by an employee. All records maintained should be in English language only. The employee translating the document must provide the following information on the document:

a. Full name of employee
b. Designation of employee
c. Date of translation

9. GUIDELINES FOR EMPLOYEES VERIFYING ORIGINAL DOCUMENTS

When original identification and supporting documents are verified by an employee, or qualified persons the copies retained must have been duly certified by the person sighting the original document.

The employee must certify on the face of the document:

(a) Name of employee sighting the document;
(b) that he or she has sighted and compared the original document;
(c) the designation;
(d) the signature of the employee sighting the document; and
(e) date.

Example: I hereby confirm that I have sighted and compared the original document and this is an accurate copy of the original document.
Name:_____
Designation:_____
Company:_____
Signature:_____
Date:_____

10. LACK OF IDENTIFICATION AND VERIFICATION

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following:
(1) not open an account;
(2) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity;
(3) close an account after attempts to verify customer's identity fail; and
(4) determine whether it is necessary to file a STR in accordance with applicable laws and regulations.

11. SCREENING

- The Company's system must include the Consolidated UN Security Council List, OFAC, DFAT, MAS Alert and Controlled Lists, First Schedule of Terrorism (Suppressing of Financing) Act List ("TSOFA")
- Database Screening System (Examples: World Check, Factiva, Dow Jones, Accuity.)
- Internet searches

Each customer and beneficiary name is entered into the Company's system and each name is screened against the UN Lists and MAS Controlled and Alert Lists and TSOFA list. If a hit is determined, the case must be escalated to the compliance officer and senior management for further analysis and no remittance transactions are allowed without Director or Manager approval.

When we receive notice that a government agency has issued a list of known suspected terrorists or a controlled list consisting of sanction persons and entities, the Compliance Officer must conduct sample screening by entering a few selected blacklisted names from the government issued list into the Company's system and database screening system to ensure these names are captured by the both systems. These sampling must be documented and dated for regulatory audit purposes.

The Company is taking a risk based approach should run each customer (or beneficiary) name through a database screening system (Accuity, Dow Jones, Factiva, World Check) to ascertain PEP status and for any adverse news (financial crimes, litigation, corruption, terrorism, bankruptcy) or sanction matches. Database screening must be done for the following situations:

a. Suspicious behavior is detected
b. High Risk rating
c. Corporate Account Opening
d. A hit notification from the Company's system
e. Onboarding a Financial Institution, Intermediary or Agent
f. High Risk Periodic Review

All screening reports in relation to false and positive hits must be documented and kept in file.

11.1 Name Hits

All hits alerted by the Company's system and database screening must be investigated to ascertain if they are either false positive or true hits.

Compliance Officer should review the following information on the screening report and make a comparison with the customer information on file and conclude if the hit on the person is considered a true hit or a false positive. Once the review is completed and recorded into the Customer Watch List Register, and the Director or Manager must make a decision to either file a STR or document the reason for not filing a STR.

Compare the following information on file against Screening Report to ascertain true or false name hit:

- Full name (any differences?)
- Date of Birth (any differences?)
- Country of Birth
- Province or State of Birth (Note: The Province is important, example born in Riau Indonesia on file records but born in Bandung, Java, Indonesia dispute having the same name may not be the same person)
- Current location
- Status of Person: Example in prison since 2016, therefore the customer cannot be the same person as such a false hit.
- Compare photograph with screening report, if available.
- Contact screening provider company to provide more information or clarification.

12. SOURCE OF FUNDS

Identifying the source of funds requires that information about the origin of the funds to be remitted to another party. The customer must provide the information on source of funds in the Individual Account Opening Application (Form A) or for large transactions the customer must complete the ***Declaration of Fund Form (Form D)***. Both copies of the forms are attached in the Appendices.
Where appropriate, supporting evidence must be requested to either clarify or validate the information given by the customer. If, for example, a customer claims that the source of fund is from work remuneration, then a certified or sighted copy of the pay slip should be requested to evidence the claim.

13. RISK ASSESSMENTS AND RATINGS

Once the customer has been identified and verified, a process must be carried out to determine a risk rating. The risk rating considers various risk factors before arriving at a final conclusion on the overall risk being posed by the client and the proposed transactions. The risk assessment is conducted during every individual and corporate account opening and during periodic review or whenever a high risk factor is detected. The exercise is done by way of an ***Individual/Corporate Risk Assessment Form (Form B)*** with scores attached to each answer. The score is tallied and depending on which band the customer belong to, the customer is classified accordingly as low, medium or high risk. This Form must be completed by any employee of the Company; however, the Compliance Officer will sign off after reviewing the risk assessments. A copy of the Individual/Corporate Account Opening Risk Assessment (Form B) are attached in the Appendices.

<u>Low Risk Rating – below 15 points</u>
Employee must complete the Individual/Corporate Risk Assessment Form (Form B) and tallies the score and classify the customer as low or medium risk.

1. Compliance Officer to review Risk Assessment Form and signs off.
2. Account may be opened and transactions may proceed.
3. Manager to sign off on the Risk Assessment.
4. Low to Medium risk Accounts to be reviewed once every two years.

<u>High Risk Rating – 15 points and above</u>

1. Employee completes the Individual/Corporate Risk Assessment Form (Form B) and tallies the score and classify the customer as high risk.

2. No Account opening and no transactions can take place if for Corporate Customer.
3. Compliance Officer to review Risk Assessment and conduct Enhance Due Diligence and provide comments, recommendations and signs off.
4. Director will review the Enhance Due Diligence results and provide approval or rejection for the new account, if for individuals where transactions has taken place Director must consider filing a STR or stop transactions
5. Director to sign off on the Risk Assessment and provide comments, if any.
6. If approved, the Account may be opened and transactions may proceed.
7. This Account must reviewed annually.

14. POLITICALLY EXPOSED PERSONS (PEP)

Account opening or transactions involving PEPs must be treated as "high" risk" and rated so in the Individual Account Opening Application Form (Form A) and ECDD should be performed, the Company may choose to adopt a risk-based approach in determining whether to perform ECDD for:

(a) Domestic politically exposed persons, their families and close associates;

(b) International organization which consist of politically exposed persons, their family members and close associates.

(c) Politically exposed persons who have stepped down from their prominent public function. Taking into consideration the level of influence such persons may continue to exercise after stepping down from their prominent public functions, their family members.

Please note PEP is a person who is, or who has been, entrusted with prominent public functions, such as:

(i) heads of state or government,
(ii) senior politicians,
(iii) senior civil servants,
(iv) senior judicial officials,
(v) senior military officials,
(vi) senior public party officials, and
(vii) senior executives of public organizations.

The term "PEP" also extends to family members or close associates of such people.

The concern placed in dealing with PEPs lies with the possibility of a person abusing their public powers for their own illicit enrichment, especially in jurisdictions where corruption is rampant, and then either directly or via a confidant placing those monies in the financial system for their own benefit.

Hence, the Company should have, in addition to their respective client due diligence process, a risk management framework (continuous monitoring and annual reviews of account) to determine whether current or new customers are PEPs, bearing in mind that a customer may become a PEP during the course of their business relationship with the Company.
In establishing whether or not the customer is a PEP, the Company should gather sufficient information from the customer and from publicly / privately available resources and perform database screening on the individual's name.

Where the Company is considering entering into, or continuing a business relationship with a PEP, or someone who has become a PEP since the start of the customer relationship, this shall be reviewed and signed off by compliance officer, after which will be subjected to the approval of the Director.

15. ENHANCED DUE DILIGENCE (EDD)

For any client with a risk rating of high it is necessary to conduct EDD. Customers may be rated high for a variety of factors, which might include individual names flagged via searches conducted through the screening data bases, money sent to a country highlighted as a high money laundering risk, business activity such as gold mining and casino operations may push the customer into high risk category.

Example of some factors which triggers mandatory EDD:

a. Sender or beneficiary are PEPs (database screening)
b. Name match against screening results, including partial match
c. Remitting to a High-risk jurisdiction (non-FATF compliant)
d. Applicant conducting high risk business activities
e Higher transaction threshold

Examples of High Risk Business:

- Casino and gambling related
- Mineral mining (gemstones, gold and silver)
- Arms and weapons related
- Online gambling
- Bitcoin mining
- Tobacco
- Nightclubs and adult entertainment

There is no one shoe fit all formula for EDD, there is little direct regulatory guidance as to what constitutes EDD.
Where the Company is required to perform ECDD, it shall either directly from the client or, if available, through publicly available sources, obtain any of the following additional information and / or documentation from the client or from third parties providers, to the satisfaction of the Compliance Officer.

(a) Database screening and internet searches on the high risk customer;
(b) Obtain more evidence tracing the origin of funds and customer to sign the Declaration of Funds Form;
(c) Conduct CDD, identification and verification on the beneficiary and the reason for beneficiary to receive the fund;
(d) Obtain supporting documents justifying the transactions;
(e) Any other measures to mitigate the identified risk.

16. CROSS BORDER REMITTANCE BELOW SGD$1500

Before effecting a remittance, the Company must perform full CDD, identification and verification procedures as required in this Policy in relation to the sender and should include in the payment instruction the following information:

a. Name of sender
b. Sender's account number or unique transaction reference number
c. Name of the recipient beneficiary
d. Recipient beneficiary's account number or unique transaction reference number
e. Relationship between parties & purpose

The Company may choose to include only (c) Name of the recipient beneficiary (d) Recipient beneficiary's account number or unique transaction reference number provided the unique transaction number will permit the transaction to be traced back to the sender and recipient beneficiary. In addition, the Company must be able to provide the above information (a) to (d) immediately upon request by law enforcement authorities, intermediary institution in Singapore, Monetary Authority of Singapore or other relevant authorities in Singapore and the beneficiary institution.

