PAA CAPITAL PTE. LTD.

Anti-Money Laundering

And

Countering Financing of Terrorism

COMPLIANCE PROGRAMME

Issued in compliance with

Notice to Holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP.186

Version 1, Issued by the company on 17th Feb 2017

Contents

Definitions

AML/CFT" means anti-money laundering and countering the financing of terrorism;

"Authority" means the Monetary Authority of Singapore;

"beneficial owner", in relation to a customer of a relevant holder, means the natural person who ultimately owns or controls the customer or the natural person (including the end-user) on whose behalf a transaction is conducted or business relations are established, and includes any person who exercises ultimate effective control over a legal person or legal arrangement;

"business relations" means the opening or maintenance of an account by the relevant holder in the name of a person (whether a natural person, legal person or legal arrangement);

"CDD measures" or "customer due diligence measures" means the measures required by paragraph 6;

"CDSA" means the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A);

connected party" -

1. in relation to a legal person (other than a partnership), means any director or any natural person having executive authority in the legal person;
2. in relation to a legal person that is a partnership, means any partner or manager[1]; and
3. in relation to a legal arrangement, means any natural person having executive authority in the legal arrangement;

"customer", in relation to a relevant holder, means a person (whether a natural person, legal person or legal arrangement) with whom the relevant holder establishes or intends to establish business relations;

"end-user" means the natural person who is the ultimate user of a relevant stored value facility;

"FATF" means the Financial Action Task Force;

"government entity" means a government of a country or jurisdiction, a ministry within such a government, or an agency specially established by such a government through written law;

"holder" has the same meaning as defined in section 2(1) of the Payment System Oversight Act, 2006.

"legal arrangement" means a trust or other similar arrangement;

"legal person" means an entity other than a natural person that can establish a permanent customer relationship with a financial institution or otherwise own property;

[1] In the case of a limited liability partnership or a limited partnership.

“officer” means any director or any member of the committee of management of the relevant holder;

“partnership” means a partnership, a limited partnership within the meaning of the Limited Partnerships Act (Cap. 163B) or a limited liability partnership within the meaning of the Limited Liability Partnerships Act (Cap. 163A);

personal data” has the same meaning as defined in section 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012);

“reasonable measures” means appropriate measures which are commensurate with the money laundering or terrorism financing risks;

“relevant holder” means a holder of a relevant stored value facility;

“relevant stored value facility” means a stored value facility which is able to contain, and make available to the customer, stored value of more than S$1,000;

"stored value facility" has the same meaning as defined in section 2(1) of the PSOA;

“STR” means suspicious transaction report;

STRO” means the Suspicious Transaction Reporting Office, Commercial Affairs Department of the Singapore Police Force; and

“TSOFA” means the Terrorism (Suppression of Financing) Act (Cap. 325).

A reference to any threshold or value limit expressed in S$ shall include a reference to the equivalent amount expressed in any other currency.

The expressions used in this Notice shall, except where defined in this Notice or where the context otherwise requires, have the same meanings as in the PSOA.

politically exposed person” means a domestic politically exposed person, foreign politically exposed person or international organisation politically exposed person;

“close associate” means a natural person who is closely connected to a politically exposed person, either socially or professionally;

“domestic politically exposed person” means a natural person who is or has been entrusted domestically with prominent public functions;

“family member” means a parent, step-parent, child, step-child, adopted child, spouse, sibling, step-sibling and adopted sibling of the politically exposed person;

“foreign politically exposed person” means a natural person who is or has been entrusted with prominent public functions in a foreign country;

"international organisation" means an entity established by formal political agreements between member countries that have the status of international treaties, whose existence is recognised by law in member countries and which is not treated as a resident institutional unit of the country in which it is located;

"international organisation politically exposed person" means a natural person who is or has been entrusted with prominent public functions in an international organisation; and

"prominent public functions" includes the roles held by a head of state, a head of government, government ministers, senior civil or public servants, senior judicial or military officials, senior executives of state owned corporations, senior political party officials, members of the legislature and senior management of international organisations.

"Senior management" is defined as the director of the company.

General Policy on Anti-Money Laundering and Countering Financing of Terrorism

Policy

The company is required to comply with a risk-based approach to anti-money laundering and countering financing of terrorism (AML/CFT) and the company takes these requirements very seriously.

In seeking and maintaining critical relationships with the institutions that bank the company and process transactions involving the company, the company is expected to take a pro-active stance on developing and implementing these policies, procedures and controls, and to comply not only with Singapore law but with the policies and practices recognised internationally as minimum requirements in this area.

Procedure

This programme is developed on a risk-based approach, using the previously completed Risk Assessment that was, after review and professional advice, issued by the company on TBA and as updated from time to time.

The company must incorporate its AML/CFT obligations and requirements into its core business systems and controls so that the company can comply effectively and reliably with its obligations in this area, and so that compliance with these obligations can be verified by management and external auditors.

Control

When the company is reviewing its Risk Assessment and Compliance Programme as required by law and by this policy, compliance with this policy must also be reviewed. Likewise when the Risk Assessment and Compliance Programme is subject to external audit.

The Compliance Officer is responsible for compliance with this policy, and for the effectiveness of the programme as a whole.

Customer Due Diligence – acceptance of new business

Policy

The company does not provide occasional transaction services, all services are provided only to customers who have established a business relationship with the company. The company shall exercise due diligence when dealing with customers, natural persons appointed to act on the customer's behalf, connected parties of the customer and beneficial owners of the customer. The company shall conduct its business in conformity with high ethical standards, and guard against establishing any business relations or undertaking any transaction, that is or may be connected with or may facilitate money laundering or terrorism financing. The company shall, to the fullest extent possible, assist and cooperate with the relevant law enforcement authorities in Singapore to prevent money laundering and terrorism financing. The company carries out simplified Customer Due Diligence (CDD) on all applicants, and, if the customer does not qualify for simplified due diligence, enhanced CDD is done.

Applicants are classified as follows:

1. Natural person
2. Legal entity
3. Legal arrangements (trusts)
4. Financial Institutions

Requirements for Acceptance:

1. The company shall not open or maintain an anonymous account or an account in a fictitious name.
2. Before establishing the business relationship with a customer, where the company has any reasonable ground to suspect that the assets or funds of a customer are proceeds of drug dealing or criminal conduct as defined in CDSA, or are property related to the facilitation or carrying out of any terrorism financing offence as defined in the TSOFA, the company shall-
    a) not establish business relations with, or undertake a transaction for, the customer; and
    b) file an STR[2], and extend a copy of the Authority for information.
3. When the company establishes a business relationship with a new customer ,
    a) the company shall identify the customer type and collect and record them in CDD portal:
        i. full name, including any aliases

[2] http://www.cad.gov.sg/aml-cft/suspicious-transaction-reporting-office/suspicious-transaction-reporting

ii. unique identification number (such as an identity card number, birth certificate number or passport number, or where the customer is not a natural person, the incorporation number or business registration number);

iii. the customer's –

- residential address; or
- registered or business address, and if different, principal place of business,

iv. date of birth, establishment, incorporation or registration (as may be appropriate); and

v. nationality, place of incorporation or place of registration (as may be appropriate).

b) Where the customer is a legal person or legal arrangement, the company shall, apart from identifying the customer, also identify the legal form, constitution and powers that regulate and bind the legal person or legal arrangement.

c) Where the customer is a legal person or legal arrangement, the company shall identify the connected parties of the customer, by obtaining at least the following information of each connected party:

i. full name, including any aliases; and

ii. unique identification number (such as an identity card number, birth certificate number or passport number of the connected party).

d) Where the customer appoints one or more natural persons to act on behalf in establishing business relations with the company or the customer is not a natural person, the company shall-

i. identify each natural person who acts or is appointed to act on behalf of the customer by obtaining at least the following information of such natural person:

- full name, including any aliases;
- unique identification number (such as an identity card number, birth certificate number or passport number);
- residential address;
- date of birth;
- nationality and

ii. Verify the identity of each natural person using reliable, independent source data, documents or information.

iii. The company shall verify the due authority of each natural person appointed to act on behalf of the customer by obtaining at least the appropriate documentary evidence authorising the appointment of such natural person by the customer to act on his or its behalf.

e) Where the customer is a Singapore Government entity, the company shall only be required to obtain such information as may be required to confirm that the customer is a Singapore Government entity as asserted.

4. Beneficial owner, in relation to a customer of the company, means the natural person who ultimately owns or controls the customer or the natural person (including the end-user) on whose behalf a transaction is conducted or business relations are established, and includes any person who exercises ultimate effective control over a legal person or legal arrangement.

a) the company shall inquire if there exists any beneficial owner in relation to a customer except paragraph 6.16 of the Notice to Holders of Stored Value facilities Monetary Authority of Singapore Act, CAP. 186 (refer policy 6 below).

b) Where there is one or more beneficial owner in relation to a customer, the company shall identify the beneficial owners and take reasonable measures to verify the identities of the beneficial owners using the relevant information or data obtained from reliable, independent sources. The company shall-

i. For customers that are legal persons-

- identify the natural persons (whether acting alone or together) who ultimately own the legal person;
- to the extent that there is doubt as to whether the natural persons who ultimately own the legal person are the beneficial owners or where no natural persons ultimately own the legal person, identify the natural persons (if any) who ultimately control the legal person or have ultimate effective control of the legal person; and
- where no natural persons who ultimately owns or controls are identified identify the natural persons having executive authority in the legal person, or in equivalent or similar positions;

ii. for customers that are legal arrangements-

- for trusts, identify the settlors, the trustees, the protector (if any), the beneficiaries (including every beneficiary that falls within a designated

characteristic or class) [3]and any natural person exercising ultimate ownership, ultimate control or ultimate effective control over the trust (including through a chain of control or ownership); and

- for other types of legal arrangements, identify persons in equivalent or similar positions, as those described above.

