COPYRIGHT

Document Version Control Log

Ver. No.	Change Summary	Change Owner	Date Approved
1-2013	Release of AML/CFT Staff and FAR Handbook	Silas Tan (Compliance)	July 2013
1-2014	Annual Updates of AML/CFT Manual:- (a) Universal change of department name from Compliance to Risk Management & Compliance (b) Amendments in accordance to AML/CFT Gap Analysis 2014 (c) Inclusion of Paragraph 13 – Information Technologies and paragraph 14 – Personal Data (d) Other minor changes.	Jayce Tan / Daniel Lim / Nancy Tan	October 2014
1-2015	Revisions of MAS FAA-N06:- (a) Additional definition of Political Exposed Person ("PEP") (b) Additional safeguards for Suspicious Transactions Reporting Addition of Section 15, AML/CFT Related Offences and Penalties	Javier Heng / Marc Ma	August 2015
2-2015	Addition of Identification of Beneficiary	Javier Heng	December 2015
1-2016	Addition of PIAS's Internal Policy on LTC in the Army and Superintendent in the Police Force to be considered as PEP	Puay Hoon	August 2016

1-2017	Annual Updates of AML/CFT Handbook: (a) Change in requirement of Corporate Customer Due Diligence (b) Inclusion of requirements for 'Cheques, Cashiers Order and I-Banking Submission' under Section 4 Customer Due Diligence (c) Change in minimum number of years for retention of documentation (d) Provide clearer interpretation of military officials under the 'Prominent Public Functions' per PIAS' policy	Jafmine Tan	October 2017
1-2018	Merge Section 10 - Reporting Procedures into Section 9 - Guidelines on Suspicious Transactions Included new section: Section 10 – Guidelines on Fraud	Jafmine Tan	August 2018
2-2018	Insert new Section 16 – Raising Queries and Reporting Concerns	Jafmine Tan	December 2018
1-2019	Updated Section 8.2 – ECDD requirements for High-Risk Countries and Jurisdiction	Kenneth Goh / Frankie Tan	December 2019
1-2021	Updated Section 10 - Guidelines on Fraud and Section 16 - Raising Queries and Reporting Concerns Included new appendices: Appendix 4 and Appendix 5	Mei Na Chua	October 2021
1-2022	Added Section 16 - Raising Queries and Reporting Concerns - Reporting Via 'Speak Out Charter and the review of Annual Updates of AML/CFT Handbook.	Maisuri Abdul Karim	April 2022

1-2023	Annual Review	Tang Ming Yang / Maisuri Abdul Karim	November 2023
1-2024	Inserted new Section 11 – Guidelines on Sanction Included new appendix: Appendix 6 – Proliferation Financing Typologies/Indicators Updated Section 5 – Beneficial Owner, Legal Arrangement and Legal Person Updated Section 8.2C: Removal of Non-Profit Organisations from List of High-Risk Occupations/Industries	Tang Ming Yang/ Mei Na Chua	June 2024

Table of Contents

1 Introduction

1.1 Singapore is an active participant in the global fight against money laundering and terrorism financing. Singapore has been a Financial Action Task Force (FATF) member since 1991 and a member of Asia/Pacific Group on Money Laundering since its inception in 1997. Singapore's comprehensive legal, institutional, policy and supervisory framework to combat money laundering and terrorism financing was endorsed under the IMF/World Bank Financial Sector Assessment Program (FSAP) in August 2003.

1.2 In Singapore, the legislation, regulations and notices governing the prevention of money laundering and countering the financing of terrorism ("AML/CFT") for Financial Advisers are the:

a) Monetary Authority of Singapore Act (Cap. 186);
b) Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A);
c) Terrorism (Suppression of Financing) Act (Cap. 325);
d) MAS Notice FAA-N06 Prevention of Money Laundering and Countering the Financing of Terrorism – Financial Advisers; and
e) MAS Notice FAA-N17 Notice on Reporting of Suspicious Activities & Incidents of Fraud.
f) Guidelines To MAS Notice FAA-N06 On Prevention of Money Laundering and Countering The Financing of Terrorism

1.3 This handbook provides guidance to all staff and Financial Adviser Representatives ("FARs") of PIAS on:

1.3.1 What is money laundering/terrorist financing;
1.3.2 The need to guard against it;
1.3.3 The money laundering risks associated with PIAS' operations;
1.3.4 Your role and responsibilities as a staff/FARs of PIAS; ands.
1.3.5 Possible suspicious transactions.

1.4 Reference to 'Politically Exposed Persons (PEP's)' in the manual includes 'Related Close Associates (RCAs)" who are natural persons connected to a PEP either socially or professionally.

2 Description of Money Laundering

2.1 **Money laundering** is a process intended to mask the benefits derived from drug trafficking, terrorism, or other criminal conduct so that they appear to have originated from a legitimate source.

2.2 Generally, the process of money laundering comprises of three stages:

a) **Placement** - The physical disposal of the benefits of criminal conduct;

b) **Layering** - The separation of the benefits of criminal conduct from their source by creating layers of financial transactions designed to disguise the audit trail;

c) **Integration** - The provision of apparent legitimacy to the benefits of criminal conduct. If the layering process succeeds, the integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds.

2.3 Due to the limitations of Financial Advisers in receiving information on 'exit' type of transactions from product providers, PIAS will predominantly be focusing our AML/CFT efforts on the "Placement" stage.