17. CROSS BORDER REMITTANCE EXCEEDING SGD$1499 AND BATCH FILE TRANSMISSION

Before effecting a remittance, the Company must perform full CDD, identification and verification procedures as required in this Policy in relation to the (i) sender and (ii) beneficiaries and include in the payment instruction the following information:

a. Name of sender
b. Sender's account number or unique transaction reference number
c. Name of the recipient beneficiary
d. Recipient beneficiary's account number or unique transaction reference number
e. Beneficiary ID [inward cash collection]
f. If beneficiary is corporate entity; current & valid business registry for record
g. Residential Address of sender, and if the sender is an entity the registered or business address
h. Identification number, or if the sender is an entity the incorporation/business number; or
i. Date and place of birth
j. Sender to complete Declaration of Fund Form
k. Sanction name check/ screening

The Company may choose to include only (c) Name of the recipient beneficiary (d) Recipient beneficiary's account number or unique transaction reference number provided the unique transaction number will permit the transaction to be traced back to the sender and recipient beneficiary. In addition, the Company must be able to provide the above information (a) to (d) immediately upon request by law enforcement authorities, intermediary institution in Singapore, Monetary Authority of Singapore or other relevant authorities in Singapore and the beneficiary institution.

18. LARGE AMOUNT REMITTANCE ABOVE SGD$5000

Full CDD, including identification and verification procedures as required in this Policy. EDD must be performed until the Company is reasonably satisfied that the proposed transaction is explained with supporting documents and each of such transactions must be recorded into a Large Transaction Register. A copy of the **Large Transaction Register** is attached in the Appendices.

The Large Transaction Register must include the following information:
a. Name of Sender and beneficiary
b. Identification number for both parties
c. Reason for Transaction
d. Source of Fund

e. Destination of Fund (Country)
f. Enter Risk Rating after the completion of the Risk Assessment (if the transaction is fully supported by documents and the parties are not PEPs such logical transactions should not be rated High Risk).
g. Explain EDD conducted
h. Compliance Officer name and sign
i. Name of Director approving the Large Transaction (if High Risk)
j. Date of Remittance

These are some examples of EDD action, as may be appropriate includes:
a. Obtaining documents evidencing source of funds
b. Parties to complete a Declaration of Fund
c. Sighting Trade invoices
d. Document evidencing proof of purchases
e. Agreement of sales or contract for employment
f. Verification of Income slips and tax return forms
h. Verification CPF contribution letter
g. Obtaining a Bank statement or a reference letter

19. PROVISION OF REMITTANCE SERVICES TO FINANCIAL INSTITUTIONS OR THROUGH FINANCIAL INSTITUTIONS AND AGENCY AGREEMENTS

The Company must perform CDD on each Financial Institution (FI) or Agent and perform the following measures:

a. The FI or Agent must complete a AML/KYC Questionnaire (on the Company letter head) given by the Company.
b. Screen the FI and Agent names on database screening system for sanctions and adverse media.
c. Consider its business activities, reputation and jurisdiction of operations to ensure the FI is not a shell financial institution.
d. Written confirmation that the FI and Agent has AML/CFT policies and procedures in place.
e. Request for a copy of the FI or Agent's AML/CFT Policy or at least a copy of the AML/CFT Manual's index page showing the policies and procedures chapters.
f. Assess whether the jurisdiction where the FI or Agent is located is a FATF compliant country.
g. Documentary evidence indicating that the FI or Agent is supervised or regulated by a competent authority.
h. Prior to business relationships, enter into service agreement contract that reflects AML/CFT obligations of each parties

i. Letter of undertakings from the financial institutions stating out that implementation of full AML/CFT obligations and procedures are in place
j. Letter of undertaking from the financial institutions ensuring that they do not provide remittance services to a shell company and prohibit the account opening for a shell company.
k. AML Questionnaire to be completed by the financial institutions with the letterhead and signed by relevant person in authority
l. Conduct risk assessment prior to business relationship to assess the risks it poses to the Company

Each FI and Agent should be assessed individually by the Compliance Office and Senior Management by completing a **Wolfsberg AML Questionnaire for FIs and Agents**, classifying if the FI/ Agent poise risk to business or not.

A list/register of Financial Institutions and Agents must be maintained and updated by the Company. A copy of the FI and Agent Register is attached in the Appendices.

20. ONGOING MONITORING FOR SUSPICIOUS ACTIVITIES

We will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business. Compliance officer/Money Laundering Reporting Officer (MLRO) will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

Events (Red Flags) that may trigger the need to file Suspicious Transaction Report (STR)

20.1 Ongoing Monitoring

The Compliance Officer should conduct periodic review for all accounts in accordance to the risk rating.

b. Once annually for High Risk accounts/clients
c. Once every two years for Medium Risk accounts/clients
d. Once every three years for Low Risk accounts/clients
e. Immediate EDD review if Low risk account/clients upgraded to High
f. Whenever a suspicion is detected that potentially may push the account to High Risk or a STR to be filed.

In addition to the above, certain customers require ongoing monitoring and the Compliance Officer should complete a Customer Watch Report Form and record in the Customer Watch List Register. The Register must contain the following information:
(a) name of client and/or beneficiary
(b) reason to be placed under Customer Watch List and Report
(c) Ongoing Action needed
(d) name of officer inserting the information
(e) Compliance comments
(f) follow up action

Examples:

a. Frequent large or small remittances from the same sender
b. Multiple senders to the same beneficiaries
c. Suspicion detected
d. STR filed
e. Hit for adverse media
f. Similar transaction pattern between customers
g. Sudden large remittance amount
h. Customer screening following fuzzy logic, name sounding like,
i. Conservative % name check for high risk country
j. Compliance & threshold reporting measure; where more than allowed limit of transaction is put in auto block, requires Compliance to approve after conducting CDD/ EDD

21. RED FLAGS

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

<u>Customers – Insufficient or Suspicious Information</u>

- Provides unusual or suspicious identification documents that cannot be readily verified.
- Reluctant to provide complete information about nature and purpose of business, business relationships, anticipated account activity, officers and directors or business location.
- Withdraw account opening application when we persist in asking applicant for complete information that applicant is apparently withholding.
- Refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect.

- Background is questionable or differs from expectations based on business activities.
- Customer with no discernable reason for using the firm's service.

Efforts to Avoid Reporting and Record keeping

- Reluctant to provide information needed to file reports or fails to proceed with transaction.
- Tries to persuade an employee not to file required reports or not to maintain required records.
- "Structures" deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or record keeping requirements.
- Unusual concern with the firm's compliance with government reporting requirements and firm's AML/CFT policies.

Certain Funds Transfer Activities

- Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent business reason.
- Many small, incoming or outgoing wire transfers or remittance inconsistent with customer's business or history.
- Remittance that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.

Other Suspicious Characteristics

- Company has no business, no revenues and no product.
- Company has experienced frequent or continuous changes in its business structure.
- Company undergoes frequent material changes in business strategy or its line of business.

Activity Inconsistent With Business

- Transactions patterns show a sudden change inconsistent with normal activities.
- Unusual transfers of funds or journal entries among accounts without any apparent business purpose.
- Maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
- Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.

Other Suspicious Customer Activity

- Unexplained high level of account activity
- Payment by third-party check or money transfer without an apparent connection to the customer.
- Payments to third-party without apparent connection to customer.

22. RESPONDING TO RED FLAGS AND SUSPICIOUS ACTIVITY

When an employee of the firm detects any red flag, or other activity that may be suspicious, he or she will notify the MLRO. Under the direction of the MLRO, the firm will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, freezing the account and/or filing a STR.
Analysis and result of the investigation is documented in the "Suspicious Transaction Report Form" Form ID: E.

Our "***Suspicious Transaction Report Form***" Form E serves as the key document that record all our investigation, analysis and findings on each case of suspicious transaction. Each report has a unique STR Number that uniquely track each case investigated. This report reference investigated transaction through the unique transaction reference number and Customer name and number. Regardless of whether the investigation result warrant filing of the STR with STROLLS, each STR is archived for future reference allowing us to build up an informative profile on each customer.

And STR investigation does not necessary escalate to filing of the STR with the STROLLS. Upon investigation, if the MLRO and senior management has reason to believe that filing with STRO is not warranted, the reason leading to this conclusion is also documented in Form E. If a joint decision between the Director and MLRO cannot be reached, the Director shall have final determination. However the MLRO must document that such a decision has taken place. The basis for not submitting a formal STR to STROLLS for any suspicious transactions escalated by any employee should be properly substantiated and documented.

Even if filing of STROLLS is not necessary, the MLRO or senior management may decide to place the customer on our internal "**Customer Watch list"**. Customer on this list are closely monitored and if evidence gathered from future transactions give reason to believe that the customer is engaged in money laundering activities, then the case will be escalated to filing of STR with STROLLS. Prior to listing the customer on this list, a "***Customer Watch List Register" Form F*** is created, which detail reason for placing customer on our

watch list. Conversely, reason for removing customer from this list are also documented.

The Money Laundering Reporting Officer (MLRO) is the single point of contact within the organization for all cases of suspicion of money laundering that employees should refer to. MLRO is also responsible for filing of STR with STROLLS.

Before an STR is filed with STROLLS and a copy forwarded to MAS, our senior management must review and sign off on the report.

23. SUSPICIOUS TRANSACTION REPORTING

Filing a STR

The Company will file a STR with STROLL CAD for any transactions where we know, suspect or have reason to suspect:

(1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade MAS law or regulation or to avoid any transaction reporting requirement under MAS law or regulation;

(2) the transaction is designed, whether through structuring or otherwise, to evade any requirements of the MAS regulations;

(3) the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or

(4) the transaction involves the use of the firm to facilitate criminal activity.

We will also file a STR and notify MAS in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes.

We may file a voluntary STR for any suspicious transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported by us under the MAS rule. It is our policy that all STR will be reported regularly to the Board of Directors and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the STR.

We will report suspicious transactions by completing a STR to STROLL, and we will collect and maintain supporting documentation as required by the MAS regulations. We must file a STR no later than 14 calendar days after the date of the initial detection of the facts that constitute a basis for filing a STR.