5. Where the customer is not a natural person, the company shall understand the nature of the customer's business and its ownership and control structure.
6. Pursuant to 6.16 of the Notice, the company shall not be required to inquire if there exists any beneficial owner (other than any end-user), in relation to a customer that is-
    a) a Singapore Government entity;
    b) a foreign government entity;
    c) an entity listed on the Singapore Exchange;
    d) an entity listed on a stock exchange outside of Singapore that is subject to –
        i. regulatory disclosure requirements; and
        ii. requirements relating to adequate transparency in respect of its beneficial owners (imposed through stock exchange rules, law or other enforceable means);
    e) Financial institutions
        i. Financial institutions that are licensed, approved, registered (including a fund management company registered under paragraph 5(1)(i) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations (Rg. 10)) or regulated by the Authority but do not include –
            - holders of stored value facilities, as defined in section 2(1) of the Payment Systems (Oversight) Act (Cap. 222A);
            - a person (other than a person referred to in paragraphs ii. and iii. (below) who is exempted from licensing, approval or regulation by the Authority under any Act administrated by the Authority, including a private trust company exempted from licensing under section 15 of the Trust Companies Act (Cap. 336) read with regulation 4 of the Trust Companies (Exemption) Regulations (Rg. 1).
        ii. Persons exempted under section 23(1)(f) of the Financial Advisers Act (Cap. 110) read with regulation 27(1)(d) of the Financial Advisers Regulations (Rg. 2).

[3] In relation to a beneficiary of a trust designated by characteristics or by class, the relevant holder shall obtain sufficient information about the beneficiary to satisfy itself that it will be able to establish the identity of the beneficiary (a) before making a distribution to that beneficiary; or (b) when that beneficiary intends to exercise vested rights

iii. Persons exempted under section 99(1) (h) of the Securities and Futures Act (Cap. 289) read with paragraph 7(1)(b) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations.

f) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF and document the basis of its determination that the requirements have been duly met;

g) an investment vehicle where the managers are financial institutions-

i. set out in Customer Due Diligence- acceptance of new business- policy- 6(e) (i) in this programme

ii. incorporated or established outside Singapore but are subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF,

unless the relevant holder has doubts about the veracity of the CDD information, or suspects that the customer, business relations with, or transaction for the customer, may be connected with money laundering or terrorism financing and the company shall document the basis of its determination that the requirements have been duly met.

7. In the case of a joint account, the company shall perform CDD measures on all of the joint account holders as if each of them were individually customers of the company.
8. The company shall, when processing the application to establish business relations, understand and as appropriate, obtain from the customer information as to the purpose and intended nature of business relations.
9. The company shall verify the information obtained is correct against the documents collected and do the membercheck screening for each entity and individual who is a signatory, customer or beneficial owner and record them in CDD portal.
10. Determine if the customer requires enhanced customer due diligence because of the following reasons: when the customer is a-

a. Politically exposed person-

i. The company shall use membercheck to determine if a customer, any natural person appointed to act on behalf of the customer, any connected party of the customer or any beneficial owner of the customer is a politically exposed person, or a family member or close associate of a politically exposed person.

ii. The company has adopted a risk-based approach in determining whether to perform enhanced CDD measures or the extent of enhanced CDD measures to be performed for -

- domestic politically exposed persons, their family members and close associates;
- international organisation politically exposed persons, their family members and close associates; or
- politically exposed persons who have stepped down from their prominent public functions, taking into consideration the level of influence such persons may continue to exercise after stepping down from their prominent public functions, their family members and close associates,

except in cases where their business relations or transactions with the company present a higher risk for money laundering or terrorism financing.

i. The company must in addition to performing the CDD measures, perform the following enhanced CDD measures where a customer or any beneficial owner of the customer is determined by the company to be a politically exposed person, or a family or close associate of a politically exposed person

i. obtain approval from the relevant holder's senior management to establish or continue business relations with the customer;

ii. establish, by appropriate and reasonable means, the source of wealth and source of funds of the customer and any beneficial owner of the customer; and

iii. conduct, during the course of business relations with the customer, enhanced monitoring of the business relations with the customer. In particular, the company shall increase the degree and nature of monitoring of the business relations with and transactions for the customer, in order to determine whether they appear unusual or suspicious.

b. Presents or may present a higher risk for money laundering or terrorism financing-

i. where a customer or any beneficial owner of the customer is from or in a country or jurisdiction in relation to which the FATF has called for countermeasures, the relevant holder shall treat any business relations with or transactions for any such customer as presenting a higher risk for money laundering or terrorism financing; and

ii. where a customer or any beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the relevant holder for itself or notified to relevant holders generally by the Authority or other foreign regulatory authorities, the relevant holder shall assess whether any such customer presents a higher risk for money laundering or terrorism financing.

11. Determine whether the applicant is a financial institution that proposed to have a correspondent banking relationship.

a. 'correspondent account services' means the provision of services under a cross-border relationship between the company and a respondent financial institution, for the relevant holder to provide access to a relevant stored value facility, whether for the respondent financial institution as principal or for that respondent financial institution's customers;

b. The company in Singapore shall perform the following measures, in addition to CDD measures, when providing correspondent account services or other similar services;

i. assess the suitability of the respondent financial institution by taking the following steps:

- gather adequate information about the respondent financial institution to understand fully the nature of the respondent financial institution's business, including making appropriate inquiries on its management, its major business activities and the countries or jurisdictions in which it operates;
- determine from any available sources the reputation of the respondent financial institution and the quality of supervision over the respondent financial institution, including whether it has been the subject of money laundering or terrorism financing investigation or regulatory action; and
- assess the respondent financial institution's AML/CFT controls and ascertain that they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which the respondent financial institution operates;

c. clearly understand and document the respective AML/CFT responsibilities of the company and the respondent financial institution; and

d. obtain approval from the company's senior management before providing correspondent account services or similar services to a new financial institution.

e. Where the correspondent account services or similar services involve a payable through account, the relevant holder shall be satisfied that-

   i. the respondent financial institution has performed appropriate measures at least equivalent to those specified in paragraph 6 of the Notice to Holders of Stored Value Facilities Monetary Authority Of Singapore Act, CAP. 186 on the third party having direct access to the payable-through account; and

   ii. the respondent financial institution is able to perform ongoing monitoring of its business relations with that third party and is willing and able to provide CDD information to the relevant holder upon request.

f. The company shall collect all documents which is required in paragraphs 11 (b) (c) (d) (e) and record them in CDD portal.

g. The company shall not enter into or continue correspondent account services or other similar services relationship with another financial institution that does not have adequate controls against money laundering or terrorism financing activities, is not effectively supervised by the relevant authorities or is a shell financial institution.

h. The company shall also take appropriate measures when establishing correspondent account services or other similar services relationship, to satisfy itself that its respondent financial institutions do not permit their accounts to be used by shell financial institutions.

12. The company must not establish or continue a business relationship with:

    a. a shell financial institution; or

    b. a financial institution that has correspondent banking relationship with a shell financial institution.

"Shell financial institution" means a financial institution incorporated, formed or established in a country or jurisdiction where the financial institution has no physical presence and which is unaffiliated with a financial group that is subject to effective consolidated supervision.

The company shall make sure that all financial institution customers must have policies prohibiting relationships with shell financial institutions.

13. New products, practices and technologies

    Before the company establishes a business relationship that involves new products, practices and technologies, the company shall identify and assess the money laundering and terrorism financing risks that may arise in relation to —

    a. the development of new products and new business practices, including new delivery mechanisms; and

    b. the use of new or developing technologies for both new and pre-existing products.

The company shall undertake the risk assessments, prior to the launch or use of such products, practices and technologies (to the extent such use is permitted by the Notice to Holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP. 186.), and shall take appropriate measures to manage and mitigate the risks.

The company shall, in complying with the requirements of paragraphs 5.1 and 5.2 of the Notice to Holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP. 186, pay special attention to any —

a. new products and new business practices, including new delivery mechanisms; and
b. new or developing technologies, that favour anonymity

This will be done on a case by case basis by the Compliance Officer unless the size of the affected transactions becomes significant.