3 Description of Terrorist Financing

3.1 Terrorism seeks to influence or compel governments into a particular course of action or seeks to intimidate the public or a section of the public through the use or threat of violence, damage to property, danger to life, serious risks to health or safety of the population or disruption of key public services or infrastructure.

3.2 Terrorists require funds to carry out acts of terrorism and terrorist financing provides the funds needed. Sources of terrorist financing may be legitimate or illegitimate. It may be derived from criminal activities such as kidnapping, extortion, fraud or drug trafficking. It may also be derived from legitimate income such as membership dues, sales of publications, donations from persons or entities sympathetic to their cause, and sometimes income from legitimate business operations belonging to terrorist organizations.

3.3 Terrorist financing involves amounts that are not always large, and the associated transactions may not necessarily be complex given that some sources of terrorist funds could actually be legitimate.

3.4 However, the methods used by terrorist organizations to move, collect, hide or make available funds for their activities remain similar to those used by criminal organizations to launder their funds. This is especially so when the funds are derived from illegitimate sources, in which case, the terrorist organization would have similar concerns to a typical criminal organization in laundering the funds. Where the funds are derived from legitimate sources, terrorist organizations would usually still need to employ the same laundering techniques to obscure or disguise the links between the organization and the funds.

4 Customer Due Diligence ("CDD")

4.1 PIAS shall complete verification of the identity of the customer before[1]:

[1] MAS Notice FAA-N06, paragraph 6.30

a) establishing any business relations with any customer; or
b) undertaking any transaction for a customer, where the customer does not have business relations with PIAS.

4.2 Under no circumstance will PIAS establish any business relations with a person on an anonymous basis or using a fictitious name[2].

4.3 Where PIAS is unable to complete CDD measures, it shall terminate the business relationship and consider if the circumstances are suspicious so as to warrant the filing of a Suspicious Transactions Report ("STR").

4.4 The identity of the customer is to be verified using reliable, independent sources to ensure that the information is authentic, before commencement of business relations. The duty of verification falls on the FARs. Examples of documents include original identity card and passport.

Individual Customers

4.4.1 The FARs shall verify the identity of individual customers (who are natural persons) and/or natural persons appointed to act on behalf of the individual customers by obtaining the following information:

a) Full name, including any aliases;
b) Unique identification number (to provide a certified true copy of photographic identity card, passport, or equivalent for unique identification number verification);
c) Existing residential address;
   - Provide proof of residential address if the address is not reflected on identification document. Examples of legitimate documents include bank statements and utility bills, etc.
d) Date of birth;
e) Nationality; and
f) For customers who appoint Natural Persons to act on behalf of him/ her, verification of due authority is required by providing photographic identification (e.g. NRIC or passport), and documentation proof of appointment. For example, legal documents such as Power of Attorney and specimen signature (where applicable).

4.4.2 The identity verification under paragraph 4.4.1 also applies to joint-account holders and a customer who is a sole-proprietor of a business.

Corporate Customers

[2] MAS Notice FAA-N06, paragraph 6.1

4.4.3 The FARs shall verify the identity of corporate customers (who are not natural persons) by obtaining the following information:

a) Full name, including any aliases and former corporate names;
b) Unique identification number (such as the incorporation number or business registration number);
c) Existing registered or business address;
d) Date of incorporation or registration;
e) Place of incorporation or registration; and
f) Ownership and control structure (ACRA Bizfile or equivalent document)

4.4.4 For corporate and other business customers, the FARs shall also obtain the following document(s), where applicable:

a) For local companies, the Bizfile or ACRA Business Report (within 6 months validity) showing the Company name, incorporation number, registered address, directors and shareholders;
b) For foreign companies, valid Certificate of Incorporation and Certificate of Incumbency. Alternatively, a document equivalent to Singapore's ACRA Business Report; and
c) Photographic identification (e.g. NRIC or passport with proof of address), specimen signatures and documentation proof of appointment of natural persons that act or are appointed to act on behalf of the corporate customer.

4.4.5 Where the customer is a Singapore government entity, only information that confirms the customer is a Singapore entity is required to be obtained.

Cheques, Cashiers Order and I-Banking Submission

4.4.6 Where the mode of payment is in the form of a cheque, FARs are strongly encouraged to submit **a photocopy of the cheque** to Business Support department in relation to the transaction. RM&C will request for a copy of the cheque from the FARs in the event it is unavailable for the purpose of AML/CFT review.

4.4.7 Where the mode of payment is in the form of a Cashier's Order, FARs are strongly encouraged to submit:

(a) a photocopy of the Cashier's Order; AND
(b) a carbon copy of the application form for Cashier's Order in respect of the transaction.

RM&C will request for the above 2 documents from the FARs in the event they are unavailable for the purpose of AML/CFT review.

4.4.8 Where the mode of payment is in the form of I-Banking, FARs are strongly encouraged to submit the relevant document that reflects the payor of the transaction:

(a) any document that reflects the name of the payor i.e. bank transaction records (hardcopy statement or print screen)

RM&C will request for the above document from the FARs in the event they are unavailable for the purpose of AML/CFT review.

4.5 All documents in foreign languages (non-English), e.g. bank letters or proof of address etc., shall be translated by independent third parties. These may include official translators, government officials or members from the notary public etc. Both the documents in foreign language and the translated documents should be submitted to Business Support for record purposes.

4.6 PIAS shall, as soon as a beneficiary of a life policy is identified to the Financial Adviser as a specifically named natural person, legal person or legal arrangement, obtain the full name, including any aliases, of such beneficiary.