We will retain copies of any STR filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the STR. We will identify and maintain supporting documentation and make such information available to MAS, any other appropriate law enforcement agencies, or STROLLs upon request.
We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the MAS regulations.

24. RECORD KEEPING

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all CDD, identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the account is closed.

24.1 AML/CFT Recordkeeping

Our Compliance Officer will be responsible for ensuring that AML/CFT records are maintained properly and that STR are filed as required.

In addition, as part of our AML/CFT policy, our firm will create and maintain STR and relevant documentation on customer identity and verification and funds and a STR Register. We will maintain STR and their accompanying documentation for at least five years. We will keep other documents per existing MAS and other recordkeeping requirements.

25. NO WARNINGS OR TIPPING-OFF TO ALERT THE SUSPICIOUS CUSTOMER

Making any disclosure that is likely to prejudice an investigation to the customer or any other related party is an offence when such investigation is known to the employee or the employee has reasonable grounds to suspect that an investigation is underway.

There is a tipping off offence punishable by the authorities, a fine not exceeding $30,000, or imprisonment for a term not exceeding three years, or both.

26. COMPLIANCE FUNCTION

The Company must appoint a Compliance Officer/MLRO with sufficient authority to have access to the senior management and the compliance officer must be suitably qualified to develop AML/CFT policies and procedures. In addition, the Compliance function must be provided with adequate resources and given timely access to all customer records and relevant information which the Compliance Officer may require to discharge his functions.

27. EMPLOYEE HIRING

The Company shall have in place screening procedures to ensure high standards when hiring employees and appointing officers.

1. Ensure the employee is fit and proper for the roles and responsibilities that will be assigned to the individual
2. Screening to ensure the employee does not have high risk or adverse media hit
3. Individual background check for all new employees

All results of screenings and background checks must be recorded and documented in accordance to the Human Resource (HR)'s policy and procedures.

28. TRAINING PROGRAMS

We will develop ongoing employee training under the leadership of the compliance officer and senior management. Our training will occur on at least on quarterly basis. It will be based on our firm's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law.

Our training will include, at a minimum:

(1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties;
(2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of STR);
(3) what employees' roles are in the firm's compliance efforts and how to perform them;
(4) the firm's record retention policy; and
(5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the MAS.

We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. We will maintain records to show the persons trained, the dates of training and the subject matter of their training.

29. AUDIT

The audit of our AML/CFT readiness will be performed at least on annual basis by an independent third party. We will evaluate the qualifications of the independent third party to ensure they have a working knowledge of applicable requirements under the MAS and its implementing regulations. Independent Audit will be performed more frequently if circumstances warrant.

APPENDIX 1

FORM A: Individual Account Opening Application Form

iSend Pte Ltd

229 Mountbatten Road #03-01 Mountbatten Square Singapore 398007 Tel: _____Fax: _____

CUSTOMER ID NUMBER …….
DATE: ……

Sender Particulars:

Name:	ID no [NRIC/PP]#:	
Alian name if any;	Issued date:	Issued by:
Date of Birthday: [dd/mm/yy]	Expiry date:	Country:
Spouse name:	DOB:	
Father name:		
Address: Postal Code:		
Tel #:	Nationality:	
Occupation:	Company/ Employer Name:	
Position:	Nature of job:	
Source of Fund: ☐ Salary ☐ Business Profit ☐ Loan from _____ ☐ Others: _____		
Annual Salary: Annual no of transfer: Amount:		
Purpose of Remittance: ☐ Family Expenses ☐ Loan to Receiver ☐ Allowances ☐ Personal Purchase _____ ☐ Others: _____		
Occupation: Self Employed Company Name: Nature of Business: Company registration number:		
Source of Fund: ☐ Salary ☐ Business Profit ☐ company Loan _____ ☐ Others: _____		
Purpose of Remittance: ☐ Family Expenses ☐ Loan to Receiver ☐ Allowances ☐ Personal Purchase _____ ☐ Others: _____		

Type of Payment:

☐ **Cash** ☐ **Bank transfer:**

Receiver Particulars [CASH COLLECTION]:

Name:	Relationship:

Country:	Nationality:	
ID type:	ID number:	
Address:		Tel#:

Bank Details (for Bank to Bank Transaction):

Name:	Relationship:	
Country:	Nationality:	
ID type:	ID number:	
Address:		Tel#:
Account Name:		
Bank Name/ Branch:	Bank Account#:	

I confirm that the information provided in this Remittance Application Form to iSend Pte Ltd is true, complete and correct.
I declare that the funds for my remittance are not derived from any illegal activities, money laundering or terrorism financing.
I hereby confirm that to iSend Pte Ltd that my residing address is as stated above and I shall inform iSend Pte Ltd for any changes to my residing address.
I confirm that all above information provided are true and correct, and I shall be held responsible and agreed to be legally prosecuted for any falsified information.

_____
Customer's signature and date

Check list for documents: official purpose:

- ☐ ID copy verified with original & copy retained
- ☐ Address proof document verified with original & copy retained
- ☐ Source of fund document i.e. salary slip, bank statement, payroll letter verified
- ☐ for those self-employed, documents is collected
- ☐ for those working in high risk industry; two ID collected

APPENDIX 2

FORM B – Individual and Corporate Risk Assessment Form

Individual / Corporate Risk Assessment Form

1. This Form is to be completed by Frontline, or Compliance, or Manager for Individual and Corporate Customers.
2. Total Score of 15 and above will provide a High-Risk rating.

Application Ref No:	**Customer Name:**
Application Date:	

No	Risk Considerations	Yes/No	Score	Remarks
	Identification and Verification			
1	Individual Customer, Corporate Customer, Beneficial Owners, and Authorized Personnel ("Applicant") provided Original identity document for identification and verification process to be completed	Yes = 0 pts No = 15 pts		
2	Customer provided proof of address and a copy of the document is retained	Yes = 0 pts No = 5 pts		
3	Name & address matches what is furnished in application form?	Yes = 0 pts No = 5 pts		
4	Is the customer sending money on behalf for another person (other party)? If yes, refer to question 5.	Yes = 3 pts No = 0 pts		
5	Can this other party be identified and verified in accordance to the AML/CFT Policy?	Yes = 1 pts No = 3 pts		
	For Government Entity Only			
6	The entity is a Government entity (based on Internet searches, Dow Jones, Website) *for entity pretending to be a government entity, file STR	Yes = 0 pts No = 15 pts		
7	Authorized person requesting transaction is identified and verified per this Policy and the authority to act on behalf of the entity is verified?	Yes = 0 pts No = 10 pts		
8	Is there a reason to suspect the requested transaction may be unusual or suspicious?	Yes = 15 pts No = 0 pts		
	Geographical Concerns			
9	Is the customer from a high-risk jurisdiction? Or is the customer conducting business in a high-risk jurisdiction or conducting high-risk business? (High-risk countries are those FATF non-compliant country; High-risk business includes Casino, mining or arms industries)	Yes = 15 pts No = 0 pts		
10	Is the proposed transaction to a beneficiary to a high-risk country? Refer to resources from FATF and MAS.	Yes = 15 pts No = 0 pts		
11	Any parties from a sanction country or proposed transactions to a sanction country?	Yes = 15 pts No = 0 pts		
	Screening Adverse Media and PEPs			
12	Any adverse media alerts from screening system in iSend Pte Ltd's Remittance System relating to: (a) Terrorism-automatic High risk (b) AML-High Risk (c) Criminal Activities-High Risk (d) Others please specify_____(1 point)	(a)Yes = 15pts (b)Yes = 15pts (c)Yes = 15pts (d)Yes = 1pts No = 0 pts		
13	Screening report states applicant is a PEP (a) transaction below SGD$1000 (10 point) (b) transaction above SGD$1000 - High Risk	(a)Yes = 10pts (b)Yes = 15pts No = 0 pts		
	Source of Funds			
14	Is the source of funds reasonably explained?	Yes = 0 pts No = 5 pts		
	Transactions			

13	Amount of transaction is below SGD$1000	Yes = 1 pts No = 0 pts
14	Amount of transaction is between SGD$1000 to SGD$5000	Yes = 2 pts No = 0 pts
15	Amount of transaction is SGD$5000 and above	Yes = 3 pts No = 0 pts
	Suspicious Behavior	
16	Any suspicious behavior detected? If Yes please specify suspicious behavior:_____	Yes = 15 pts No = 0 pts

Customer Service Officer: _____(*insert name*) **Total Score**

Risk Rating **Low | High**

Reviewed by Compliance Manager: *(insert name)*

Compliance Remarks:

Signature & date: _____

_____

Approval by Director: *(insert name)*

Remarks for approval:

Signature & date: _____

_____

Rejected by Director: *(insert name)*

Remarks for rejection:

Signature & date: _____

_____

APPENDIX 3

FORM C – Corporate Application Form

Corporate Account Application Form [FORM C]

CUSTOMER ID NUMBER:……
Date: ……

Please complete all fields.