14. Where the customer is a financial institution, a more detailed review of the background of the individuals associated with the applicant is required, including appropriate business, professional reference checking. The amount of background investigation required depends on the risk level of the customer and the customer's proposed business with the company. The company must be able to satisfy itself that it understands the ML/FT risk associated with the proposed business and that it has established that the risk is acceptable and that the backgrounds of the individuals associated with the customer are reasonably acceptable to the company. The following backgrounds are generally not acceptable to the company:
    a. Those with criminal convictions for money laundering offences
    b. Those with criminal convictions for selling, importing or exporting illegal drugs
    c. Those with criminal convictions for dishonesty offences within the last 10 years
    d. Those facing charges relating to the source of wealth that is connected to the funds that are proposed to be, have been, or are likely to be included in the funds that will end up in the customer account.
    e. Those with a significant number of criminal convictions over a substantial period of time
    f. Those with a significant history of misleading or deceptive business practices, insider trading, business disputes, bankruptcies etc. sufficient to cast serious doubt over the honesty and character of the person
15. The customer must not be restricted from having a business relationship with the company based on the country:
    a. In which the beneficial owners or signatories or persons on behalf of which the customer transacts or holds funds are nationals of or reside in

b. In which it carries on business
c. In which it invests
d. In which its suppliers or customers are based

16. For the purpose of the above policy, the company shall maintain a list of unacceptable countries, and for each country listed as unacceptable a description of the type of connection that is unacceptable and the rationale for the country being restricted in this way.
17. The customer must not be restricted from having a business relationship with the company based on any designation or sanctions or similar restriction applicable. These countries and these restrictions will be maintained in the same list mentioned above.
18. Where there is no policy in relation to any AML/CFT CDD or customer relationship issue, the Compliance Officer is entitled to make any decisions on the case and must have regard to industry practice, legal or AML/CFT advice, supervisor advice if and as available or applicable. Where any exception is required to policy or procedure, this may be approved by the Compliance Officer provided it is not unlawful, and the exception must be recorded in a log in the company's AML/CFT records.

Procedure

To establish a business relationship with the company a customer must apply through standard forms or channels.

Any documents or evidence presented that is not in English must have a translation to English performed or certified by an acceptable certifier or other person adequately qualified and independent of the person/company to which the document and the translation relates. Where necessary the certifier or translator should be contacted to verify the authenticity of the certificate or translation.

On such application, the Compliance Officer or an authorised processing staff must assess the application as follows.

1. The company shall collect the basic information of the customer from CDD portal, EBANQ system or the application form and record them in CDD portal.
2. Identify the customer type. Is the customer an individual, legal person or legal arrangement or financial institution?
3. The purpose or rationale for the structure should be checked for comprehensibility and acceptability. If the structure's purpose or rationale is not clear, the company must probe and clarify the background of the structure and the people behind the structure to determine whether it cannot be credibly and acceptably explained. If the structure's purpose or rationale cannot be credibly and acceptably explained, the application must be rejected for this reason.
4. When the company establishes a business relationship with a new customer,

the company must identify the customers, natural person appointed to act on the customer's behalf, connected parties of the customer and the beneficial owners of the customer and the company shall collect following information and record them in CDD portal:

a. full name, including any aliases
b. unique identification number such as:
    i. an identity card number,
    ii. birth certificate number or
    iii. passport number, or
    iv. for the customer who is not a natural person:
        - the incorporation number or
        - business registration number;
c. the customer's –
    i. residential address; or
    ii. registered or business address, and if different, principal place of business,
d. date of birth for the natural person(s), beneficial owner(s) and
e. establishment, incorporation or registration date for legal person and legal arrangements; and
f. nationality for the natural person(s), beneficial owner(s) and
g. place of incorporation or place of registration for legal person and legal arrangements.

5. The company shall collect the certified documents to prove the personal identity of each customer type and upload them in CDD portal.
    a. The company must obtain any of the following document(s) to verify the name and date of birth of the natural person(s) and beneficial owner(s):
        i. Passport and
        ii. national ID card, or
        iii. Birth certificate or
        iv. Driver's licence
    b. To verify the address of the customer the company shall accept any of the following:
        i. passport,
        ii. national ID card,
        iii. driver licence,
        iv. utility bill,
        v. bank statement,
        vi. tenancy agreement,

vii. land title,
viii. rates notice,
ix. tax notice or correspondence.

c. Assess the applicant's legal form. If the customer is a legal person or legal arrangement, the company must identify the legal form, constitution and powers that regulate and bind the legal person or legal arrangement, the business registration number or incorporation number, place of incorporation or place of registration from the following documents:
   i. certificate of incorporation,
   ii. certificate of registration,
   iii. company extract,
   iv. certificate of incumbency
   v. the constitution or memorandum and articles of association
   vi. operating agreement (for LLCs) and
   vii. any shareholder agreement,
   viii. the partnership agreement,
   ix. the trust deed,
   x. the foundation charter,
   xi. Any other constitutional document
d. The company shall also need to collect the nationality of the natural person(s), and beneficial owner(s) and following documents can be used to verify the nationality:
   i. Passport/ travel document
   ii. Birth certificate
   iii. Citizenship certificate
   iv. National Identity card
e. Where the customer is a legal person or legal arrangement, the company shall identify the connected parties of the customer. The connected party can be defined as follows:
   i. director or any natural person having executive authority (other than partnership)
   ii. any partner or manager for partnership
   iii. any natural person having executive authority in the legal arrangement

   The company shall collect the below given information of the connected party of the customer:

   i. full name, including aliases; and

ii. unique identification number such as an identity card number, birth certificate number or passport number.

The company shall collect passport and birth certificate or national id card or driver's licence to obtain the name and unique identification number of the connected party.

f. The signatory's relationship to the customer must be recorded, and, according to the level of risk involved, the signatory's authority to act on behalf of the customer must be verified. The level of risk varies according to the customer type. The company shall verify the signatory who act on behalf of the customer as per the procedure of new customer's verification stated in Policy 3 and 4. The company must understand the authority of the signatory by any of the following documents;

i. The customer who is an individual, signing the application form authorising the signatory to act on his behalf,

ii. The entity documents showing the signatory's position and authority to bind the customer entity,

iii. the resolution of the board of directors to appoint the signatory to act on behalf of the customer, or

iv. the power of attorney issued by the customer which gives the authority to act on behalf of the customer.

6. Beneficial ownership

a. Beneficial owner, in relation to a customer of the company, means the natural person who ultimately owns or controls the customer or the natural person (including the end-user) on whose behalf a transaction is conducted or business relations are established, and includes any person who exercises ultimate effective control over a legal person or legal arrangement.

b. The company shall identify the natural person who is acting alone or together who ultimately own the legal person according to documents mentioned in 4(c) of the procedures of Customer Due Diligence- Acceptance of New Business.

Ownership interests:

i. Companies/corporations: Any individual who singly holds more than 50% of the ordinary shares or membership interest in the company or corporation

ii. Partnerships: any individual who singly holds more than 50% of the capital interests in the partnership, or more than 50% of the profit interests in the partnership

iii. Trusts: any individual who has a vested interest in more than 50% of the net assets of the trust

iv. Foundations: any individual with a vested interest in more than 50% of the net assets of the foundation

v. Any other entity: any individual with a legal or equitable right to more than 50% of profits, capital or distributions.

c. If the company cannot identify a natural person who ultimately own the legal person, then company needs to identify a natural person who ultimately controls the legal person. This can be done by collecting and verifying the documents mentioned in 4(c) of the procedures of Customer Due Diligence- Acceptance of New Business.

Control interests:

i. Companies/corporations: any individual who is sole director, sole managing member, or who holds more than half of the voting interests in the company or corporation, or who holds the right to appoint more than half of the company's or corporation's directors or managers, or who holds a General Power of Attorney to act for and bind the company or corporation.

ii. Partnerships: any individual who is the General Partner, or controls a general partner and any individual who holds a General Power of Attorney to act for and bind the partnership.

iii. Trusts: any individual who is sole trustee, or is sole managing trustee, or any individual who controls such a trustee. Any individual who holds a General Power of Attorney to act for and bind the Trustee(s) in respect of the trust. Any individual who, under the terms of the trust, has the power to revoke the trust as the settlor of the trust. Any individual who has so many rights or powers under the terms of the trust, e.g. protector, powers to replacement of trustees, powers to determine the investment or operating policies of the trust etc. so as to give that individual effective control over the trust.

iv. Foundations: any individual who is sole councillor of the foundation, or who is the managing councillor of the foundation, or holds a General Power of Attorney to act for and bind the foundation. Any individual who, under the foundation charter, has so many rights as protector, replacement of members of the council, or to control investment or operating policies etc. so as to give that person effective control over the foundation.

v. All entity types: any other means by which an individual has effective control over the entity.

Note: For the purpose of measuring control interests, interests held by any individual in his personal capacity must be aggregated with the same individual's interests held by any trustee or nominee that he is a beneficial owner of, and any other entity of which he is a beneficial owner, e.g. Corporate directors/trustees/general partners

d. In case the company cannot identify a natural person who ultimately owns or controls the legal person, the company shall identify the person who has executive authority in the legal person according to the documents mentioned in 4(c) of the procedures of Customer Due Diligence- Acceptance of New Business.