4.7 PIAS should obtain sufficient information concerning the beneficiary such as full name, identification number, date of birth and address to satisfy that the direct life insurer will be able to establish the identity of the beneficiary at the time of payout.

5 Beneficial Owner, Legal Arrangement and Legal Person

5.1 Definitions of the terms “Beneficial Owner”, “Legal Arrangement” and “Legal Person” as per FAA-N06

(a) “Beneficial Owner”- in relation to a customer of a financial adviser, means the natural person who ultimately owns or controls the customer or the natural person 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) “Legal Arrangement” means a trust or other similar arrangement

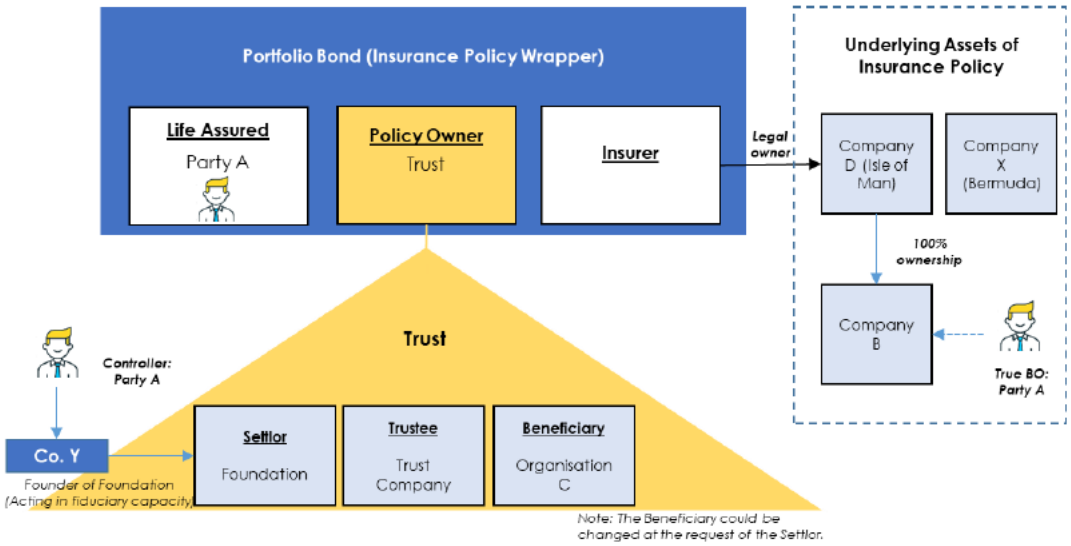
(c) “Legal Person” means an entity other than a natural person that can establish a permanent customer relationship with a financial institution or otherwise own property

5.2 PIAS will inquire if there exists any beneficial owner in relation to a customer through the Financial Planner (Fact-Find Form). Where there is one or more beneficial owner in relation to a customer, PIAS shall take reasonable measures to obtain sufficient information to identify and verify the identity(ies) of the beneficial owner.

5.2 If the customer is not a natural person, PIAS shall better understand the nature of the customer’s business, ownership and control structure. This is because complex structures and arrangement pose additional money laundering/terrorism financing (“ML/TF”) risk concerns as it can be misused for illicit purposes. Below are some examples:

(a) Facilitate pass-through or round tripping transactions without any clear economic purpose. In some cases, these transactions were made with related entities or entities purported to be in the same industry to appear legitimate.

(b) Create complex layers of ownership with no clear legitimate reasons, but instead with the sole intention of obscuring true beneficial ownership.



The diagram above illustrates how complex wealth management insurance products and ownership structures could be abused to obfuscate the beneficial ownership (i.e. Party A).

5.3 Examples of red flags:

- Unusual or rapid changes to corporate structures, including beneficial ownerships, after account opening
- The BO owning a company through a nominee shareholder without a clear economic rationale or purpose
- A trust layer in the complex structure and the use of the Foundation as settlor of the trust for no legitimate reason
- Discrepancies in the purpose of the complex arrangements such as foundation as set out in the charter documents vis-à-vis your understanding of the client's purpose and nature of business relations
- The listing of an unrelated entity as Beneficiary for no legitimate reason

6 Name Screening

6.1 PIAS utilises a specialised commercial platform to screen all customers against Politically Exposed Persons (PEPs), Sanctioned, Terrorists, and High-Risk Persons list.

6.2 All customers (including persons appointed to act on behalf of customers, connected parties, beneficial owners, joint account holders, third party payor, director(s), partner(s), person(s) of

executive authority of corporate customer), PIAS FARs, staff and introducers are subject to screening.

6.3 The results of screening are used to inform a risk-based decision whether to engage in business with a client, associated person or other third party, or to participate in a business transaction.

7 Safeguarding Against the Laundering of Proceeds of Tax Crimes

7.1 Since June 2013, Singapore has updated the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 ("CDSA") by June 2013 to criminalize the laundering of proceeds from tax crimes committed with wilful intent. This comes after the MAS announcement in October 2011 that Singapore intends to implement the new recommendation by the FATF that jurisdictions designate serious tax crimes as predicate offences for money laundering.

7.2 PIAS shall give focus to any adverse information relating to any customer in relation to tax crimes. There shall also be appropriate affordability checks to ensure that customer's income and/or net worth commensurate with the premium or investment amount paid.