PART 1: BUSINESS INFORMATION			
Organisation Full name			
Business Registration Number (UEN)			
Registered Address			
Business Address			
Place and Date of Incorporation			
Form of Organisation	☐ Sole Proprietorship ☐ Company ☐ Limited Liability Partnership ☐ Financial Institution ☐ Partnership ☐ Others: _____		
Email address			
Website address			
Telephone (1)		Fax (1)	
Telephone (2)		Fax (2)	
Nature of Business			
Source of fund	☐ business ☐ Personal borrowing ☐ capital ☐ borrowing from Financial Institution ☐ Others:		
Head Office Location			
Branches or other Offices [if diff to HO]			

PART 2: REMITTANCE NEEDS			
Purpose of transaction:			
☐ Payment to suppliers	☐ Business Expansion	☐ Purchase operation equipment	
☐ Salary pay out to employees	☐ Others: _____		
Countries of remittance:			
☐ Malaysia	☐ Thailand	☐ Vietnam	☐ Australia

☐ Indonesia	☐ India	☐ Taiwan	☐ Others: _____
☐ Philippines	☐ China	☐ Japan	_____
Currency:			
☐ MYR (Ringgit)	☐ THB (Baht)	☐ VND (Dong)	☐ CNY (Yuan)
☐ IDR (Rupiah)	☐ INR (Rupee)	☐ NTD (Taiwan Dollar)	☐ Others: _____
☐ PHP (Peso)	☐ AUD(Australia Dollar)	☐ JPY (Yen)	_____

PART 3: DIRECTORS OR PARTNERS	
Please list down all the Directors as reflected in ACRA	
1.	Name as per NRIC/Passport:
	NRIC/FIN/Passport No.:
	Nationality:
	Email:
	Telephone:
2.	Name as per NRIC/Passport:
	NRIC/FIN/Passport No.:
	Nationality:
	Email:
	Telephone:
3.	Name as per NRIC/Passport:
	NRIC/FIN/Passport No.:
	Nationality:
	Email:
	Telephone:
4.	Name as per NRIC/Passport:
	NRIC/FIN/Passport No.:
	Nationality:
	Email:
	Telephone:
5.	Name as per NRIC/Passport:
	NRIC/FIN/Passport No.:
	Nationality:
	Email:
	Telephone:
6.	Name as per NRIC/Passport:
	NRIC/FIN/Passport No.:
	Nationality:

	Email:
	Telephone:

Pls submit documents duly confirming matching authority to undertake transaction on the behalf of the company.
Pls submit documents confirming Ultimate Beneficiary ownership along with below information;

PART 4: BENEFICIAL OWNERS	
1.	Name as per NRIC/Passport:
	NRIC/FIN/Passport No.:
	Nationality:
	Email:
	Telephone:
2.	Name as per NRIC/Passport:
	NRIC/FIN/Passport No.:
	Nationality:
	Email:
	Telephone:
3.	Name as per NRIC/Passport:
	NRIC/FIN/Passport No.:
	Nationality:
	Email:
	Telephone:
4.	Name as per NRIC/Passport:
	NRIC/FIN/Passport No.:
	Nationality:
	Email:
	Telephone:
5.	Name as per NRIC/Passport:
	NRIC/FIN/Passport No.:
	Nationality:
	Email:
	Telephone:

PART 5: OWNERSHIP AND CONTROL STRUCTURE

Please provide information of the ownership and control structure of your Organization by indicating the percentage of ownership by each party. For complicated structure of organization, kindly attach a diagram of ownership and shareholding.

PART 6: AUTHORIZED PERSONNEL		
Information of authorized personnel to act on behalf of your Organization in relation to remittance transactions.		
1.	Name as per NRIC/Passport:	Signature:
	NRIC/FIN/Passport No.:	
	Designation:	
	Nationality:	
	Email:	
	Telephone:	
2.	Name as per NRIC/Passport:	Signature:
	NRIC/FIN/Passport No.:	
	Designation:	
	Nationality:	
	Email:	
	Telephone:	
3.	Name as per NRIC/Passport:	Signature:
	NRIC/FIN/Passport No.:	
	Designation:	
	Nationality:	
	Email:	
	Telephone:	

4.	Name as per NRIC/Passport:	Signature:
	NRIC/FIN/Passport No.:	
	Designation:	
	Nationality:	
	Email:	
	Telephone:	

PART 7: ANTI MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM (AML&CFT)

1. We confirm that our remittance transactions are for lawful and legitimate business purpose and not for the illegal activities, including but not limited to money laundering and terrorism financing.	☐ Yes ☐ No
2. We confirm that our source of fund for the remittance are originated from lawful and legitimate business activities.	☐ Yes ☐ No
3. None of our Directors/Shareholders/Beneficial Owners/Authorized Personnel are Politically Exposed Person (PEP) or related to PEP. *If answer is "No", please specify which individual is PEP or related to PEP and the current designation of the individual:* *Name:* _____ *Designation:* _____ *Country:* _____	☐ Yes ☐ No

PART 8: DECLARATION

1. *We hereby confirm that all information provided in this form are true and correct.*
2. *We hereby grant consent to iSend Pte Ltd and their representatives and/or agents collecting, using and disclosing my personal data to provide me with remittance service.*
3. *If there are any changes to the information provided in this form, we will be responsible to inform iSend Pte Ltd for such changes.*
4. *We hereby confirm that all information provided are true & correct, and we agree for legal prosecution for any wrong & falsified information.*

Signature: ……. Name: _____ Date: _____	Signature: ……. Name: _____ Date: _____
Signature: ……. Name: _____ Date: _____	Company Stamp: ……. Date: _____

PART 9: DOCUMENTS REQUIRED
1. Company ACRA 2. NRIC/ PP of all Directors, Shareholders and Authorized Personnel 3. Authorization Letter or board resolution authoring director to undertake transaction 4. ____ 5. ____

Application received date: ……..
Application approved date: ……

APPENDIX 4

FORM D – Declaration Form

DECLARATION FORM FROM SENDER [FORM D]

I, with my identity as below:

Name	Ms/Mr/Mrs/ Dr/…/
NRIC#	
PP#	
Present Address	
Contact number	Transferred amount SGD …….

Hereby declare that my source of fund and purpose of the remittance are as the following:

Source of Fund	☐ Salary ☐ Business Profit ☐ Bonus from Employer ☐ Loan from _____ ☐ Others: _____
Nature of Work/ Employer/ Position Self EMPLOYED/ INDUSTRY	
Purpose of Remittance	☐ Family Expenses ☐ Purchase Property (House/Land/Car/_____) ☐ Savings ☐ Child's School Fee ☐ Others: _____

I hereby certify that above information are true and correct to the best of my knowledge.
I declare that the funds for remittance are not derived from any illegal activities, tax evasion, money laundering or terrorism financing.
I indemnify iSend Pte Ltd from any liabilities incurred for any wrong and incomplete information which may lead to any disturbance, undelivered, claims and litigation actions by any parties in relation to this remittance.
And, that iSend Pte Ltd and its management will not be liable for any declaration/statement I provided the company.

I shall be held responsible and agree to be prosecuted legally for providing any falsify information to the company or its authorised representative.

(Copy Customer's ID here)

…… in the premise of iSend Pte Ltd 229 Mountbatten Road #03-01 Mountbatten Square Singapore 398007
Signature / Date

APPENDIX 5

FORM E – Suspicious Transaction Report

Date: _____

Internal Reference: STR ref No. _____

☐ NATURAL PERSONS/ ☐ COMPANY PAYMENT

STR escalated by:	
Name of Personnel:	
Designation:	
Date of report escalation:	
Reason of suspicion:	*Partial name match* *Beneficiary from Sanction country* *Amount being received from Multiple senders* *Amount being sent to Multiple beneficiaries* *Small amount received in quite regular interval/ frequency* *PEP name matching* *Requested transfer amount not matching to earning;* *Requested transfer amount not as per principle nature of business* *……..* *……* *……*
Customer's Particulars	
Name:	
Alias/Alternative Names:	
NRIC/Passport No.:	
ID Issuing Country:	
Identification Type:	☐ NRIC ☐FIN ☐Passport ☐ If others, please state _____
Birth Date:	
Country of Birth:	
Gender:	
Nationality:	
Company Name	
Principle nature of business:	

Registered/ Residential Address:	
Contact No.:	
Occupation:	
Date when particulars were last updated (where available):	
Beneficiary Account information:	☐ account name……☐*number*.....☐ address…… ☐*amount* ..... ☐ contact details.
Relationship with Sender	

Suspicious Transaction(s)

Amount in SGD	**Amount in Foreign Currency**	**Date of Transaction**	**Source of Funds**	**Destination (for funds remitted)**
Example				

Internal Analysis and finding based on the reason(s) of suspicion:

(elaborate in detail)

Other relevant information (including any actions taken by the reporting licensee in response to the transaction):

A copy each of the following documents is attached with this report:

- Customer Identification Documents
- Relevant Documents Supporting the Suspicious Transactions
- Invoice of transactions

STR Investigated by *(name of personnel)*
STR filed to STRO *(Yes/No)*

Date of STR filed to STRO	*(insert date)*
If not filed to STRO, state the reason(s)	*(elaborate reason for not filing)*
Signature of Reporting Officer	*(signature of reporting personnel)*
Approved by Senior Management	*(signature of senior management)*

APPENDIX 6

FORM F - Customer Watch List

Customer Watch List

This list contains constantly updated listing of existing customers of iSend Pte Ltd for close monitoring. Customers on this list are not blacklisted and are allowed to continue with remittance transactions. However, customers on this watch list are required to be closely monitored as the remittance activities are raising attention but do not qualify to be reported as Suspicious Transaction or blacklisted. Compliance Officer should review the customers' remittance activities on this list and apply risk-based approach to review the remittance activities and if necessary, escalate to Senior Management approval.

No.	Customer No.	Customer Name	Beneficiary Name	Listed Date	Reason for Listing	Actions taken	Future Actions to Take
1							
2							
3							
4							
5							
6							
7							

APPENDIX 7

Wolfsberg AML Questionnaire

ISEND PARTNER DUE DILIGIENCE QUESTIONNAIRE

Financial Institution Name:	
Location (Country) : Location (Country):	

The questionnaire is required to be answered by Compliance Team. The Financial Institution/Correspondent agent will answer the questionnaire at an ultimate parent / head office & subsidiary level for which any branches would be considered covered by that parent/subsidiary DDQ. This questionnaire should cover only one Legal Entity . Each question in the DDQ will need to be addressed from the perspective of the LE and on behalf of all of its branches. If a response for the LE differed for one of its branches this needs to be highlighted and detail regarding this difference captured at the end of each subsection. If a branch business activity (products offered, client base etc.) is significantly different than its head office, the branch should complete a separate questionnaire.