7. The company shall identify and verify the customer when establishes a business relationship with a customer in non-face-to- face situation as per the procedure 3 of acceptance of new business and confirm the identity by:
   a. Telephone call to the customer using a publically verifiable phone number (e.g. white-pages listing)
   b. Skype or other video call (e.g. facebook) where we can verify that the person is the person on the identity document (i.e. the person's appearance matches the identity document)
   c. Sending a letter to the person's address in the population register (or equivalent verified official address)
8. The company shall maintain the report of the PEP screening of the customer in CDD portal system.
9. All the verification documents must be uploaded in CDD portal system and must be retained. If the person's identity has been confirmed by using skype or facebook etc. a screen shot must be taken and attached in the CDD system as evidence this step has been done – this should show the image of the person's face.
10. All the documents must be certified and must be translated to English if not in English.
11. Collect the residence and nationality of the customer to ensure that he/she is not from any prohibited or restricted country.
12. The company shall maintain a list of high risk as well as prohibited and restricted country according to the Singapore Law.
13. The company must do risk assessment for the customer and if the risk assessment is high, the customer shall be subject to the enhanced customer due diligence process. The documentation can be done on the CDD portal for the decision on the same.

14. When a business relationship is established or an individual transaction is carried out with a natural person who is not physically present, the company must do risk assessment process. If the customer is on low or medium risk, they shall be exempt from the enhanced customer due diligence. If the customer is on high risk, the company shall require the customer to fill out the enhanced customer due diligence form and the details obtained from the form can be used to make subjective decision.
15. Verification of certificates or references is only required where there are additional indicators of business or AML risk, or as part of any research required into the customer's background or proposed business activities
16. If there is a need of additional verification, the documents of verification must be collected and attached in CDD Portal.
17. Any verification of certifiers and referees needs to meet these standards:
    a. The identity and standing of the certifier or referee should be confirmed from independent sources. e.g. professional organisation membership list, regulatory licensee list, etc.
    b. The contact details of the certifier or referee should be obtained from public sources. e.g. white pages, yellow pages to ensure that the person being contacted is the professional or certifier listed.
    c. The certifier or referee should be contacted by telephone or email and requested to confirm the authenticity of the reference given.
18. All the verification must be done before the business relationship is established and all verification documents must be uploaded in CDD portal and retained it for further review.
19. The company may establish business relations with a customer before completing the verification of the identity of the natural person, signatory appointed to act on behalf of the customer and beneficial owners of the customer if-
    a. the deferral of completion of the verification is essential in order not to interrupt the normal conduct of business operations; and
    b. the risks of money laundering and terrorism financing can be effectively managed by the company.
20. The company shall complete verification of the identity of a customer as required by paragraph 6.9 of the Notice to Holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP. 186 natural persons appointed to act on behalf of the customer as required by paragraph 6.10(b) of the Notice to Holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP. 186 and beneficial owners of the customer as required by

paragraph 6.14 of the Notice to Holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP. 186 before the company establishes business relations with the customer.

21. Where the company establishes business relations with a customer before verifying the identity of the natural person, signatory appointed to act on behalf of the customer, and beneficial owners of the customer, the company shall:
    a. the deferral of completion of the verification is essential in order not to interrupt the normal conduct of business operations; and
    b. the risks of money laundering and terrorism financing can be effectively managed by the company.
22. Customers cannot be accepted pending completion of customer due diligence, the process must be complete and the application approved before the account can be activated.
23. Where the company is unable to complete the measures as required by paragraphs 6, 7 and 8 of the Notice Holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP. 186, it shall not commence or continue business relations with any customer, or undertake any transaction for any customer. The company shall consider if the circumstances are suspicious so as to warrant the filing of an STR.
24. For the purposes of paragraph 6.34 of the Notice Holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP. 186, completion of the measures means the situation where the company has obtained, screened and verified (including by delayed verification as allowed under paragraphs 6.32 and 6.33 of the Notice Holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP. 186) all necessary CDD information under paragraphs 6, 7 and 8 of the Notice Holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP. 186, and where the company has received satisfactory responses to all inquiries in relation to such necessary CDD information.
25. The company shall identify if the customer qualifies for simplified customer due diligence.
    a) The company may perform simplified CDD measures as it considers adequate to effectively identify and verify the identity of a customer, any natural person appointed to act on behalf of the customer and any beneficial owner of the customer (other than any beneficial owner that the relevant holder is exempted from making inquiries about under paragraph 6.16 of the Notice to Holders of Stored Value facilities Monetary Authority of Singapore Act, CAP. 186) if it is satisfied that the risks of money laundering and terrorism financing are low.
    b) The assessment of low risks shall be supported by an adequate analysis of risks by the company.

c) The simplified CDD measures shall be commensurate with the level of risk, based on the risk factors identified by the company.

d) The company shall not perform simplified CDD measures-

   i. where one or more transactions undertaken by the company for a customer (other than transactions undertaken by the company transfer funds from the customer's relevant stored value facility directly to that customer's bank account) in any one year period cumulatively exceeds S$5,000;

   ii. where a customer or any beneficial owner of the customer is from or in a country or jurisdiction in relation to which the FATF has called for countermeasures;

   iii. where a customer or any beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the relevant holder for itself or notified to relevant holders generally by the Authority, or other foreign regulatory authorities; or

   iv. where the company suspects that money laundering or terrorism financing is involved.

e) A transaction undertaken by the company to transfer funds from a customer's relevant stored value facility directly to that customer's bank account shall not be a transaction for the purposes of paragraph 7.4(a) of the Notice to Holders of Stored Value facilities Monetary Authority of Singapore Act, CAP. 186, if that the bank account is not opened or maintained in a country or jurisdiction known to have inadequate AML/CFT measures (as determined by the company for itself or notified to company generally by the Authority or by other foreign regulatory authorities).

f) Subject to paragraphs 7.2, 7.3 and 7.4 of the Notice to Holders of Stored Value facilities Monetary Authority of Singapore Act, CAP. 186, the company may perform simplified CDD measures in relation to a customer that is a financial institution set out in policy 6 (f) of the customer due diligence- acceptance of new business.

g) Where the company performs simplified CDD measures in relation to a customer, any natural person appointed to act on behalf of the customer and any beneficial owner of the customer, it shall document -

   i. the details of its risk assessment; and

   ii. the nature of the simplified CDD measures.

h) The company must determine if the customer qualifies for simplified due diligence by collecting adequate documentary evidence of its status from the applicant or from public sources. If the customer qualifies for simplified customer due diligence.

26. Determine if the customer is a financial institution.

a) A financial institution means a person who, in the ordinary course of business, carries on 1 or more of the following financial activities:

i. accepting deposits or other repayable funds from the public:

ii. lending to or for a customer, including consumer credit, mortgage credit, factoring (with or without recourse), and financing of commercial transactions (including forfeiting):

iii. financial leasing (excluding financial leasing arrangements in relation to consumer products):

iv. transferring money or value for, or on behalf of, a customer:

v. issuing or managing the means of payment (for example, credit or debit cards, cheques, traveller's cheques, money orders, bankers' drafts, or electronic money):

vi. undertaking financial guarantees and commitments:

vii. trading for the person's own account or for the accounts of customers in any of the following:

- money market instruments (for example: cheques, bills, certificates of deposit, or derivatives):
- foreign exchange:
- exchange, interest rate, or index instruments:
- transferable securities:
- commodity futures trading:

viii. participating in securities issues and the provision of financial services related to those issues:

ix. managing individual or collective portfolios:

x. safe keeping or administering of cash or liquid securities on behalf of other persons:

xi. investing, administering, or managing funds or money on behalf of other persons:

xii. issuing, or undertaking liability under, life insurance policies as an insurer:

xiii. money or currency changing

b) A shell bank is defined as a corporation that—

Shell financial institution" means a financial institution incorporated, formed or established in a country or jurisdiction where the financial institution has no physical

presence and which is unaffiliated with a financial group that is subject to effective consolidated supervision.

c) The company shall make sure that all financial institution customers must have policies prohibiting relationships with shell financial institutions. The definition of a shell financial institution is, included in the policy above.

d) To prove the customer is not a shell financial institution, the company shall collect an evidence of adequate local presence. For this the company maintains local presence declaration form which should be signed by the proposed financial institution. The nature of local banking operations, local presence of the bank and local management must be clear to the company and the documents of verification must be uploaded in CDD portal.

e) If the customer is a shell financial institution, or it holds a banking licence in its country of incorporation but cannot produce adequate evidence it is not a shell financial institution, it cannot be accepted.

f) the company shall:

   i. use the application form to gather enough information about the nature and purpose of the respondent's business, including whether it is subject to AML/CFT regulation and if so under which laws, whether it is subject to AML/CFT supervision and if so the name of the AML/CFT supervisor(s).

   ii. rely on the membercheck to determine the reputation of the respondent including whether the respondent has been subject to a money laundering or financing of terrorism investigation or regulatory action. The application form requests the applicant to disclose any publically verifiable sources that show its supervised status for AML/CFT and if provided these must be checked.

   iii. collect and analyse the AML/CFT compliance program, risk assessment and its audit report to assess the adequacy and effectiveness of the applicant's AML/CFT controls. A Wolfsberg Questionnaire is also used to assist this process. The responses on the Wolfsberg questionnaire must be checked against the AML programme documentation or other documents provided to confirm that the answers provided are substantiated. Any non-standard answers are not acceptable and the applicant must be advised about the nature of the problem and given an opportunity to amend their controls to bring them up to Wolfsberg group standards.

   iv. require approval from the senior management, for financial institution customers.

v. AML/CFT responsibilities of the company and the respondent financial institutions are set out in the terms. These include responsibility of the respondent financial institution to comply with the laws it is subject to (or otherwise adopt adequate AML/CFT controls) and the provision of originator data in the appropriate form for wire transfers.

vi. identify all signatories with direct access to company accounts the same as any other signatory. The company shall not provide direct access to the customers of its respondent financial institutions to the respondent's accounts with company.