8 Enhanced Customer Due Diligence ("ECDD")

8.1 PIAS shall perform ECDD measures on PEPs, higher risk customers and/or when the beneficial owner is of higher risk (where applicable).

8.2 Staff and FARs shall give particular attention to business relations and transactions with:

a) Any customers, business relations or transactions where higher risk for money laundering and terrorist financing is present. Examples include:
- Cash-intensive businesses including money changers and casinos etc.
- Customers who are in a public position which could create a risk of exposure to the possibility of corruption - Please refer to Section 8.3 for "Politically Exposed Persons".
- Customers with potentially higher tax-risks

b) Any customer who is a national or resident or incorporated in a country/jurisdiction that is found in the PIAS List of High Risk Countries and Jurisdiction.
- All FARs and staff will be kept updated of any notice issued by MAS on the prohibition of transactions with countries and jurisdictions known to have on-going and substantial money laundering and terrorist financing (ML/FT) risks emanating from these jurisdictions.
  Upon discovery of such customers/ beneficial owners, the ECDD form is required to be completed by customer and submitted to Business Support along with the

lodgment documents, if any. This will then be forwarded to RM&C for further review.

C) Customer who is from a High-Risk Occupations/Industries subjected as High-Risk Customers ("HRCs"). HRCs will have to complete the Enhanced Client Due Diligence ("ECDD") form along with the SOW/SOF supporting documents.

- Consider customer's occupational profile (i.e., roles and type of businesses/ activities/ sectors) as a risk factor to identify HRCs.

Please refer to below table for the list of High-Risk Occupations/Industries:

S/N	Nature of Business	Occupation
1	Dealers in Precious Metals or Stones	- Directors/Senior Management (Precious Metals or Stones) - Buyer/Purchaser (Precious Metals or Stones)
2	Oil/Petroleum Industry	- Directors/Senior Management (Oil or Petroleum)
3	Money Services Business (exclude Banks)	- Money Changer - Debt Collector - Non-Office - Debt Collector - Office Based - Pawnbroker - Credit Controller - Moneylenders - Remittance Agents
4	Casino or Other Types of Gaming Operators	- Casino/Gaming/Gambling Worker - Directors/Senior Management (Casino or Gaming Operators)
5	Virtual / Digital Currencies	- Dealers/Traders of Digital/Virtual Currencies - Directors/Senior Management (Virtual / Digital Currencies)

Politically Exposed Persons

8.3 The definition of a "Politically Exposed Person"[3] includes:

(a) a natural person who is or has been entrusted with prominent public functions in Singapore or a foreign country;
(b) family members of such a person; or
(c) close associates of such a person.

[3] FAA-N06, paragraph 8.1

The revised MAS Notice FAA-N06 further categorises "politically exposed person" as a domestic politically exposed person, foreign politically exposed person or international organisation politically exposed person.

"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.

Note: PIAS's Internal Policy sets out the interpretation for military officials under the "Prominent Public Functions" as follows:

(a) Lieutenant Colonel (LTC) and above in the Army, Navy or Airforce; or
(b) Superintendent and above in the Police Force;
will be considered as PEP for the purpose of customer's declaration on PEP in the Financial Planner.

"Close associate" means a natural person who is closely connected to a politically exposed person, either socially or professionally;

"Family member" means a parent, step-parent, child, step-child, adopted child, spouse, sibling, step-sibling and adopted sibling of the politically exposed person;

The ECDD form is required to be completed for customers* who are PEPs and/or when the beneficial owner of the policy is a PEP. The completed form is to be submitted to Business Support along with the lodgment documents, if any, and this will then be forwarded to RM&C for further review.

** Including new and existing customers who are transacting with new monies and have not completed the ECDD form before. Completed ECDD form is valid for 1 year provided there is no material change to client's net worth.*

9 Guidelines on Suspicious Transactions

9.1 One of the ways to help detect suspicious transactions is to note transactions that are not typical of the business. ***Appendix 1*** provides a guideline to staff/FARs on what transactions are considered as suspicious. Whilst each scenario may not suggest the presence of AML/CFT activities, a combination of such scenarios when put together, may indicate suspicious activities. This list is not exhaustive and is limited only to the creativity and ingenuity of the money launderer and/or the terrorist.

9.2 If (a) any customer information/profile or any transaction raises suspicion of criminal activity, Money Laundering and/or Terrorist Financing, or (b) the customer is reluctant, unable or unwilling to provide any information requested by PIAS, decides to withdraw a pending

application to establish business relations or a pending transaction, or to terminate existing business relations, this shall be reported to the RM&C by filling in an Internal Suspicious Reporting Form ***(Appendix 2)*** **within 7 calendar days from discovery date**.

9.3 An assessment will be conducted by RM&C before escalation for Management's approval to file an STR.

9.4 Pursuant to FAA-N17, upon discovery of any suspicious activities and incidents of fraud where such activities or incidents are material to the safety, soundness or reputation of PIAS, the Company will file a report to MAS **within 5 working days after the discovery of the activity or incident**. The format for reference is found in ***Appendix 3***.

10 Guidelines on Fraud

10.1 Fraud can be defined as an act or omission intended to gain dishonest or unlawful advantage for the party committing fraud or for other related parties. In the case of insurance fraud, this would usually involve an exaggeration of an otherwise legitimate claim, premeditated fabrication of a claim or fraudulent misrepresentation of material information.