No #	Question	Answer
1. ENTITY & OWNERSHIP		
1	Full Legal Name	
2	Append a list of branches which are covered by this questionnaire	
3	Full Legal (Registered) Address	
4	Full Primary Business Address (if different from above)	
5	Date of Entity incorporation/ establishment	
6	Select type of ownership and append an ownership chart if available	

6a	Publicly Traded (25% of shares publicly traded)	**Y/N**
6a1	If Y, indicate the exchange traded on and ticker symbol	
6b	Government or State Owned by 25% or more	
6c	Privately Owned	
6c1	If Y, provide details of shareholders or ultimate beneficial owners with a holding of 10% or more	
7	Does the Entity, or any of its branches, operate under an Offshore Banking License (OBL) ?	
7a	If Y, provide the name of the relevant branch/es which operate under an OBL	
8	Name of primary financial regulator / supervisory authority	
9	Provide Legal Entity Identifier (LEI) if available [Brand Name]	
10	Provide the full legal name of the ultimate parent (if different from the Entity completing the DDQ)	
11	Jurisdiction of licensing authority and regulator of ultimate parent/holding company	
12	Select the business areas applicable to the Entity	
12a	Commercial Bank	
12b	Money Service Business	
12c	Money Service Business & money Changers	
12d	Money Transfer Operation	
12e	Merchant Banker	
12f	Securities Trader	
12g	Broker, Dealer	
12h	Other	

13	Does the Entity have a significant (10% or more) offshore customer base, either by number of customers or by revenues (where off-shore means not domiciled in the jurisdiction where bank services are being provided) ?	
13a	If Y, provide details of the country and %	
14	Number of employees	
15	Confirm that all responses provided in the above Section ENTITY & OWNERSHIP are representative of all the LE's branches	
2. PRODUCTS & SERVICES		
16	Does the Entity offer the following products and services:	
16a	Agency Business	
16a1	If Y	
16a2	Does the Entity offer Agency services to agent at local level?	
16a3	Does the Entity allow local agents to provide downstream relationships?	
16a4	Does the Entity have processes and procedures in place to identify downstream relationships with customer?	
16a5	Does the Entity offer agency business services to Foreign Company/Banks?	
16a6	Does the Entity allow downstream relationships with Foreign Agency/Banks?	
16a7	Does the Entity have processes and procedures in place to identify downstream relationships with Foreign Agency/Banks?	

16a8	Does the Entity offer services to regulated MSBs/MVTS?	
16a9	Does the Entity allow downstream relationships with MSBs/MVTS?	
16a10	Does the Entity have processes and procedures in place to identify downstream relationships with MSB /MVTS?	
16b	Stored Value Instruments	
16d	Cross Border Bulk Cash Delivery	
16e	Domestic Bulk Cash Delivery	
16f	Virtual /Digital Currencies	
16g	Cross Border Remittances	
16h	Service to walk-in customers (non-account holders)	
16i	Sponsoring Private ATMs/Payment Gateway	
16j	Others	
17	Confirm that all responses provided in the above Section PRODUCTS & SERVICES are representative of all the LE's branches	
3. AML, CTF & SANCTIONS PROGRAMME		
18	Does the Entity have a programme that sets minimum AML, CTF and Sanctions standards regarding the following components:	
18a	Appointed Compliance Officer with sufficient experience/expertise	
18b	Cash Reporting	
18c	CDD	
18d	EDD	
18e	Beneficial Ownership	
18f	Independent Testing	
18g	Periodic Review	
18h	Policies and Procedures	
18i	Risk Assessment	
18j	Sanctions	
18k	PEP Screening	

18l	Adverse Information Screening	
18m	Suspicious Activity Reporting/ Suspicious Matter Reporting	
18n	Training and Education AND Frequency	
18o	Transaction Monitoring	
19	How many full time employees are in the Entity's AML, CTF & Sanctions Compliance Department?	
20	Is the Entity's AML, CTF & Sanctions policy approved at least annually by the Board or equivalent Senior Management Committee?	
21	Does the Board or equivalent Senior Management Committee receive regular reporting on the status of the AML, CTF & Sanctions programme?	
22	Does the Entity use third parties to carry out any components of its AML, CTF & Sanctions programme?	
22a	If Y, provide further details	
4. POLICIES & PROCEDURES		
23	Has the Entity documented policies and procedures consistent with applicable AML, CTF & Sanctions regulations and requirements to reasonably prevent, detect and report:	
23a	Money Laundering	
23b	Terrorist Financing	
23c	Sanctions Violations	
24	Does the Entity have policies and procedures that:	
24a	Prohibit the opening and dealing with anonymous and fictitious named accounts	
24b	Prohibit the opening and dealing with unlicensed banks and/or NBFIs	

24c	Prohibit dealing with other entities that provide banking services to unlicensed banks	
24d	Prohibit accounts/relationships with shell banks/company	
24e	Prohibit dealing with another entity that provides services to shell banks/company	
24f	Prohibit opening and keeping of accounts for any of unlicensed/unregulated remittance agents, exchanges houses, casa de cambio, bureaux de change or money transfer agents	
24g	Assess the risks of relationships with PEPs, including their family and close associates	
24h	Define escalation processes for financial crime risk issues	
24i	Define the process, where appropriate, for terminating existing customer relationships due to financial crime risk	
24j	Specify how potentially suspicious activity identified by employees is to be escalated and investigated	
24k	Outline the processes regarding screening for sanctions, PEPs and negative media	
24l	Outline the processes for the maintenance of internal "watchlists"	
25	Has the Entity defined a risk tolerance statement or similar document which defines a risk boundary around their business?	
26	Does the Entity have a record retention procedures that comply with applicable laws?	
26a	If Y, what is the retention period?	

27	Confirm that all responses provided in the above Section POLICIES & PROCEDURES are representative of all the LE's branches	
5. AML, CTF & SANCTIONS RISK ASSESSMENT		
28	Does the Entity's AML & CTF EWRA cover the inherent risk components detailed below:	
28a	Client	
28b	Product	
28c	Channel	
28d	Geography	
29	Does the Entity's AML & CTF EWRA cover the controls effectiveness components detailed below:	
29a	Transaction Monitoring	
29b	Customer Due Diligence	
29c	PEP Identification	
29d	Transaction Screening	
29e	Name Screening against Adverse Media & Negative News	
29f	Training and Education	
29g	Governance	
29h	Management Information	
30	Has the Entity's AML & CTF EWRA been completed in the last 12 months?	
30a	If N, provide the date when the last AML & CTF EWRA was completed.	
31	Does the Entity's Sanctions EWRA cover the inherent risk components detailed below:	
31a	Client	
31b	Product	
31c	Channel	
31d	Geography	
32	Does the Entity's Sanctions EWRA cover the controls effectiveness components detailed below:	
32a	Customer Due Diligence	

32b	Transaction Screening	
32c	Name Screening	
32d	List Management	
32e	Training and Education	
32f	Governance	
32g	Management Information	
33	Has the Entity's Sanctions EWRA been completed in the last 12 months?	
33a	If N, provide the date when the last Sanctions EWRA was completed.	
34	Confirm that all responses provided in the above Section AML, CTF & SANCTIONS RISK ASSESSMENT are representative of all the LE's branches	
6. KYC, CDD and EDD		
35	Does the Entity verify the identity of the customer?	
36	Which of the following does the Entity gather and retain when conducting CDD? Select that apply:	
36a	Ownership structure	
36b	Customer identification (Dual ID for EDD)	
36c	Exposed Activity / Turnover & no of transactions	
36d	Nature of business/employment	
36e	Product usage	
36f	Purpose and nature of relationship	
36g	Source of funds	
36h	Source of wealth	
37	Are each of the following identified:	
37a	Ultimate beneficial ownership	
37a1	Are ultimate beneficial owners verified?	

37b	Authorised signatories (where applicable) / Matching Authority	
37c	Key controllers	
37d	Other relevant parties, if any	
38	What is the Entity's minimum (lowest) threshold applied to beneficial ownership identification ?	
39	Does the due diligence process result in customers receiving a risk classification?	
40	If Y, what factors/criteria are used to determine the customer's risk classification? Select all that apply:	
40a	Product Usage	
40b	Geography	
40c	Business Type/Industry	
40d	Legal Entity type	
40e	Adverse Information	
40f	Other (specify)	
41	Does entity reject to offer service to client belonging to High Risk Category?	
42	Does Entity record such client as watchlist client for future mapping?	
43	Does the Entity have a risk based approach to screening customers for adverse media/negative news?	
44	If Y, is this at:	
44a	Onboarding	
44b	KYC renewal	
44c	Trigger event	
45	What is the method used by the Entity to screen for adverse media / negative news?	
45a	Automated	
45b	Manual	

45c	Combination of automated and manual	
46	Does the Entity have a risk based approach to screening customers and connected parties to determine whether they are PEPs, or controlled by PEPs?	
47	If Y, is this at:	
47a	Onboarding	
47b	KYC renewal	
47c	Trigger event	
48	What is the method used by the Entity to screen PEPs?	
48a	Automated	
48b	Manual	
48c	Combination of automated and manual	
49	Does the Entity have policies, procedures and processes to review and escalate potential matches from screening customers and connected parties to determine whether they are PEPs, or controlled by PEPs?	
50	Does the Entity have a process to review and update customer information based on:	
50a	KYC renewal	
50b	Trigger event / Material Event	
51	Does the Entity maintain and report metrics on current and past periodic or trigger event due diligence reviews?	
52	From the list below, which categories of customers or industries are subject to EDD and/or are restricted, or prohibited by the Entity's risk program?	
52a	Offshore customers	
52b	Shell banks/company	
52c	MVTS MSB customers	
52d	PEPs	

52e	PEP Related	
52f	PEP Close Associate	
52g	Arms, defense, military	
52h	Atomic power	
52i	Precious metals and stones	
52j	Unregulated charities	
52k	Red light business / Adult entertainment	
52l	Non-Government Organisations	
52m	Virtual currencies	
52n	Marijuana / Banned Substances	
52o	Embassies/Consulates	
52p	Gambling	
52q	Other (specify)	
53	If restricted, provide details of the restriction	
54	Does the Entity perform an additional control or quality review on clients subject to EDD?	
55	Confirm that all responses provided in the above Section KYC, CDD and EDD are representative of all the LE's branches	
7. MONITORING & REPORTING		
56	Does the Entity have risk based policies, procedures and monitoring processes for the identification and reporting of suspicious activity?	
57	What is the method used by the Entity to monitor transactions for suspicious activities?	
57a	Automated	
57b	Manual	
58	Combination of automated and manual	
59	If manual or combination selected, specify what type of transactions are monitored manually.	