27. The company must check if the customer requires for enhanced customer due diligence. Enhanced Customer Due Diligence usually requires:

a. when the company establishes a business relationship with a customer, natural person appointed to act on behalf of the customer, any connected part of the customer or beneficial owner of the customer that is a politically exposed person or family member or close associate of a politically exposed person.

i. the company shall do memebercheck to identify if a signatory, an individual customer or any beneficial owner is a politically exposed person as soon as practicable before or after establishing a business relationship,

ii. In such circumstances, the company shall obtain the approval from the senior management of the company in order to establish or continue the business relationship with the customer,

iii. The source of wealth and source of funds of the customer and beneficial owner of the customer must be collected and record them in CDD portal, generally the company can collect any of the following document(s) to get the information of source of fund or wealth:

- a declaration of trust or nomine agreement, in relation to nominee shareholders, showing who they hold or act for
- the trust deed showing who settled the trust
- the bank statement showing the source of income or wealth of the customer
- business plan
- documents confirming the source such as a sale of a house, sale of shares, receipt of a personal injuries award, a bequest under an estate or a win from gambling activities,
- any other relevant evidence that proves the source of fund or wealth.

iv. conduct, during the course of business relations with the customer, enhanced monitoring of the business relations with the customer. In particular, the bank shall increase the degree and nature of monitoring of the business relations with and transactions for the customer, in order to determine whether they appear unusual or suspicious.

b. Receives an application from a person of a country which has a higher risk for money laundering or terrorism financing.

c. where a customer or any beneficial owner of the customer is from or in a country or jurisdiction in relation to which the FATF has called for countermeasures, the company shall treat any business relations with or transactions for any such customer as presenting a higher risk for money laundering or terrorism financing; and

d. where a customer or any beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the company for itself or notified to relevant holders generally by the Authority or other foreign regulatory authorities, the relevant holder shall assess whether any such customer presents a higher risk for money laundering or terrorism financing.

i. When the company receives an application of a customer who is mentioned in 22 (b), (c) and (d) of the procedure of Customer due diligence- acceptance of new business, proceed to 11 of the procedure of Customer Due Diligence- Acceptance of new business.

ii. Identify the jurisdiction the entity is formed, registered or incorporated in. Check the jurisdiction against the list of unacceptable jurisdictions. Applicants from such jurisdictions cannot be accepted.

iii. When the company assess the application of a customer from a country that has insufficient AML systems, the company shall use FATF [4]as a credible source to identify the countries which lacks adequate AML/CFT systems/ measures or controls. The company maintains a list of affected countries for this purpose. If the country is mentioned on the list, the applicant is subject to enhanced CDD and the if the country is not mentioned in the list, the company shall not perform enhanced CDD to accept the application of the customer.

28. All the verification documents must be uploaded in CDD portal for further review.

[4] http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/

29. Before the company establishes a business relationship that involves new or developing technologies, or new or developing products, that might favour anonymity, the company must,
    a. the company shall rely on the application form to identify if the proposed business relationship uses or intend to use new or developing technologies or new or developing products or new delivery mechanisms that might favour anonymity,
    b. the company uses internet technology to facilitate business with customers on a non-face-to-face basis,
    c. the company shall follow the procedure of ongoing CDD to identify any material change in the nature and purpose of the business relationship,
    d. annual review of low, medium and high risk customers and account and transaction ongoing monitoring will help the company to identify if there is any involvement of new or developing technologies or products,
    e. the company shall keep up-to-date of the new products and technologies, which may favour money launderers and terrorist financers.
30. Assess the application as a whole. If there is enough information to accept the customer and the customer is acceptable, accept the customer and open the account(s). If there is indications of higher risk, or if the information provided is inadequate to assess the risk level and to meet legal requirements, advise the customer that more information is required and make a list of all information and evidence likely to be required to assess the application.
31. When adequate information is received to make a decision on the application, make a decision and communicate this to the customer and ensure that the assessment and basis for the decision, and the supporting documents are properly recorded and filed.
32. For new accounts opened, assign the customer to an expected account turnover band to allow ongoing monitoring of transaction levels.

Control

The Customer Service Representative is responsible for day to day operation of the procedures. The Compliance Officer is responsible for supervising the Customer Service Officer and making decisions on applications that require senior management approval.

The assessment and supporting documents is uploaded to the customer profile in CDD portal, the customer relationship management software that holds the customer information.

Customer due diligence – ongoing relationships, material change to nature or purpose of the business relationship

Policy

1. The company shall monitor on an ongoing basis, its business relations with customers.
2. According to the size and complexity of the business, the company shall monitor its business relations with customers and detect and must make sure to report suspicious, complex, usually large or unusual patterns of transactions.
3. The company shall perform the measures as required by paragraphs 6, 7 and 8 according to the Notice to Holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP. 186 in relation to its existing customers based on its own assessment of materiality and risk, taking into account any previous measures applied, the time when the measures were last applied to such existing customers and the adequacy of data, documents or information obtained.
4. If there is a material change in the nature or purpose of the business relationship, ***and*** the company considers that it has insufficient information about the customer, the company must conduct customer due diligence again on the customer. This will generally be when:
    a) The customer requests a change to the signatory on the account as a result of the death or incapacity of the signatory. As part of the request, the customer provides us with information about a change to the business relationship, e.g. liquidating the company or closing the business operations.
    b) The customer requests a change to the signatory on the account as a result of a sale of the shares in the company, or a sale of the business, or having a new major shareholder.
    c) The company notices a material change to the customer's transaction patterns and wants to validate the information it holds about the customer's business or affairs.
    d) The company's transaction monitoring indicates a material change in the nature or purpose of the business relationship, and where there is unexpected higher risk transactions occurring, e.g. high value transactions with high risk countries.
    e) The customer advises us of a material change to the nature and purpose of the business relationship, and as a result the company considers that it has insufficient information about the customer.
5. Where there are changes in the customer situation that do not involve a material change in the nature and purpose of the business relationship, or where the company does not consider that is has insufficient information about the customer, the customer's details can be updated as required without completing the customer due diligence process. For example if the customer advises of a change of address or requests a new currency account this can normally be processed without doing CDD again.

Procedure

Collect (or check and update if required) and verify the following information on the customer and any signatories and beneficial owners:

1. Full name, including aliases
2. Unique identification number such as passport number, identity card number, birth certificate number.
3. Residential or registered or business address
4. Date of birth
5. The person's relationship to the customer (for persons who are not the customer)
6. Company number or registration number (if applicable)

The process should focus on re-validating the beneficial ownership of the customer to ensure all beneficial owners are named and identified. This can be done by requesting updated copies of the share register or register of members certified by the registered agent, or a certificate of incumbency issued after the changes were effected. Any new beneficial owners will need to be identified with certified documents as per the procedure on establishing a new business relationship.

Review of the customer's business activity and other aspects of the CDD process for new business are only required if and to the extent that this is appropriate in the situation. Where it is reasonable and acceptable to do so, existing customers are to be shown loyalty and flexibility, and so they should not have their business relationship terminated solely because the company would not accept them as a new business relationship.

Take the opportunity to review all customer profile data on file and update if/as necessary.

If it is necessary to terminate a business relationship because it can no longer be accepted, nevertheless the customer should where possible be given a reasonable notice period so that they can make other arrangements.

Control

The Customer Service Representative or AML/CFT compliance officer is responsible for conducting CDD on customers in these circumstances, however any customer service employee may identify situations where this policy is applicable and request updated documents from affected customers, and then escalate to the compliance officer for assistance if required.

Customer due diligence - account monitoring

Policy

Accounts monitoring occurs by reviewing account turnover every 3 months against the customer's assigned account turnover band.

Customers are placed into 3 broad account transaction volume ranges when the customer relationship begins, based on information provided by the customer.

The ranges are:

- Less than SGD10,000/month
- SGD10,000-100,000/month
- More than SGD100,000/month

Where the actual volumes exceed the ranges by more than 200%, or more than 200% above the previous monthly average in the case of the highest band, a review must be done to either:

1. Change the volume range assigned to the customer, or
2. Keep the volume range the same, or
3. Contact the customer to investigate their business or activity situation and, if applicable, complete the procedure for a material change in business relationship mentioned above.

The same applies where the actual volumes are less than 33% of the minimum of their existing range.