10.2 Insurance fraud can include the following:

(a) Policyholder and claims fraud **-** fraud against the insurer by the policyholder and other parties in the purchase and/or execution of an insurance product;
(b) Intermediary fraud - fraud by intermediaries against the insurer or policyholders; and
(c) Internal fraud – fraud against the insurer by its director or employee on his/her own, in collusion with parties internal or external to the insurer, or fraud perpetuated by any external party (e.g. accountants, auditors, consultants, claims adjusters) engaged as a service provider by the insurer.

10.3 Fraud poses a serious risk to the financial industry and policyholders. Fraudulent activities committed within or against PIAS can adversely affect PIAS' financial soundness and reputation. There may also be an indirect impact on the policyholders through premium increases arising from higher claims cost experienced by the insurer.

10.4 Pursuant to FAA-N17, upon discovery of any suspicious activities and incidents of fraud where such activities or incidents are material to the safety, soundness or reputation of PIAS, the Company will file a report to MAS **within 5 working days after the discovery of the activity or incident**. The format for reference is found in ***Appendix 3***.

10.5 Pursuant to MAS Notices FAA-N14 and 504, upon discovery of representative committing fraud, dishonesty, cheating, forgery, misappropriation of monies or criminal breach of trust, PIAS shall file a Misconduct Report, a copy of the police report along with the name of the police officer investigating the case, an update on the progress of the police investigation and result of the

criminal proceeding (if any) to MAS through MASNET **not later than 14 days after the discovery of the misconduct by the representative.**

This applies to representative who has ceased to be a representative as well, as the case may be, before the misconduct was discovered, or before disciplinary action has been decided upon or taken. If a police report was not lodged, PIAS should notify MAS of the reasons for its decision. The format for Misconduct Report is found in ***Appendix 4***.

If PIAS has not concluded its investigation or has not taken any disciplinary action against the representative concerned, PIAS shall submit an Update Report to MAS through MASNET to provide an update of the case as and when there is any significant development. The format for Update Report is found in ***Appendix 5***.

11 Guidelines on Sanction

11.1 Sanction is defined as an official order, such as the stopping of trade, that is taken against a country in order to make it obey international law. It includes a wide range of restrictive/coercive measures. They can include arms embargoes, travel or investment bans, financial sanctions (primarily asset freezes), reduced diplomatic links, reductions / cessation of any military relationship, flight bans, suspension from international organizations, withdrawal of aid, trade embargoes, restriction on cultural /sporting links, etc. Sanction is usually imposed with the goal of changing the behaviour of the target. For example, to penalize states for violating international law, to force a change in policies related to human rights or nuclear proliferation, or counter-terrorism or organized crime, to change the behaviour of a regime and to promote democracy, peace, and stability in a region.
Proliferation is defined by the Financial Action Task Force (FATF) as the illegal manufacture, acquisition development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, or biological weapons and their means of delivery and related materials.

Proliferation financing is defined by the FATF as the provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

11.2 Types of Sanctions

Sanctions are divided into 2 categories:

(a) Financial Sanctions

Restrictions put in place by the UN, EU or UK and other national governments to achieve a specific foreign policy or national security objective. They can either limit the provision of certain financial services or restrict access to financial markets, funds and economic resources.

(b)Trade Sanctions

Include restrictions on exports implemented for political reasons by countries and international organizations to maintain international peace and security. Sanctions measures include arms embargoes* and other trade control restrictions.

** An arms embargo is a prohibition or sanction against the export of weaponry and dual-use items - goods which have both a civil and military use. This can include raw materials to components and complete systems, such as aluminium alloys, bearings, or lasers. Dual use goods could also be items used in the production or development of military goods, such as machine tools, chemical manufacturing equipment and computers.*

11.3 A non-exhaustive list of indicators of Proliferation Financing, which are relevant for customer and transaction monitoring can be found in Appendix 6. It is limited only to the creativity and ingenuity of the proliferators to develop more sophisticated networks to hide such activities. Information contained in Appendix 6 is not uniquely determinative of proliferation financing, and proliferation financing activities may share similar traits with money laundering (especially trade-based money laundering) and terrorist financing activities.

12 Record Keeping

12.1 The following shall be maintained:

a) Customer due diligence information relating to the business relations and transaction undertaken in the course of establishing business relations as well as policy files, business correspondences and results of any analysis undertaken
➔ For a minimum of 7 years after termination of such business relations

b) Data, documents and information relating to transactions undertaken in the course of business relations, including any information needed to explain and reconstruct the transaction
➔ For a minimum of 7 years after the completion of transaction

12.2 Documentation can be maintained as originals or copies, paper or electronic form or on microfilm, as long as they are admissible evidence in a Singapore court of law.

12.3 Notwithstanding paragraph 11.1, records pertaining to a matter

a) which is under investigation; or
b) which has been the subject of an STR

shall be retained for as long as necessary, in accordance with any request or order from STRO or from other relevant competent authorities.

13 Training

13.1 This handbook is part of your training as staff/FARs of PIAS. Besides this handbook, you will be required to undergo other forms of training, such as AML/CFT induction training for new joiners/ representatives, AML/CFT refresher training via Learning Management System. This handbook, along with other trainings relating to AML/CFT which may be introduced to you in the course of your work, serve as reference material.

13.2 This handbook will be updated regularly to reflect current laws and regulations and company procedures, and you will be notified when changes are made. It is your responsibility to read this handbook regularly to educate yourself and maintain the necessary level of awareness of AML/CFT procedures.

