Fraud Risk Management Policy

2024

Version Control

Revision Date	Version	Amendments	Author	Approver
01/06/2020	1	First Issuance to align to the Minimum Compliance Standards	Frankie Tan	PIAS Risk Committee
01/09/2022	2	Annual review	Tang Ming Yang / James Tan	PIAS Risk Committee
10/11/2023	2.1	Annual review	Tang Ming Yang / Maisuri Abdul Karim	PIAS Risk Committee
30/11/2024	2.2	Annual review	Tang Ming Yang / Maisuri Abdul Karim	PIAS Risk Committee

TABLE OF CONTENTS

1 Overview

1.1 Applicable Legislations

Professional Investment Advisory Services Pte Ltd ("PIAS") is committed to ensure compliance with all applicable regulations that may be issued by the relevant authorities in Singapore. The applicable local regulations for Financial Crime Management Policy ("Policy") are set out in Financial Advisers Act 2001 ("FAA"), Financial Advisers Regulations ("FAR") and its ensuing Notices/Guidelines.

Fraud is locally governed by the Financial Advisers Act 2001 ("FAA"), MAS FAA Notice 17 – Notice on Reporting of Suspicious Activities & Incidents of Fraud ("FAA-N17") and LIA MU 55/19 – Life Insurance Association guidelines on risk management practices in respect of life insurance intermediary fraud risk.

Frequency

This policy shall be kept up-to-date and reviewed annually, or when a material event occurs, whichever is earlier.

1.2 Group Financial Crime Policy

PIAS has a legal, moral and social responsibility to its customers, shareholders and employees to deter and detect those who seek to use our systems to facilitate financial crime. Violations of laws and regulations relating to financial crime may result in criminal, civil or regulatory penalties for Singlife Group, its directors and employees.

PIAS has zero tolerance for financial crime which includes bribery and corruption, facilitation of tax evasion, money laundering and terrorism financing, internal and external fraud, market abuse and economic sanctions violations. Violations of financial crime laws and regulations may result in criminal, civil or regulatory penalties for Singlife Group, its directors and employees.

Financial crime includes:

- Bribery and Corruption;
- Economic Sanctions Violations (including Proliferation Financing);
- Internal and External Fraud;
- Money Laundering and Terrorist Financing; and
- Facilitation of Tax Evasion.

PIAS is committed to comply with the Group's Financial Crime Policy and its relevant guidelines, procedures and risk preference statements and seeks to ensure that its businesses, products and

services are not misused for the purpose of money laundering, terrorism financing, sanctions, bribery and corruption, facilitation of tax evasion and fraud events.

PIAS strictly prohibits its directors, management, employees and financial adviser representatives from engaging in acts of financial crime and will investigate and support prosecution, where appropriate, of those who are involved. PIAS reserves the right to reject any customers, payment, or business(es) that is not consistent with Group's risk preference statements and aims to continuously strengthen their processes to ensure compliance with applicable laws and regulations.

Any waiver or deviation from this policy requires approval by Senior Management on reasonable grounds and needs to be in line with the Group Financial Crime Policy and all applicable regulations.

1.2.1 Reporting on Waiver/Deviation to Group Financial Crime

Any non-compliance with the policy must be immediately reported to PIAS CEO and PIAS Head of Risk Management & Compliance ("RM&C") stating the nature and reasons for the non-compliance. PIAS CEO and PIAS Head of RM&C will escalate incidents of non-compliance to the Group Head of Legal & Compliance as soon as possible, together with a remediation action plan.

1.3 Top-Level Commitment

PIAS Senior Management promotes an ethical and compliant culture to deter acts of financial crime. This includes enhancing awareness and reinforcing understanding of employees' personal responsibilities under the Group's Business Ethics Code and promoting an ethical and compliant culture in third parties that are carrying out, retaining or obtaining business on behalf of PIAS.