Procedure

A report is run after the end of each quarter identifying customers with account turnovers outside the ranges by more than the tolerances contained in the policy. The transaction activity is reviewed to determine if there is an apparent reason for the deviation, e.g. the sale of a building identified as such on the transaction records. If the reason for the deviation appears to be a non-recurring situation, the account band is left the same. If the reason for the deviation is apparent and acceptable from a review of the account, e.g. a growing business, the account band can be changed accordingly. If the review raises concerns about the adequacy of information the company holds, the customer will be contacted to discuss their account and to update existing information or add new information that adequately records the customer's business situation. If the account review raises reasonable grounds for suspicion of money laundering, the company must consider whether it is required to report any of the transactions as suspicious transactions, see below. In these circumstances the company must also seek source of wealth or source of funds information and evidence, see below.

Control

The Compliance Officer is required to run these reports and to complete the reviews required. Records of these reports and reviews must be kept.

Customer due diligence - Transaction monitoring

Policy

1. The company shall, during the course of business relations with a customer, observe the conduct of the customer's account and scrutinise transactions undertaken throughout the course of business relations, to ensure that the transactions are consistent with the company's knowledge of the customer, its business and risk profile and where appropriate, the source of funds.
2. The company shall pay special attention and inquire into the background and purpose of the to all complex, unusually large or unusual patterns of transactions, undertaken throughout the course of business relations that have no apparent or visible economic or lawful purpose and document its findings with a view to making this information available to the relevant authorities should the need arise.
3. Individual transactions, both incoming and outgoing, are monitored and reviewed if they exceed the following thresholds:

- Above SGD200,000
- Above SGD20,000, and involving a high risk country, or with missing or incomplete originator details on an incoming wire transfer

Procedure

The review procedure is:

1. Is this transaction within the known business of the customer? e.g. to a regular supplier or from a regular customer. If so, it is approved and processed as normal
2. Is the transaction unusual or unexplained? If so, contact the customer to ask for an explanation. If a reasonable explanation is given, it is approved and processed as normal.
3. Is the explanation unreasonable or doubtful? If so, request supporting evidence as to the nature of the transaction
4. Is the supporting evidence unavailable, refused, or suspicious? If so, consider whether there is reasonable grounds to file a suspicious transaction report. Consider whether the transaction should be accepted or processed. Consider whether the business relationship should be continued.

Control

Transaction processing employees can review and approve transactions in line with this policy and procedure. All affected transactions must be marked as identified for review to allow internal control and external auditing. Any transactions that cannot be approved on review are escalated to the

Compliance Officer for assessment and either processing or put on hold pending resolution of the concern.

Customer Due Diligence – customer information reviews

Policy

Financial institution customer accounts are subject to annual review, involving a discussion with the customer concerning their situation and activities and needs, and a request for evidence to confirm that the beneficial ownership details are still valid.

The annual review timing should be to coincide with the availability due date of the financial institution's annual report or review of its AML risk assess and compliance programme. The company must diarise, collect and review the financial institution's audits or inspections or annual reports of its AML compliance programme to ensure the company is aware of any issues identified and is satisfied with the financial institution's response to those issues.

Any customer classified as high risk is also subject to an annual review, involving a discussion with the customer concerning their situation and activities and needs, and a request for evidence to confirm that the beneficial ownership details are still valid.

Medium and low risk customers are subject to annual review involving a discussion with the customer concerning their situation, activities and needs. No evidence will be requested unless:

1. When questioned the customer discloses material changes to their situation, e.g. major change in shareholding
2. The company considers that the information should be supported with evidence.

Procedure

1. The company shall identify all financial institution customers and review their dates for annual review.
2. Review activity does not need to be done strictly one year from the date the business relationship commenced, but it should be done within 3 months of the anniversary of this date or the date of the anniversary of the last review.
3. Reviews can be done in conjunction with any customer service activity, and by customer service employees, and may also be done by the Compliance Officer.
4. An internet banking message should be sent to customers before the call is made, advising them about the upcoming review and the documents required. If this message is not read within 1 month, an email should be sent with the same content.

5. The company shall send the financial institution annual review form to the customers to collect the information to review.
6. At this time the company can also do ongoing CDD on the FI customers and collect the missing or additional documents.
7. The call should be made during an acceptable time where the person being called lives.
8. The company shall use the following table to assign the FI customers in different turnover bands based on their monthly transactions and do risk assessment and change their band in CDD portal or review the status if necessary.

Following table is used to assign the turn over bands for each customer type based on their monthly transactions in their account with the company.

Turn over bands	**Amount in SGD/month**
Band 1	< 10,000
Band 2	10,000-100,000
Band 3	100,000 – 500,000
Band 4	500,000 -2M
Band 5	Above 2M

The company uses the following table to understand the effectiveness of financial institution customer's AML controls.

Status	AML control
T1	Good, proven
T2	Medium
T3	Low

The company uses the customer's transaction, AML control, type of industry and the country(s) exposed to as a source to estimate the risks of each customer types.

9. The company shall upload any annual review report, audit or any other supporting documents in CDD portal. Also any pending or additional documents if necessary.
10. If the customer cannot be contacted for more than 1 month, for high risk customers the account can be blocked from making outgoing payments until the review is satisfactorily completed. Before the account is blocked, the customer must be sent a follow up email message advising of the issue and of the consequences of not completing the review and providing the supporting documents, and this message must be sent at least 2 weeks before the account is blocked. The account can be unblocked on an undertaking from the customer to complete the discussion promptly and supply the supporting documents within 1 month.

Control

The AML/CFT Compliance Officer is responsible for assigning risk levels to customers, coordinating the review programme, and making decisions about blocking accounts. Customer service employees can engage customers in discussions about their situation, checking and updating of information, and advising of supporting evidence required according to this policy. Customer service employees can unblock customer accounts unless the Compliance Office has put a note on the customer account prohibiting the account from being unblocked.

Suspicious Transaction Reporting

Policy

1. Where the company is unable to complete the customer due diligence measures for any customer type, it shall not commence or continue business relations with any customer, or undertake any transaction for any customer. The company shall consider if the circumstances are suspicious so as to warrant the filing of an STR.
2. The company shall keep in mind the provisions in the CDSA and in the TSOFA that provide for the reporting to the authorities of transactions suspected of being connected with money laundering or terrorism financing and implement appropriate internal policies, procedures and controls for meeting its obligations under the law, including the following:
    a) establish a single reference point within the organisation to whom all employees and officers are instructed to promptly refer all transactions suspected of being connected with money laundering or terrorism financing, for possible referral to STRO via STRs; and
    b) keep records of all transactions referred to STRO, together with all internal findings and analysis done in relation to them.

3. The company shall promptly submit reports on suspicious transactions (including attempted transactions), regardless of the amount of the transaction, to STRO, and extend a copy to the Authority for information.
4. The company shall consider if the circumstances are suspicious so as to warrant the filing of an STR and document the basis for its determination, including where-
   a) The company is for any reason unable to complete the customer due diligence measures for any reason,
   b) the customer is reluctant, unable or unwilling to provide any information requested by the company, decides to withdraw a pending application to establish business relations or a pending transaction, or to terminate existing business relations.
5. Where company forms a suspicion of money laundering or terrorism financing, and reasonably believes that performing any of the measures as required by paragraphs 6, 7 or 8 of the Notice to Holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP.186 will tip-off a customer, a natural person appointed to act on behalf of the customer, a connected party of the customer or a beneficial owner of the customer, the company may stop performing those measures. The company shall document the basis for its assessment and file an STR.
6. Where there are any reasonable grounds for suspicion that existing business relations with a customer are connected with money laundering or terrorism financing, and where the company considers it appropriate to retain the customer -

   (a) the company shall substantiate and document the reasons for retaining the customer; and

   (b) the customer's business relations with the company shall be subject to commensurate risk mitigation measures, including enhanced ongoing monitoring.
6. Where the company assesses the customer or the business relations with the customer referred to in paragraph 6.25 of the Notice to Holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP.186 to be of higher risk, the relevant holder shall perform enhanced CDD measures, which shall include obtaining the approval of the company's senior management to retain the customer

Confidentiality

The company has a ***strict duty of confidentiality*** in respect of all its applicants, customers and former customers which covers the customer details, beneficial ownership details, signatory details, transaction history, customer financial information and any credit limits or financial facilities the customer has or has had.

This strict duty has several exceptions, one of which is where the disclosure is required by compulsion of law. This is the exception relied on in this case. Disclosure at the discretion of the company is not permitted as this is inconsistent with and a breach of the company's strict duty of confidentiality. Accordingly the company must determine whether the disclosure is required by compulsion of law before filing any suspicious transaction report (STR).

Function of Confidentiality

The company recognises that the principal function of the strict duty of confidentiality is to protect sensitive information from being used to shame, embarrass, and discriminate against or to take civil or criminal legal action against customers, signatories and beneficial owners and anyone else connected to the customer's relationship with the company. Necessarily, confidentiality obligations protect embarrassing, adverse, shameful, civil liability supporting and incriminating information, as well as information that is innocuous.