14 Information Technologies

14.1 PIAS shall adopt a risk-based approach and take into consideration money laundering and terrorist financing risk that may arise from the use of new or developing technologies, especially those that favour anonymity, in formulating internal policies, procedures and controls.

15 Personal Data

15.1 For the purposes of complying with FAA-N06, PIAS shall not be required to provide a customer, including persons appointed to act on behalf of customers, beneficial owners, joint account holders, director(s), partner(s) and executive authority of corporate customer, staff, FARs and introducer with:

a) Any access to personal data about the individual that is in the possession or under the control of PIAS, except for;
   (i) full name, including any alias;
   (ii) unique identification number (such as NRIC number, birth certificate number or passport number);
   (iii) residential address;
   (iv) date of birth; and
   (v) nationality;

b) Any information about the ways in which the personal data of the individual mentioned above has been or may have been used or disclosed by PIAS; 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 PIAS, except for personal data mentioned in paragraph 15.1(a)(i) to (v) where PIAS is satisfied that there are reasonable grounds for such request.

15.2 For the purposes of complying with FAA-N06, PIAS may, whether directly or through a third party, collect, use and disclose personal data of a customer, including persons appointed to act on behalf of customers, beneficial owners, joint account holders, director(s), partner(s) and executive authority of corporate customer**,** staff, FARs and introducer, without the respective individual's consent.

16 AML/CFT Related Offences and Penalties

16.1 The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act ("CDSA"), is the primary legislation enacted to combat money laundering in Singapore. The CDSA criminalises the laundering of benefits or proceeds from predicate offences prescribed under the Act which include criminal conduct and drug trafficking committed in or outside of Singapore.

According to the provisions in the CDSA, it is an offence if any person(s):

a) assist another to retain benefits of drug dealing/to retain benefits from criminal conduct;
b) enter into or otherwise facilitate an arrangement knowing or having reasonable grounds to believe that another person has been/is involved in, or has benefited from drug dealing or criminal conduct;
c) facilitate to acquire, possess, use, conceal, convert, transfer or remove from jurisdiction any property which, directly or indirectly, represents another person's benefits of drug dealing or criminal conduct.

16.2 Any persons found to have committed the offences set out in the CDSA are liable to be punished with a fine not exceeding $500,000 or imprisonment for a term not exceeding 10 years, or to both. If the offence is committed by an entity other than an individual e.g. a company, the penalty is a fine not exceeding $1 million or twice the value of the property in respect of which the offence was committed, whichever is higher.

16.3 It is also an offence to withhold knowledge, suspicion or information on any act in the course of business or employment that may constitute drug dealing or criminal conduct.

16.4 Any person knowing or having reasonable grounds to suspect that an investigation under the CDSA is taking place/to take place and discloses to any other person information or any other matter which is likely to prejudice such an investigation will be guilty of an offence. Tipping off

constitutes an offence punishable by a fine not exceeding $250,000 or imprisonment for a term not exceeding 3 years, or to both.

16.5 The Terrorism (Suppression of Financing) Act 2002 ("TSOFA") was passed on 8 July 2002 by Parliament and it is an offence if any person is engaged in the following:

i) providing or collecting property (e.g. funds, assets, documents or instruments) for terrorist acts;

ii) provision of property and services for terrorist purposes;

iii) use or possession of property for terrorist purposes; and

iv) dealing with property of terrorists.

Any person who is guilty of the above offences shall be liable on conviction to a fine not exceeding $500,000 or to imprisonment for a term not exceeding 10 years or to both; or in any other case, to a fine not exceeding the higher of $1 million or twice the value of the property (including funds derived or generated from the property), financial services or other related services, or financial transactions in respect of the offence.

16.6 TSOFA not only criminalises terrorism financing but also imposes a duty on everyone to provide information pertaining to terrorism financing to the Authority. Failure to do so may constitute a criminal offence with a fine not exceeding $50,000 or to imprisonment for a term not exceeding 5 years, or to both. No criminal or civil proceedings shall lie against a person for any disclosure made in good faith.

16.7 Under the Reporting of Cross Border Movement of Physical Currency and Bearer Negotiable Instruments (CBNI) requirements, foreign visitors and Singapore residents will be required to make a declaration if the money they carry in or out of the country exceeds S$20,000. This requirement to submit a report, when stipulated amounts are exceeded, was put in place to detect and monitor the movements of CBNI and take enforcement actions against cash couriers supporting terrorism financing or money laundering activities.

"Bearer negotiable instrument" means a) a traveller's cheque; or b) any negotiable instrument that is in bearer form, indorsed without any restriction, made out to a fictitious payee or otherwise in such form that title passes upon delivery, and includes a negotiable instrument that has been signed but with the payee's name omitted. A person convicted of such an offence is liable to a fine of up to $50,000, an imprisonment term of up to three years, or both. The cash may be seized by CBNI if the person fails to provide the report.

Examples of negotiable instruments are a bill of exchange, cheque or promissory note.

17 Raising Queries And Reporting Concerns

17.1 In the event an employee or Representative considers that he/she has identified or is suspicious of any malpractice, either on the part of Management or by fellow colleagues or Representatives, they should contact the Head of Risk Management & Compliance.

17.2 Upon discovery of any incident of fraud, an employee shall inform risk team upon identification of risk event. On the other hand, Representatives shall report the incidence of fraud via GRC system (MetricStream) within 10 working days of discovery ***(Appendix 7)***.