60	Does the Entity have regulatory requirements to report currency transactions?	
60a	If Y, does the Entity have policies, procedures and processes to comply with currency reporting requirements?	
61	Does the Entity have policies, procedures and processes to review and escalate matters arising from the monitoring of customer transactions and activity?	
62	Confirm that all responses provided in the above Section MONITORING & REPORTING are representative of all the LE's branches	
63	Does Entity has requirement to report full address of both reciepient & sender to regulator as mandatory reporting?	
8. PAYMENT TRANSPARENCY		
64	Does the Entity adhere to the Wolfsberg Group Payment Transparency Standards?	
65	Does the Entity have policies, procedures and processes to [reasonably] comply with and have controls in place to ensure compliance with:	
65a	FATF Recommendation 16	??
65b	Local Regulations	
65b1	Specify the regulation (PAYMENT ACT)	
65c	If N, explain	
66	Does the Entity have processes in place to respond to Request For Information (RFIs) from other entities in a timely manner?	Y/N
67	Does the Entity have controls to support the inclusion of required and accurate originator information in international payment messages?	Y/N

68	Does the Entity have controls to support the inclusion of required beneficiary in international payment messages?/CROSS BORDER Payment Service	
69	Confirm that all responses provided in the above Section PAYMENT TRANSPARENCY are representative of all the LE's branches	
9. SANCTIONS		
70	Has the Entity included in AML Policy, approved by Management regarding compliance sanctions law applicable to the Entity, including with respect its business conducted with, or through accounts held at foreign financial institutions?	Y/N
71	Does the Entity have policies, procedures, or other controls reasonably designed to prevent the use of another entity's accounts or services in a manner causing the other entity to violate sanctions prohibitions applicable to the other entity (including prohibitions applicable to the other entity's local jurisdiction)?	
72	Does the Entity have policies, procedures or other controls reasonably designed to prohibit and/or detect actions taken to evade applicable sanctions prohibitions, such as stripping, or the resubmission and/or masking, of sanctions relevant information in cross border transactions?	
73	Does the Entity screen its customers, including beneficial ownership information collected by the Entity, during onboarding and regularly thereafter against Sanctions Lists?	

74	What is the method used by the Entity?	
74a	Manual	
74b	Automated	
74c	Combination of Automated and Manual	
75	Does the Entity screen all sanctions relevant data, including at a minimum, entity and location information, contained in cross border transactions against Sanctions Lists?	
76	What is the method used by the Entity?	
76a	Manual	
76b	Automated	
76c	Combination of Automated and Manual	
77	Select the Sanctions Lists used by the Entity in its sanctions screening processes:	
77a	Consolidated United Nations Security Council Sanctions List (UN)	
77b	United States Department of the Treasury's Office of Foreign Assets Control (OFAC)	
77c	Office of Financial Sanctions Implementation HMT (OFSI)	
77d	European Union Consolidated List(EU)	
77e	Others	
78	When new entities and natural persons are added to sanctions lists, how many business days before the Entity updates its lists?	

79	When updates or additions to the Sanctions Lists are made, how many business days before the Entity updates their active manual and/or automated screening system against:	
79a	Customer Data	
79b	Transactions	
80	Does the Entity have a physical presence, e.g., branches, subsidiaries, or representative offices located in countries/regions against which UN have enacted comprehensive jurisdiction-based Sanctions?	
81	Confirm that all responses provided in the above Sectin SANCTIONS are representative of all the LE's branches.	
10. TRAINING & EDUCATION		
82	Does the Entity provide mandatory training, which includes :	
82a	Identification and reporting of transactions to government authorities	
82b	Examples of different forms of money laundering, terrorist financing and sanctions violations relevant for the types of products and services offered	
82c	Internal policies for controlling money laundering, terrorist financing and sanctions violations	
82d	New issues that occur in the market, e.g., significant regulatory actions or new regulations	
82e	Conduct and Culture	
83	Is the above mandatory training provided to :	
83a	Board and Senior Committee Management	
83b	1st Line of Defence	
83c	2nd Line of Defence	

83d	3rd Line of Defence	
83e	3rd parties to which specific FCC activities have been outsourced	
83f	non employers	
84	Does the Entity provide customised training for AML, CTF and Sanctions staff?	
11. COMPLIANCE AUDIT		
85	Are the Entity's KYC processes and documents subject to quality assurance testing?	
86	Does the Entity have a program wide risk based Compliance Audit?	
87	Confirm that all responses provided in the above Section QUALITY ASSURANCE / COMPLIANCE TESTING are representative of all the LE's branches	
12. AUDIT		
88	In addition to inspections by the government supervisors/regulators, does the Entity have an internal audit function, a testing function or other independent third party, or both, that assesses FCC AML, CTF and Sanctions policies and practices on a regular basis?	
89	How often is the Entity audited on its AML, CTF & Sanctions programme by the following:	
89a	Internal Audit Department	
89b	External Third Party	
90	Does the internal audit function or other independent third party cover the following areas:	
90a	AML, CTF & Sanctions policy and procedures	
90b	KYC/CDD/EDD and underlying methodologies	

90c	Transaction Monitoring	
90d	Transaction Screening including for sanctions	
90e	Name Screening & List Management	
90f	Training & Education	
90g	Technology	
90h	Governance	
90i	Suspicious Activity Filing	
90j	Enterprise Wide Risk Assessment	
90k	Other (specify)	
91	Are adverse findings from internal & external audit tracked to completion and assessed for adequacy and completeness and brought to knowledge of Board/Senior Management?	
92	Confirm that all responses provided in the above section, AUDIT are representative of all the LE's branches	

Version 2023:

ACRA 201418080H

PSO 20200205

AML / CFT – Revision Document

Revision to ISEND Policy and Procedure on Anti Money Laundering (AML) and Customer Due Diligence (CDD)

With reference to the original copy of ISEND Policy Procedure on Anti Money Laundering (AML) and Customer Due Diligence (CDD), this addendum has been prepared to cover the following:

Company ISEND PTE. LTD. hereby is referred as ISEND.

PART A of the revisions made:

1. ISEND has developed Compliance and BSA/AML program that is sufficiently detailed with standards and criteria addressing compliance with Applicable Law.
2. ISEND compliance policies and procedures will be periodically reviewed, updated, and approved by an individual or committee with sufficient oversight of the compliance program (i.e., Board of Directors, Chief Compliance Officer, etc.)
3. Client will conduct Internal training for compliance employees pertinent to the Program and Client's functions.
4. ISEND's policies and procedures will contain controls for preventing accounts being opened for customers operating as or in connection with.

    - The creation, facilitation, sale or distribution of any prohibited or illegal good or service or an activity that requires a governmental license where the customer lacks such a license;
    - The creation, facilitation, sale or distribution of marijuana or marijuana paraphernalia, regardless of whether such sale is lawful in the jurisdiction in which customer operates, or our jurisdiction.
    - The creation, facilitation, sale or distribution of any material that promotes violence or hatred;
    - The creation, facilitation, sale or distribution of adult content, including, but not limited to, online dating or marriage services, pornographic services and goods, adult entertainment related activities, or escort services.
    - The creation, facilitation, sale or distribution of goods or services that violate the intellectual property rights of a third party;
    - The sale, distribution, or exchange of cryptocurrencies.
    - Any Ponzi-scheme or pyramid selling.
    - Any gambling or regulated financial services you or the customer may provide.
    - Offshore companies.
    - Casinos and card rooms, except licensed, U.S. institutions that do not accept cash.
    - Outbound telemarketing.
    - Online payday lenders

- The facilitation, sale or distribution of firearms or other weapons, military or semi-military goods, military software, or technologies.
- The facilitation, sale or distribution of chemicals
- The facilitation, sale, or distribution of prescription medications
- The facilitation, sale or distribution of seeds or plants, dietary supplements, alcoholic beverages, tobacco goods, jewels, precious metals or stones.

Part B of the revisions made:

1. ISEND is responsible for documenting and implementing a written Customer Identification Program (CIP) as outlined in 31 CFR 1020.220
2. ISEND will provide new customers with the below, or similar subject to approval by the Bank, notice requesting CIP information to verify their identity
3. Customer Identification Requirements
4. IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT – To help the government fight the funding of terrorism and money laundering activities, federal law requires all financial institutions and their third parties to obtain, verify, and record information that identifies each person who opens a new account. This means, when we open an account, we will ask for customer's name, address, date of birth, and other information that will allow us to identify the customer. We may ask to see customer's driver's license or other identifying documents.

   Customer Identification: Client is responsible for documenting and implementing a written Customer Identification Program (CIP) including collecting the following customer identifying information:

   1. Full Name

   2. Date of birth for individuals

   3. Address, which shall be:

• For an individual, a residential or business street address;

• For an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number;

• For a "person" other than an individual (such as a corporation, partnership, or trust), a principal place of business, local office, or other physical location.

5. Identification number, which shall be:

   - For a U.S. person, a taxpayer identification number; or
   - For a non-U.S. person, one or more of the following: A taxpayer identification number; passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard; or
   - For a customer that has applied for, but has not received, a taxpayer identification number, ISEND's CIP will include procedures to confirm that the application was

filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.