PIAS Senior Management sets the 'tone from the top' by communicating Group's approach to financial crime in line with Financial Crime Risk Preference Statements and Group's Business Ethics Code at least annually. Such communication shall explain Group's approach to financial crime; explain the consequences of breaching Group's standards; contain a commitment to carry out business fairly, honestly and openly; information on how to report financial crime; highlight mechanisms for confidentiality raising concerns through whistleblowing (e.g., Group's 'Speak Out Charter' programme); local regulatory requirements; promote a culture that financial crime is not acceptable.

The evidence of communication of the 'tone from the top' will be retained for at least 7 years.

1.4 Definition of Fraud

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.

1.4.1 The broad categories of insurance fraud include:

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

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 to the insurer

1.4.2 Any intentional wrongdoing intended to cause a financial loss but which is prevented by controls is still considered to be a fraud.

1.5 Risk Appetite Statements

PIAS aligns its internal risk appetite, and supporting policies, procedures and practices, to Group's Financial Crime Risk Preference Statements as follows:

- PIAS has no appetite for acts of fraud or dishonesty perpetrated by employees, directors orand representatives of PIAS.

- PIAS has no appetite for acts of fraud or dishonesty directed against or enabled through PIAS by customers, suppliers, distributors and third parties including those where PIAS has no business relationship.

- PIAS seeks a continually improving trend on instances of fraud loss or acts of dishonesty.

1.6 Employee Culture

The Head of Risk Management & Compliance ["RM&C"] shall ensure that all employees acknowledge and commit to Group's approach to financial crime risks via annual attestation to Business Ethics Code upon completion of Learning Management System/Essential Learning Course. The annual attestation and Learning Management System/ Essential Learning Course are applicable to existing and new employees, permanent or temporary contract workers including contractors. They are reminded that any financial crime related incident involving an employee will be considered gross misconduct and dealt with accordingly through the Group's disciplinary procedures.

In addition, in areas where there is higher risk of exposure to financial crime (for example through the Enterprise Wide Risk Assessment (EWRA) or occurrence of risk events), PIAS will consider to issue additional internal communications as part of an ongoing training and awareness programme.

Communication from Group Financial Crime is also available on Group's Business Ethics Code and employee handbooks.

The evidence of acknowledgement of the Code will be retained by PIAS for at least 7 years.

1.7 Third Party Culture

Where third parties are carrying out, promoting, obtaining or administering business on behalf of PIAS, PIAS function managing the third party relationship will take reasonable steps to ensure that the third party understands Group's approach to financial crime risks and has implemented appropriate procedures to mitigate these risks to PIAS.

PIAS will encourage all suppliers to sign up to the Supplier Code of Behaviour, where the supplier commits to complying with all applicable financial crime laws and regulations.

The Singlife Legal Counsel will ensure that the contract clauses, terms and conditions, statements of work, or other formal communication with those individuals or businesses acting on behalf of PIAS, includes references to Group's approach to financial crime.

In addition, where PIAS identifies areas as being of higher risk or exposure to financial crime, , PIAS will consider issuing additional external communication will be issued to emphasise PIAS approach to financial crime risk and consequences for non-compliance as well as raise awareness of expected Group financial crime compliance standards/ procedures/controls. The additional communications will demonstrate senior management commitment on the prevention of financial crime and reassure existing and prospective associated persons.

The evidence of communication to third parties and their formal acknowledgements (where applicable) will be retained for at least 7 years.

1.8 External Communications

The Head of Risk Management & Compliance identifies and documents any local regulatory or legal requirement for public disclosure of PIAS' approach to managing their financial crime risks.

2 Governance & Accountabilities

2.1 Risk Governance

PIAS Risk Committee is responsible for ensuring a strong and effective compliance culture is in place for the deterrence of financial crime activities.