Adverse Disclosure Policy

Before disclosing any customer information protected by confidentiality obligations to parties that are likely to use the information against the customer or any person connected to the customer relationship, for example disclosure to law enforcement, the company must:

1. Identify and confirm the availability of an exception to confidentiality that applies to the disclosure, AND
2. Ensure that the correct and adequate procedural requirements to permit or mandate this disclosure are followed strictly.

This policy applies to STRs.

Company Policy on Compliance with Rule

Transaction

Suspicious Transaction Reports (STRs) only apply to transactions and attempted transactions, they do

Procedure

Transactions to which the procedure may apply

Transactions which may be suspicious should be checked for reporting obligations in the following situations:

1. Inward wire transfer received that has missing or incomplete originator details.
2. When conducting ongoing customer due diligence including account monitoring, transaction monitoring and customer information reviews
3. When customer due diligence could not be completed because the customer refused or was unable to provide the necessary information or supporting evidence. This applies to both applications for new business relationships and reviews of existing relationships.
4. When completing any enhanced CDD in relation to a transaction or attempted transaction that is complex, unusually large or any unusual pattern of transactions.
5. Any other situation where the company becomes aware of a transaction that has features that result in suspicion of the relevant kind.

Transaction Selection

Only transactions identified as potentially suspicious are assessed using this full procedure. Simply because a transaction is unusual or subject to review or has an indication does not mean that it will be subject to the assessment procedure below. Based on experience and training on the AML Compliance Programme the Compliance Officer and other employees should have sufficient knowledge and awareness to identify transactions that require formal assessment under this procedure.

Reasonable Ground for Suspicion Assessment

Identify Indicators

All the transaction characteristics must be assessed against the indicators listed by the Financial Intelligence Unit's Suspicious Transaction Guideline 2013 (or any updated version). This will produce a list of indicators but the presence of one or more indicators does not, by itself, mean that the company has reasonable grounds for suspicion. These indicators are just some of the information that must be assessed to decide whether the company has reasonable grounds for the specific suspicions necessary to make the STR mandatory.

Identify the Covered Offence Type

The identification of the offence type relevant to the suspicion is necessary to test whether the company has an obligation to report the suspicion with an STR. If the offence type cannot be identified, the transaction cannot be suspected as relevant to an offence to which STR obligations may apply.

Forms

The company's forms should be used to follow the above procedures and complete and document the facts, indicators, identifications, assessments and conclusions made for STRs.

Making the STRs

The STRs must be made on the STROLLS system at the following address:

http://www.police.gov.sg/about-us/organisational-structure/specialist-staff-departments/commercial-affairs-department/aml-cft/suspicious-transaction-reporting-office/suspicious-transaction-reporting#content

If necessary, register the company as an entity, and proceed to fill out the details and submit the form.

Control

Transactions that may require this procedure can be identified by any employees performing duties of account and transaction monitoring and payment processing. All transactions that may require this procedure must be notified to the Compliance Officer who is responsible for completing the assessments and filing any STRs required.

Reliance on third parties

Policy

1. For the purposes of paragraph 9 of the Notice to holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP. 186, "third party" means financial institutions include:
    a) Banks in Singapore licensed under section 7 of the Banking Act (Cap.19).
    b) Merchant banks approved under section 28 of the Monetary Authority of Singapore Act (Cap. 186).
    c) Finance companies licensed under section 6 of the Finance Companies Act (Cap. 108).
    d) Financial advisers licensed under section 6 of the Financial Advisers Act (Cap. 110) except those which only provide advice by issuing or promulgating research analyses or research reports, whether in electronic, print or other form, concerning any investment product.
    e) Holders of a capital markets services licence under section 82 of the Securities and Futures Act (Cap. 289).
    f) Fund management companies registered under paragraph 5(1)(i) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations (Rg. 10).
    g) Persons exempted under section 23(1)(f) of the Financial Advisers Act read with regulation 27(1)(d) of the Financial Advisers Regulations (Rg. 2) except those which only provide

advice by issuing or promulgating research analyses or research reports, whether in electronic, print or other form, concerning any investment product.

h) Persons exempted under section 99(1)(h) of the Securities and Futures Act read with paragraph 7(1)(b) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations.

i) Approved trustees approved under section 289 of the Securities and Futures Act.

j) Trust companies licensed under section 5 of the Trust Companies Act (Cap. 336).

k) Direct life insurers licensed under section 8 of the Insurance Act (Cap. 142).

l) Insurance brokers registered under the Insurance Act which, by virtue of such registration, are exempted under section 23(1)(c) of the Financial Advisers Act except those which only provide advice by issuing or promulgating research analyses or research reports, whether in electronic, print or other form, concerning any investment product.

2. a financial institution which is subject to and supervised by a foreign authority for compliance with AML/CFT requirements consistent with standards set by the FATF (other than a holder of a money-changer's licence or a holder of a remittance licence, or equivalent licences).

3. Subject to paragraph 9.3, of the Notice to holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP. 186, the company may rely on a third party to perform the measures as required by paragraphs 6, 7 and 8 of the Notice to holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP. 186 if the following requirements are met:

a) the company is satisfied that the third party it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, and has adequate AML/CFT measures in place to comply with those requirements;

b) the company takes appropriate steps to identify, assess and understand the money laundering and terrorism financing risks particular to the countries or jurisdictions that the third party operates in;

c) the third party is not one which the company has been specifically precluded by the Authority from relying upon; and

d) the third party is able and willing to provide, without delay, upon the company's request, any data, documents or information obtained by the third party with respect to the measures applied on the relevant holder's customer, which the relevant holder would be required or would want to obtain.

4. The company shall not rely on a third party to conduct ongoing monitoring of business relations with customers.
5. Where a relevant holder relies on a third party to perform the measures as required by paragraphs 6, 7 and 8 of the Notice to holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP. 186 it shall:
    a) document the basis for its satisfaction that the requirements in paragraph 9.2(a) and (b) of the Notice to holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP. 186 have been met, except where the third party is a financial institution set out in Policy 1 of the Reliance on third parties; and
    b) immediately obtain from the third party the CDD information which the third party had obtained.
6. For the avoidance of doubt, notwithstanding the reliance upon a third party, the relevant holder shall remain responsible for its AML/CFT obligations in this Notice.

Procedure

1) The company shall collect adequate information of the third party and document the basis for its satisfaction that the requirements in paragraph 9.2(a) and (b) of the Notice to holders of Stored Value Facilities Monetary Authority of Singapore Act, CAP. 186 have been met, except where the third party is a financial institution set out in Policy 1 of the Reliance on third parties.
2) The company must make sure that the third party must hold a professional registration, recognised by the law of the country.
3) The company shall identify that the third party shall meet the customer due diligence requirements and book keeping requirements, asper the Singapore law.
4) Third parties must be informed by the company to make information available on request without delay to the institution or customer is being referred. Relevant documents on identification and verification of the person's or institution's or beneficial owner's identity should be forwarded to the customer is being referred.
5) Third party must keep the professional privacy of the data of the customer and it should not be disclosed to anyone unless and otherwise it is required by the government or by the compulsion of the law.
6) The company does not have to enter into an outsourcing agreement with a third party if the company itself can perform it.
7) The company shall not rely on third party to conduct ongoing business relations with customers.

Control

The AML/CFT compliance officer is responsible to get adequate information about the third party and decide to outsource customer due diligence. The AML/CFT compliance officer shall inform the rules and regulations on the privacy of the customer's data and documents.

Compliance Officer Appointment

Policy

The company must appoint an AML/CFT compliance officer who is, or who reports to a senior manager. The senior manager must be a director of the company. The compliance officer must have adequate experience, qualifications and/or training to perform the duties of the compliance officer to a high standard. The compliance officer must administer and maintain the AML/CFT programme of the company.

Procedure

The AML/CFT compliance officer must be officially appointed or designated by the company before the company commences business providing financial services.

Control

A copy of the appointment or designation must be attached to the compliance programme at the time programme is first issued.

Personal Data

Policy

1. The company shall not be required to provide an individual customer, a signatory appointed to act on behalf of a customer, an individual connected party of a customer or an individual beneficial owner of a customer, with-
    a) any access to personal data about the individual that is in the possession or under the control of the company;
    b) any information about the ways in which the personal data of the individual has been or may have been used or disclosed by the company; and
    c) any right to correct an error or omission of the personal data about the individual that is in the possession or under the control of the company.
2. The company shall, as soon as reasonably practicable, upon the request of an individual customer, an individual appointed to act on behalf of a customer, an individual connected party of a customer or an individual beneficial owner of a customer, provide the requesting individual with the right to-
    a) access the following types of personal data of that individual, that is in the possession or under the control of the company:

i. the full name, including any alias;

ii. unique identification number (such as an identity card number, birth certificate number or passport number);

iii. residential address;

iv. date of birth;

v. nationality;

vi. subject to section 21(2) and (3) read with the Fifth Schedule to the Personal Data Protection Act 2012 (Act 26 of 2012), any other personal data of the respective individual provided by that individual to the company; and

b) subject to section 22(7) read with the Sixth Schedule to the Personal Data Protection Act, correct an error or omission in relation to the types of personal data set out in subparagraphs (a)(i) to (vi), provided the relevant holder is satisfied that there are reasonable grounds for such request.