17.3 Pursuant to FAA-N17, upon discovery of any suspicious activities and incidents of fraud where such activities or incidents are material to the safety, soundness or reputation of PIAS, the Company will file a report to MAS **within 5 working days after the discovery of the activity or incident**.

17.4 Pursuant to MAS Notices FAA-N14 and 504, upon discovery of representative committing fraud, dishonesty, cheating, forgery, misappropriation of monies or criminal breach of trust, PIAS shall file a Misconduct Report ***(Appendix 4),*** a copy of the police report along with the name of the police officer investigating the case, an update on the progress of the police investigation and result of the criminal proceeding (if any) to MAS through MASNET **not later than 14 days after the discovery of the misconduct by the representative.** This applies to representative who has ceased to be a representative as well, as the case may be, before the misconduct was discovered, or before disciplinary action has been decided upon or taken. If a police report was not lodged, PIAS should notify MAS of the reasons for its decision. If PIAS has not concluded its investigation or has not taken any disciplinary action against the representative concerned, PIAS shall submit an Update Report ***(Appendix 5)*** to MAS through MASNET to provide an update of the case as and when there is any significant development.

Reporting Via 'Speak Out Charter'

In order to provide employee with an alternative option, the Group has established the "Speak Out Charter", an externally provided service that allows you to report your concerns confidentially. All concerns raised through 'Speak Out Charter' are independently investigated by Group Internal Audit.

Employees should Speak Out when there is a concern on illegal or unethical practices, or wrong doings that affect others. This includes issues which could negatively impact our customers, the public, employees, or the Group.

There are various ways to raise our concerns via Speak Out:

a) Internally and Confidentially (confidential but non-anonymous);

I. Leader/Leadership Team
- Discuss concerns or potential issues with our leaders or the leadership team, unless the concern or issue is directly in relation to the leader or leadership team members

II. People Function

- When it is not easy to raise concerns or not appropriate to discuss the issue with leader or the leadership team, the concerns can be discussed with People Function

b) Speak Out channels managed by Ernst and Young (option for anonymity)

Concerns can be reported via the independent Speak Out channels managed by Ernst and Young (EY). There are five channels available (email, postal, telephone, voicemail or website) for us to report concerns confidentially and anonymously (if desired). The concerns received from EY are reported to Internal Audit who ensures concerns are investigated, concluded and reported appropriately. The channel can be assessed as follows:

Email:	reports@singlife-speakout.com
Postal Address:	Ernst and Young Singapore North Tower Level 18, 1 Raffles Quay, Singapore 048583 Reference: Stacy Chai
Telephone/Voicemail:	800 321 1465
Website:	www.singlife-speakout.com

c) Independently to Internal Audit (option for anonymity)

Concerns can also be shared directly to a member of Internal Audit.

The Group does not tolerate retaliation against employees who speak out, raising concern(s). If employees believe they have been unfavourably treated as a consequence of raising a concern, they should contact the Group Internal Audit who will independently review the circumstances and escalate to the Group Audit Committee where applicable. Disciplinary actions will then be meted out as appropriate in line with the Group's Grievance, Harassment & Disciplinary Policy. Group Internal Audit will treat all information confidentially, subject to legal obligations.

Money Laundering Reporting Officer ["MLRO"]

Following the reporting channel for any queries and/or concerns relating to AML/CFT:

Ms Kelly Lam
Head of Risk Management & Compliance
Email : kelly.lam@singlife.com
Phone : 6911 1259

APPENDICES

Appendix 1 - Guidelines on Suspicious Transactions

The list of situations given below is intended to highlight the basic ways in which money may be laundered through the use of financial products. While a solitary situation may not always be sufficient to suggest a suspicious transaction, repeated occurrences or a combination of such situations may necessitate a Suspicious Transaction Report to be filed.

A customer's declarations regarding the background of such transactions should be checked for plausibility. Not every explanation offered by the customer can be accepted without scrutiny.

It is reasonable to suspect any customer who is reluctant to provide normal information and documents required routinely in the course of the business relationship. Staff/FARs should pay attention to customers who provide minimal, false or misleading information or, when applying for a policy/buying an investment, provide information that is difficult to verify.

The following table illustrates possible typologies of suspicious transactions and is meant to be a guide. Staff/FARs will, however, be reminded that the following typologies are not meant to be exhaustive.

	Typologies of Suspicious Transactions
A.	**Transactions Which May Not Make Economic Sense**
1	A customer relationship with PIAS where the customer carries out frequent large transactions which are beyond the customer's apparent financial means (for example, customer requests for a single premium contract with large sum assured).
2	Transactions where the nature, size or frequency appears unusual, for example, a sudden request for a significant purchase of a lump sum contract from an existing customer whose current contracts are small and of regular payment only.
3	Transactions in which funds are received by way of a third party cheque, especially where there is no apparent connection between the third party and the customer.
B.	**Transactions Involving Large Sums or Cash**
1	Transactions where the customer makes a single payment exceeding $20,000 in cash.
2	Transactions in which funds are received from or paid to a customer's bank account in a financial haven, or in foreign currency, especially when such transactions are not consistent with the customer's transaction history.
3	Overpayment of premiums with a request to refund the excess to a third party or to a bank account held in a different country.
C.	**Transactions Involving Transfers Abroad**