- For a “person” other than an individual (such as a corporation, partnership, or trust) a Tax Identification Number (TIN).

Customer Verification: ISEND’s CIP will contain procedures for verifying the identity of the customer prior to allowing funding of customer’s account. The procedures will describe when the bank will use documents, non-documentary methods, or a combination of both methods.

Verification through documents: For Programs relying on documentary verification, the CIP will contain procedures that set forth the acceptable documentation, which at minimum includes the collection of one unexpired government-issued ID and one supplemental document. Acceptable forms of unexpired government-issued identification includes the following:

- For an individual, unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- For a person other than an individual (such as a corporation, partnership, or trust), documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or trust instrument.

The program's list of acceptable forms of ID should comply as;

Verification through documents: For Programs relying on documentary verification, the CIP will contain procedures that set forth the acceptable documentation, which at minimum includes the collection of one unexpired government-issued ID and one supplemental document. Acceptable forms of supplemental documentation includes the following:

• Utility bill, lease agreement, current paystub, bank or credit card statement showing customer’s name and current address

• Debit or credit card with name and signature matching other forms of identification

• State-issued birth certificate

• Marriage license, divorce decree, or other court documentation

• Current School or work ID with photo

• ITIN letter

Verification through documents: The Bank requires that ISEND confirm at least two of the following data points when verifying a customer’s identity via documentary methods:

- Confirm signatures, as well as the photo, to the person

- Confirm that the permanent address supplied matches to the name by comparing against the name and address on the photo ID
- Confirm that the date of birth supplied matches to the name by comparing to the name and date of birth on the photo ID
- Confirm the ID number supplied matches to name by comparing to the name and ID number on the photo ID.

Verification through non-documentary methods: For Programs relying on non-documentary methods, the CIP will contain procedures that set forth the non-documentary methods ISEND will use, which a will at minimum include:

- Using publicly available data sources and systems
- Contacting the customer and independently verifying the customer's identity through comparison of information provided by the customer with information obtained from a customer reporting agency, public database, or other source; OR
- Using knowledge-based authentication (KBA) questions offered by a third-party vendor. In order to use this method, sufficient data will be found in the customer's public data record to generate KBA questions.

Ultimate Beneficial Ownership: ISEND will obtain and maintain the necessary information required under FinCEN's Final Rule on Beneficial Ownership and Risk-Based Customer Due Diligence (81 FR 29398) beginning on May 11th, 2018, which includes collecting the required CIP information (Name, DOB, Address, and Identification Number for:

1. all beneficial owner(s) (all natural person(s)), who directly or indirectly own at minimum 25 percent or greater of the equity interest in the legal entity customer for U.S. entities OR at minimum 10% or more for non-U.S. entities;
2. the control person, a single individual with significant responsibility to control, manage, the legal entity customer including an executive officer or senior manager, or any individual who regularly perform similar functions.

Ultimate Beneficial Ownership: ISEND is responsible for collecting copies of acceptable forms of identification for all beneficial owners, control persons, and account signatories;

Ultimate Beneficial Ownership: ISEND is responsible for verifying the identity of the beneficial owners, control person, and authorized signers and their connection to the legal entity;

Ultimate Beneficial Ownership: ISEND is responsible for collecting the completed Beneficial Ownership Certification Form (or similar form approved by CFSB), reviewing it for accuracy, and submitting it to the Bank within 14 calendar days of the account being opened for a customer.

Accounts cannot be opened for any new legal entity customers who do not complete and provide this form beginning on May 11th, 2018.

Ultimate Beneficial Ownership: ISEND is responsible for documenting triggering events for ISEND to collected the required beneficial ownership and control person information for ISENDs on-boarded prior to May 11th, 2018.

ISEND will develop and maintain procedures to address circumstances in which a customer's identity cannot be verified and include the following:

- Criteria or decision points at which an account should not be opened
- Parameters for when a customer is conditionally permitted to use an account while ISEND attempts to verify the customer
- When ISEND should close an account, after attempts to verify a customer's identity have failed

ISEND will automatically decline customers or have procedures in place to verify customer's identity with the following anomalies:

- Customers whose identity cannot be verified
- SSN reported as deceased
- Invalid SSN
- SSN not yet issued

ISEND will develop and maintain procedures for identifying customers presenting increased risk and performing additional due diligence on the customer

ISEND will develop and maintain procedures addressing how customer and account profile information will be kept current and up to date

ISEND will compile a formal monthly report containing the results of the due diligence conducted regarding business Customers that apply to use ISEND as a means of transferring money and present a copy to the Bank for review.

ISEND will store the Customer data on the Bank's behalf during the Term. ISEND will grant the Bank ongoing access to its systems whereby the Bank can access customer information. Parties may develop a joint plan to share information necessary for customer identification and anti-money-laundering obligations efficiently, subject to the Bank's approval, direction and oversight. Information collected for anti-money-laundering or similar purposes may not be used for marketing purposes except to the extent agreed by the Parties and permitted under Applicable Law.

Consistent with the Fair and Accurate Credit Transactions (FACT) Act, ISEND will document and maintain an identity theft prevention policies and procedures designed to detect, prevent, and mitigate identity theft specific to ISEND Program.

ISEND will document and maintain a Identity Theft Red Flags Risk Assessment relative to the products, services, customer, and geography risks associated with the ISEND Program.

ISEND is required to retain all customer information and verification records and information for five years from the date of the last transaction using the prepaid access or five years from the date of the account/card closure. ISEND will also provide the Bank with access to this information for five years from the date of the last transaction.

ISEND will develop and maintain procedures for determining whether the customer, beneficial owners, and control person(s), which includes any entity that is 50 percent or more owned, in the aggregate, by one or more blocked persons, regardless of whether the entity is formally listed on the SDN list, appears on any list of sanctioned entities and known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by Treasury in consultation with the Federal functional regulators.

Customer - Account Opening Screening: ISEND will document and maintain a process to screen customers prior to account opening.

Customer - Ongoing Screening: ISEND will document and maintain a process to screen customers on an ongoing basis, at minimum when the update to the lists is made.

Ultimate Beneficial Ownership - Account Opening Screening: ISEND is responsible for screening the beneficial owners, control person, and authorized signers at account opening.

Ultimate Beneficial Ownership - Ongoing Screening: ISEND is responsible for screening the beneficial owners, control person, and authorized signers on an ongoing basis.

ISEND will document and maintain a process to review potential matches to watchlist entities, which at minimum, will include clearing potential matches to watchlist entities based on, at minimum, two customer identifying factors, such as name and date of birth OR name and country of citizenship.

ISEND will document and maintain a process for escalating positive matches to the Bank. ISEND will notify the Bank's Compliance department within one hour of any positive matches to any terrorist or sanctioned entities.

ISEND will document and maintain a process for whitelisting or excluding customer from screening. ISEND will not whitelist or exclude entities from monitoring without written approval from the Bank's Compliance department.

ISEND will automatically decline customers or have procedures in place to verify customer's identity with the following anomalies:

- Valid match to sanctioned entity

ISEND will not open or maintain accounts for any sanctioned entity or known or suspected terrorists or terrorist organizations.

ISEND will maintain documentation demonstrating ISEND's review of potential matches and factors contributing to ISEND's decision that a customer was not a match to the watchlist entity.

ISEND will retain information and records as prescribed by Applicable Laws for the Program.

ISEND will develop and maintain a suspicious and fraudulent activity monitoring coverage assessment which identifies the customer, transactional, and geographical risks associated with the Program and develop mitigating controls to prevent and detect potentially suspicious or fraudulent activity associated with the risks. ISEND will update this coverage assessment as program features change, including, but not limited, to changes in Program's customer base, geographic footprint, or transactional funding, transfer, or withdrawal methods. ISEND will provide this assessment to the Bank for approval prior to the program going live, prior to the implementation of new features, and as requested by the Bank.

ISEND will perform on-going monitoring for suspicious and fraudulent activity for all risks identified in the suspicious and fraudulent activity monitoring coverage assessment. ISEND will escalate any identified unusual, suspicious or fraudulent activity to the Bank's Compliance department within 48 hours of detection via a reporting template provided by the Bank.

ISEND will maintain documentation demonstrating ISEND's review of potentially suspicious or fraudulent activity and the factors contributing to ISEND's decision that activity was not suspicious or fraudulent.

ISEND will periodically, at least annually, assess the effectiveness of its suspicious activity and fraud monitoring controls.

ISEND will maintain documented policies and procedures for responding to official requests from government and law enforcement agencies

ISEND will review the performance of all businesses regarding chargebacks, payment disputes, cancellations, reversals, off-sets, suspicious activity and complaints and provide a monthly report to the Bank.

ISEND will develop, implement, and maintain controls to prevent the loading or remitting of more than the agreed upon limits.

ISEND is required to retain transaction-specific records generated in the ordinary course of business for five years, including any information necessary to reconstruct activity associated with the account activity. The information will reflect the transaction's amount, location, date and time, and any other unique identifier. ISEND will also provide the Bank will access to this information for five years from the date of the last transaction or five years from the date of the account/card closure.

ISEND will provide annual training to all employees on relevant aspects of BSA/AML/OFAC regulations and ISEND's BSA/AML/OFAC and related policies.

Training shall include assessments to verify comprehension of the information taught, and training policy shall include remediation procedures for employees who do not pass these assessments.

ISEND will provide appropriate BSA/AML/OFAC and Consumer Compliance training to newly-hired employees within thirty days of employment

ISEND will provide training logs documenting, for each training session:

- The topic(s) covered in the session

- Who conducted the training

- Who attended the training (with confirmation of attendance via signed attendance sheet or other method)

- The date of the training

- Results of all assessments given during or immediately after the training

These logs should be maintained for no less than five years following the date on which the training was provided

ISEND will provide the Bank's Compliance department with a report by the first Friday of every month reports that includes the following information related specifically to the accounts/customers onboarding within the jurisdictions ISEND is operating under Program Services Agreement:

- Number of new accounts opened during the reporting period
- Number of accounts deleted during the reporting period

- Number of total accounts since Program inception
- Number of potentially suspicious or fraudulent activity
- instances escalated to the Bank during the reporting period
- Number of potentially suspicious or fraudulent activity instances escalated to the Bank since Program inception.
- Number of accounts maintained by any identified Politically Exposed Persons (PEPs) along with names and account numbers.