3. For the purposes of complying with this Notice, the company may, whether directly or through a third party, collect, use and disclose personal data of an individual customer, an individual appointed to act on behalf of a customer, an individual connected party of a customer or an individual beneficial owner of a customer, without the respective individual's consent.

Employee Vetting Programme

Policy

Senior managers, the AML/CFT compliance officer, and all employees who have AML/CFT duties must be vetted.

Procedure

Vetting must consist of a PEP check, and adequate business, employment or character references. Vetting must be done by the AML/CFT compliance officer. Records of the vetting activity and the results of the checks must be retained by the company in the employee file.

However, the founding director of the company who is drafting this programme and who has been subject to a criminal record check as part of the Financial Service Provider registration is not required to be vetted unless required by the AML supervisor or by a bank or financial service provider who the company has a business relationship with.

Control

The Compliance Officer is responsible for the performance of the vetting. No employees can commence any duties that include AML/CFT obligations until they have passed these checks.

Employee Training Programme

Policy

All employees who have AML/CFT duties must have training that covers:

1. AML/CFT laws and regulations, and in particular, CDD measures, detecting and reporting of suspicious transactions;
2. The contents of this programme, or as much of the programme is applicable to their duties,
3. prevailing techniques, methods and trends in money laundering and terrorism financing; and
4. The contacts and resources available should the employee need additional support to apply the programme or to resolve any problem with the programme or its application.

All employees including senior managers and the AML/CFT compliance officer must undertake initial and ongoing training, however the founding director of the company who is drafting this programme does not need to initial training, but must do ongoing training to keep up to date with AML/CFT issues so long as he is the Compliance Officer.

A training programme must be established to ensure that employees with AML/CFT duties maintain knowledge of the requirements, ability to comply with the AML/CFT obligations, and updates required by any changes to the laws, policies, procedures and risks.

Procedure

The company maintains an employee training program which is based on the Notice of Holders of stored value facilities Monetary Authority of Singapore Act, CAP. 186.

The training programme includes demonstration of the procedures and performance of the procedures on a test or example basis for the most important procedures relevant to the employee's duties.

The company follows a learning and development approach to training, based on each employee's development level and requires ongoing learning and progress measurement. These developments are part of each employee's performance measures, and are ongoing. The employee training program contains a chart of tasks and duties of each department of the company. This would give an idea of the responsibilities of each person (s) associated to AML/ CFT duties.

The company also maintains an employee training record which covers the names of each person related to the AML/CFT duties and their responsibilities. The trainer and the employee signs the record after they cover each training session. By maintain this record the company can ensure that each employee gets adequate training in their related areas.

External training opportunities are to be identified and where appropriate used to ensure that training benefits from industry practices where appropriate.

Controls

The Compliance Office is responsible for training all who require training. Records of the training given (including training materials used), the trainer, and coverage of the training and the learning results must be kept in the employee's file.

The training programme must be reviewed annually when this compliance programme is being reviewed. The review of the training programme must ensure that ongoing training is being given covering updates to laws, policies, practices and ML/FT risks.

Record Keeping

Policy

1. Customer and transaction records, including identity verification evidence, are to be maintained for at least 5 years after the transaction or after the account is closed.
2. Customer due diligence records on account opening must be uploaded to the CDD Portal, customer relationship management software by the customer and/or by the company employees as part of the new customer relationship activity.
3. Customer, account and transaction reviews must be loaded against the relevant customer and/or transaction in CDD portal.
4. Suspicious Transaction Reports made must be loaded against the relevant customer and/or account in CDD portal.
5. Employee vetting and training records must be retained in the employee files of the relevant employees.
6. The Compliance Programme, and Risk Assessment, including all versions, and notes on updates/changes, must be recorded in the AML folder on Google Drive.
7. Current and past versions of all restricted/approved countries lists, forms and supporting document templates etc. must be kept in the AML folder on Google Drive.
8. Documents must be retained for at least 5 years as required by the AML/CFT Act, or longer if required by any other law. The company does not have a policy of requiring destruction of documents or records when retaining them is no longer required.

Procedure

1. Customer due diligence records and documents must be recorded in or uploaded to CDD portal at the time the customer applies for the account and/or as part of the customer acceptance procedure.
2. The company shall retain every transaction record in NexorONE or EBANQ, online banking software.
3. The transaction records must contain the following information:
    a) the nature of the transaction:
    b) the amount of the transaction and the currency in which it was denominated:
    c) the date on which the transaction was conducted:
    d) the parties to the transaction:
    e) if applicable, the facility through which the transaction was conducted, and any other facilities (whether or not provided by the company) directly involved in the transaction:

f) the name of the officer or employee or agent of the reporting entity who handled the transaction, if that officer, employee, or agent—

g) has face-to-face dealings in respect of the transaction with any of the parties to the transaction; and

h) has formed a suspicion (of the kind referred to in section 40(1)(b)) about the transaction:

i) any other information prescribed by regulations.

4. CDD portal database records must be backed up on an at least business daily basis.
5. Customer, account and transaction reviews are to be recorded in or uploaded to CDD portal at the time review activity is taking place or concludes.
6. Suspicious Transaction Reports are to be uploaded against the customer or transaction at the time the reports are made.
7. Vetting and training records must be added to the employee files at the time the vetting activity is completed, or the training session(s) are completed.
8. Current and past versions of all restricted/approved countries lists, forms and supporting document templates etc. must be added to the AML folder in Google Drive at the time they are updated or approved for use.

Control

The Compliance Officer is responsible to oversee record keeping activities and compliance therewith.

Management of ML/FT risks

Policy

The company manages ML/FT risks by:

1. Assessing ML/FT risks of customers at the time they apply for a banking relationship, as documented in the Customer Due Diligence – acceptance of new business. Where the risks is assessed as high, the business will be subject to additional monitoring.
2. Assessing ML/FT risks of existing customers and transactions in an ongoing manner, as documented in the Customer Due Diligence - ongoing relationships, material change to nature or purpose of the business relationship, Customer Due Diligence – account monitoring, Customer Due Diligence – transaction monitoring and Customer Due Diligence – customer information reviews policies and procedures detailed above. Where the risk of ML/FT is unacceptably high, customer relationships can be discontinued and/or transactions refused.
3. Collecting and maintaining all information and evidence required by law to ensure this information is available for law enforcement purposes where disclosure for this purpose is legally required.

Procedure

The procedures for these policies are documented in the relevant parts of this Compliance Programme.

Control

The controls for these policies and procedures are documented in the relevant parts of this Compliance Programme.

Monitoring and Managing Compliance with Programme

Policy

The company reviews the operation of and compliance with the programme annually as part of the annual report and the company reviews the risk assessment at the same time.

External audit of the operation of and compliance with the programme, and the risk assessment is required every 2 years, or on request of the supervisor, the Monetary Authority of Singapore.

The company must take prompt and effective action to address any issues found on review.

Procedure

The Compliance Officer must review:

1. The adequacy of the record keeping and information system(s) that are used to maintain the information and documents that are required by law or by this programme, and their adequacy for control purposes, and for audit purposes.
2. The way the compliance programme is operating, and the most significant issues of concern about its adequacy, effectiveness, costs and/or reliability.
3. How the programme and the operation of the programme compare to industry practice, and best practice, and the expectations of the institutions we deal with.

The Compliance Officer must prepare a review report at the same time as or as part of the Annual Report required by the company's supervisor, Monetary Authority of Singapore.

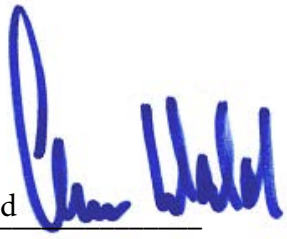
Control

The Compliance Officer is responsible for performing these reviews.

Compliance Officer of the company

The company hereby appoints Cem Wald Geb. Büyükgüner, the first AML/CFT Compliance Officer of the company. This appointment is to meet the requirement of the Notice to holders of stored value facilities monetary authority of Singapore Act, CAP. 186.

The AML/CFT Compliance Officer hereby issues this new AML/CFT Compliance Programme effective from 17th February 2017 as version 1 of this document.

Signed 

Name: Cem Wald

Position: Director

Date: 17 Feb 2017

Duties

The duties of the AML/CFT Compliance Officer are:

1. To administer and maintain the company's AML/CFT programme
2. The incorporation by the company of its AML/CFT obligations into its core business systems and controls
3. Considering and deciding on any exceptions to policy and documenting any decisions approving such action
4. Assessment of new business applications, and documenting assessments and decisions made
5. Completing CDD on existing customers who require this to be done again
6. Completing account monitoring reports and activities
7. Handling transaction monitoring reviews requiring approval
8. Assigning risk levels to customers, coordinating the review programme, and making decisions about blocking accounts
9. Assessing and reporting suspicious transactions
10. Vetting new employees
11. Training employees on AML/CFT obligations and duties and policies and procedures
12. Oversight of record keeping systems and activities related to AML/CFT
13. Completing reviews and the AML/CFT programme Annual Report
14. Assisting the auditor and providing explanations and evidence of the compliance with and operation of the programme.