	Typologies of Suspicious Transactions
1	A customer introduced by an overseas bank, affiliate or other customer, where both the customer and introducer are based in countries associated with (i) the production, processing or marketing of narcotics or other illegal drugs; or (ii) other criminal conduct.
D.	**Transactions Involving Unidentified Parties**
1	A customer, who is a natural person, for whom verification of identity proves unusually difficult and who is reluctant to provide details.
2	A customer, who is a corporation, where there are difficulties and delays in obtaining copies of the financial accounts or other documents of incorporation.
3	Assignment of a policy to unidentified third parties and for which no plausible reasons could be ascertained.
4	A number of policies taken out by the same customer for low premiums, each purchased with cash and then cancelled with return of premiums to a third party.
E.	**Other Type of Transactions**
1	Frequent changes to the address or authorised signatories.
2	The use of an address that is not the customer's permanent address.
3	A customer may exercise cancellation rights or cooling off rights (collectively known as free look) on life policies or unit trusts where the sum invested must be repaid (subject to any shortfall deduction where applicable). Free-look transactions could be suspicious if a policyowner exercises free-look on 3 or more policies owned.

Appendix 2 - PIAS Internal Suspicious Transaction Reporting Form

To: Risk Management & Compliance

Reporting Staff's/FAR's Particulars	
Name:	
Designation:	
Date:	
Signature:	
Customer's Particulars	
Name:	
NRIC/ Passport No./ Registration No.:	
Birth Date/ Registration Date *:	
Nationality/ Country of Registration *:	
Address:	
Telephone:	
Occupation/ Business Activities *:	
Policy Details	
Policy/Investment No.:	
Policy/Investment Name:	
Product Provider:	
Date of Commencement:	
Name of FAR:	
FAR's NRIC/Passport No.*: (If applicable)	
Sum Assured:	
Payment Mode:	Yearly/ Half-yearly/ Quarterly/ Monthly*
Premiums Payable (in Singapore Currency)	Regular/ Single*
Other Business Relationships:	

* Delete whichever is inappropriate

Suspicious Transaction		
Amount	**Date**	**Description of Transaction (E.g. Nature/Type of Transaction, Source of Funds, Destination, etc.)**
Reason(s) for Suspicion:		

Assessment by Compliance Department
☐ **REPORT** to STRO **STR Reference**: _____ **Remarks:**
☐ **DO NOT REPORT** to STRO **Reason(s) for not reporting**: **Follow-up Action**:
Name:

Date:
Signature:

Appendix 3 - Suspicious Activities and Incidents of Fraud Report

https://www.mas.gov.sg/-/media/mas/notices/pdf/notice-faan17.pdf - Form F1

Appendix 4 - Report on Misconduct of Financial Adviser Representatives / Broking Staff

https://www.mas.gov.sg/-/media/mas/sectors/notices/cmg/notice-faa-n14/faa_n14_rep.pdf

https://www.mas.gov.sg/-/media/MAS/Notices/PDF/MAS-504.pdf

Appendix 5 - Update on Report of Misconduct of Financial Adviser Representatives / Broking Staff

https://www.mas.gov.sg/-/media/mas/sectors/notices/cmg/notice-faa-n14/faa_n14_rep.pdf

https://www.mas.gov.sg/-/media/MAS/Notices/PDF/MAS-504.pdf

Appendix 6 – Proliferation Financing Typologies/Indicators

The following is a non-exhaustive list of indicators of Proliferation Financing, which are relevant for customer and transaction monitoring:

- The customer's transaction involves an individual or entity in a foreign country associated with proliferation and/or sanctions evasion concern;
- The customer or counterparty or its address is similar to one of the parties found on publicly available lists of persons who have been denied export licences, or has a history of export control contraventions;
- The customer's transactions involve possible shell companies (e.g. companies that do not appear to have real business activities in Singapore and display other shell company indicators);
- The customer is vague and resistant to providing additional information when asked;
- The customer has a sudden change in business activities.
- The customer is known or believed to have previous dealings with individuals or entities in countries subject to UNSC sanctions; or
- Sudden/frequent changes in directorship/authorised signatories which are not well-explained or intended to conceal links with individuals associated with sanctioned countries/activities.
- The customer's activity does not match its business profile or the end-user information does not match the end-user's business profile;
- The transaction involves designated persons;
- The transaction involves higher risk jurisdictions which are known to be involved in proliferation of weapons of mass destruction or proliferation financing activities;
- The transaction involves other financial institutions with known deficiencies in AML/CFT controls or controls for combating proliferation financing;
- The transaction involves possible shell companies (e.g. companies that do not have a high level of capitalisation or display other shell company indicators).

Appendix 7 - Guidance Notes

1) When an operational risk event happens:
   - Inform risk team upon identification of risk event
   - Log the risk event in the GRC system (MetricStream) single sign-on within 10 working days of discovery.
   - Understand the root cause of the error
   - Develop action plans to ensure such errors will not happen again
   - Confirmed or potential regulatory events/ breaches need to be escalated to Compliance.

2) Following are reportable operational risk events:
   a. Frauds
   b. Regulatory breaches
   c. Confidentiality or data breaches
   d. Adverse media reports
   e. Outage to services and/or systems resulting in disruption of services for > 2 hours (core services and critical systems)
   f. IT and cyber security incidents
   g. Losses/ near misses exceeding SGD 10K. For example,
      - Process execution error
      - Loss arising from product design flaws
      - Legal suits/ disputes taken by/ against the business unit

      Consult the Risk Management and Compliance team in case of doubt.

3) GRC system - Metric Stream Platform
   https://singlife.a09a.metricstream.com/metricstream/auth/dualLogin.jsp