ISEND will provide copies of any complaints or lawsuits received regarding the activities of any customer in the Program that transfer funds through the ISEND system, including those submitted by or through governmental agencies, to the Bank's Compliance department within three business days of receipt of such lawsuits or complaints.

ISEND will inform the Bank within three business days regarding receipt of any governmental investigation or criminal or enforcement proceeding initiated against it or any ISEND Affiliate, as well as any filed civil litigation or correspondence from an attorney threatening litigation that alleges or reasonably is anticipated to allege or that otherwise reasonably may result in exposure of fifty thousand dollars ($50,000) or greater.

ISEND will provide the updated board or senior management approved policies and procedures on an annual basis or as requested by the Bank.

ISEND will provide the internal training logs on an annual basis or as requested by the Bank.

ISEND will notify the Bank of any new appointment of a Chief Compliance or BSA/AML Compliance Officer.

ISEND will notify the Bank of any of the following, within two business days after the occurrence of any of the events listed below:

- The institution of revocation or suspension proceedings or any regulatory action against ISEND by any state or governmental authority, or any self-reporting organization.

ISEND will notify the Bank of any of the following, within two business days after the occurrence of any of the events listed below:

• The institution of revocation or suspension proceedings or any regulatory action against ISEND by any state or governmental authority, or NACHA.

• Any felony indictment or conviction of ISEND, or any of its Principals, directors, officers, or employees related to any money transmission activity.

REGULATION GG

Prohibition on Funding of Unlawful Internet Gambling

Regulation GG implements the Unlawful Internet Gambling Enforcement Act (UIGEA). The Act prohibits businesses from knowingly accepting payments in connection with unlawful internet gambling, including payments made through credit cards, electronic funds transfers and checks. Such transactions are termed "restricted transactions." The act generally defines "unlawful internet gambling" as placing, receiving, or otherwise knowingly transmitting a bet or wager by any means which involves the use, at least in part, of the internet where such bet or wager is unlawful under

any applicable federal or state law in the state or tribal lands in which the bet or wager is initiated, received, or otherwise made.

ISEND restricts accepting payments in connection with unlawful internet gambling, business of betting or wagering, knowingly accepting payments in connection with the participation of another person or business in unlawful Internet gambling.

REGULATION E

Electronic Fund Transfer Act

Regulation E provides a basic framework that establishes the rights, liabilities, and responsibilities of participants in electronic fund transfer systems such as automated teller machine transfers, telephone bill-payment services, point-of-sale (POS) terminal transfers in stores, and preauthorized transfers from or to a consumer's account (such as direct deposit and social security payments). The term "electronic fund transfer" (EFT) generally refers to a transaction initiated through an electronic terminal, telephone, computer, or magnetic tape that instructs a financial institution either to credit or to debit a consumer's asset account.

ISEND follows the guidance of REGULATION E at all times.

UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES (UDAAP)

Unfair, deceptive, or abusive acts and practices (UDAAP) can cause significant financial injury to consumers, erode consumer confidence, and undermine the financial marketplace. Under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), it is unlawful for any provider of consumer financial products or services or a service provider to engage in any unfair, deceptive, or abusive act or practice.

Unfair Acts or Practices - ISEND considers unfair act / practices as under;

1. To cause substantial injury to consumers.
2. The injury is not reasonably avoidable by consumers; and
3. The injury is not outweighed by countervailing benefits to consumers or to competition

Deceptive Acts or Practices – ISEND considers practice is deceptive when

1. The representation, omission, act, or practice misleads or is likely to mislead the consumer;
2. The consumer’s interpretation of the representation, omission, act, or practice is reasonable under the circumstances; and
3. The misleading representation, omission, act, or practice is material

Abusive Acts or Practices – ISEND always acts in the interest of consumers and never engage itself to materially interfere with the ability of a consumer to understand its terms and condition or a its products’ terms and conditions. It also never takes unreasonable advantage of;

- The consumer’s lack of understanding of the material risks, costs, or conditions of the product or service,

- The consumer's inability to protect his or her interests in selecting or using ISEND's product or service.

E – SIGN ACT

ISEND follows four major requirements for an electronic signature to be recognized as valid under US law as per E – Sign act of the US. Those requirements are:

- Intent to sign – Electronic signatures, like traditional wet ink signatures, are valid only if each party intended to sign.
- Consent to do business electronically – The parties to the transaction must consent to do business electronically. Establishing that a business consented can be done by analysing the circumstances of the interaction, but consumers require special considerations. Electronic records may be used in transactions with consumers only when the consumer has:
    - Affirmatively agreed to use electronic records for the transaction.
    - Has not withdrawn such consent.
- Association of signature with the record – In order to qualify as an electronic signature under the ESIGN Act the system used to capture the transaction must keep an associated record that reflects the process by which the signature was created or generate a textual or graphic statement (which is added to the signed record) proving that it was executed with an electronic signature.
- Record retention – ISEND follows that under U.S. laws on eSignatures and electronic transactions it is required that electronic signature records be capable of retention and accurate reproduction for reference by all parties or persons entitled to retain the contract or record.

THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT (FACTA)

Following The Fair And Accurate Credit Transactions Act (FACTA), ISEND insures the information it gathers and distributes is a fair and accurate summary of a consumer's credit history. It understands the requirements for information privacy & accuracy. It also understands the risk of identity theft and has all proper measures to tackle it.

ISEND Identifies Relevant Red Flags considering;

Risk Factors. When ISEND is identifying key red flags, it thinks about the types of accounts it offers or maintain such as the ways the customer's account is opened and how access is provided.

Sources of Red Flags. ISEND considers other sources of information, including the experience of other members of the industry. Considering that technology and criminal techniques change constantly, it keeps up-to-date on new threats.

Categories of Common Red Flags. ISEND thinks about relevant red flags in the context of its own business as;

- **Alerts, Notifications, and Warnings from a Credit Reporting Company**. Changes in a credit report or a consumer's credit activity might signal identity theft:
    - a fraud or active duty alert on a credit report
    - a notice of credit freeze in response to a request for a credit report

    - a notice of address discrepancy provided by a credit reporting company
- **Suspicious Documents**. Documents can offer hints of identity theft:
    - identification looks altered or forged
    - the person presenting the identification doesn't look like the photo or match the physical description
    - information on the identification differs from what the person with identification is telling ISEND or doesn't match a signature card or recent check
    - an application looks like it's been altered, forged, or torn up and reassembled
- **Personal Identifying Information**. Personal identifying information can indicate identity theft:
    - inconsistencies with what ISEND knows — for example, an address that doesn't match the credit report or the use of a Social Security number that's listed on the Social Security Administration Death Master File.
    - inconsistencies in the information a customer has submitted to ISEND
    - an address, phone number, or other personal information already used on an account ISEND knows to be fraudulent
    - a bogus address, an address for a mail drop or prison, a phone number that's invalid, or one that's associated with a pager or answering service
    - a Social Security number used by someone else opening an account
    - an address or telephone number used by several people opening accounts
    - a person who omits required information on an application and doesn't respond to notices that the application is incomplete
    - a person who can't provide authenticating information beyond what's generally available from a wallet or credit report — for example, someone who can't answer a challenge question
- **Account Activity**. How the account is being used can be a tip-off to identity theft:
    - shortly after ISEND is notified of a change of address, ISEND is asked for new or additional credit cards, or to add users to the account
    - a new account used in ways associated with fraud — for example, the customer doesn't make the first payment, or makes only an initial payment.
    - an account that is inactive is used again
    - mail sent to the customer that is returned repeatedly as undeliverable although transactions continue to be conducted on the account
    - information that the customer isn't receiving an account statement by mail or email
- **Notice from Other Sources.** A customer, a victim of identity theft, a law enforcement authority, or someone else may be trying to tell that an account has been opened or used fraudulently.

For detecting a red flag, ISEND uses programs to monitor transactions, identify behavior that indicates the possibility of fraud and identity theft, or validate changes of address. It has incorporated these tools into ITS program.

Prevent And Mitigate Identity Theft

When ISEND spots a red flag, it is prepared to respond appropriately. ISEND understands that it may need to accommodate other legal obligations, like laws about providing and terminating service.

The Guidelines in the Red Flags Rule it considers:

- monitoring the account for evidence of identity theft
- contacting the customer
- changing passwords, security codes, or other ways to access the account
- closing an existing account
- reopening an account with a new customer ID
- not opening a new account
- notifying law enforcement

ISEND understands that the new red flags emerges as technology changes or identity thieves change their tactics. Hence it does periodic updates to its program considering the factors in its own experience with identity theft if any, changes in how identity thieves operate, new methods to detect, prevent, and mitigate identity theft, changes in the accounts it offers and changes in its business, like mergers, acquisitions, alliances, joint ventures, and arrangements with service providers.

OFAC AND SANCTION POLICY

ISEND PTE LTD always follows the list of below sanctions.

Sanctions Program

1. Comprehensive Sanction

Cuba
Iran
Sudan
Syria

2. Significant Sanctions

North Korea
Burma (Myanmar)

3. Limited Sanctions
W. Balkans
Belarus
Cote D I'voire
Democratic Republic of Congo
Iraq
Lebanon
Liberia
Libya
Somalia
Yemen
Zimbabwe

4. Entity Person - based Sanctions (Comprehensive ban against listed person / entities

Specially Designated Nationals
Terrorists
Narcotics
Traffickers
WMD Proliferators
Transnational Criminals Organizations
Foreign Sanctions Envaders