PIAS is to ensure that business processes are robust and there are adequate risk mitigating measures in place. PIAS should:

a) receive sufficient, frequent and objective information to form an accurate picture of the financial crime risks including emerging or new ML/TF risks which PIAS is exposed to through its activities and business relations;

b) receive sufficient and objective information to assess whether controls are adequate and effective;

c) receive information on the legal and regulatory developments and understand the impact these have on the financial crime risk management framework; and

d) ensure that processes are in place to escalate important decisions that directly impact the ability of the business to address and control financial crime risks, especially where controls are assessed to be inadequate or ineffective.

2.2 Governance Responsibilities

PIAS Risk Committee provides oversight on the management of financial crime risk and ensure that any gaps or deficiencies identified from the risk assessment are addressed in a timely manner. The PIAS Risk Committee is required to escalate to the Board Risk Committee via the Group Head of Legal & Compliance on any financial crime breaches, control failures, issues and risks outside tolerance.

In addition, the PIAS Risk Committee will review and approve any financial crime policies and procedures as well as approve the approach for training, internal communications relating to financial crime. All public disclosures of matters relating to financial crime risk management (including publication on an external PIAS website) will be approved by Group Financial Crime.

An annual approval of the accountabilities and responsibilities (by PIAS Risk Committee) for PIAS' designated individual, the Money Laundering Reporting Officer ["MLRO"] and the Nominated Reporting Officer(s) are required. For PIAS, the designated individual and money laundering reporting officer are the same individual (i.e. the Head of Risk Management & Compliance). The Nominated Officer is the Risk & Regulatory Team Lead reporting to the Head of Risk Management & Compliance.

2.3 The Three Lines of Defence Operating Model

Roles and responsibilities of Three Lines of Defence:

First line of defence (1st LOD): Business Operations and Other Support Functions

- Financial Adviser Representatives, Operations, Training & Competency, Finance, Partnership Management, People Function, Adviser Maintenance Unit, Business Development and Channel Marketing and Transformation.

Roles and responsibilities include

- Risk identification, ownership, management and control, including a supportive risk culture
- Execute the requirements of an adequate and appropriate Financial Crime Risk Management Framework [FCRMF]
- Escalations to Risk & Regulatory Team (including appropriate reporting) where required in a timely, transparent and open manner
- Apply and execute the Group Financial Crime Risk policies as they apply to the Business Area
- Support a resourcing model adequate and appropriate to maintaining a Financial Crime Risk Management Framework
- Develop open communication channels with Second line of defence ("2nd LOD") to ensure specialist support, advice and guidance is obtained from financial crime compliance experts as required
- Partner with 2nd LOD to design and implement an assurance testing strategy and framework for all financial crime controls
- Ownership of all data
- Undergo annual financial crime training (minimally covering ML/TF) to be aware of the latest trends and developments and the related regulatory compliance obligations

Second line of defence (2nd LOD): Financial Crime Function

- Risk Management & Compliance

Roles and responsibilities include:

<u>Strategy</u>

- Define and implement a Financial Crime Risk Management Framework
- Provide insight, advice and guidance to the Group and Business on current financial crime regulatory, legal and industry challenges

<u>Advisory and Oversight</u>

- Design, implement and maintain a robust financial crime risk management control framework as well as ongoing monitoring of the relevant internal controls
- Monitor and review 1st LOD control adequacy and effectiveness and provide increasing oversight and challenge

- Remediate any non-conforming or ineffective systems and controls in 1st LOD and 2nd LOD
- Provide training and awareness on Financial Crime related matters
- Design and maintain the management information reporting framework
- Support a resourcing model to fulfil the Group Financial Crime Risk Management requirements and provide expert advisory support and guidance to 1st LOD

Policy
- Own and develop appropriate financial crime policies, standards and guidance as to how these should be interpreted and implemented
- Provide oversight, challenge and approval on all exceptions to financial crime policies and standards

Assurance
- Provide advice, guidance and support to 1st LOD testing and assurance activity

The Risk & Regulatory Team is responsible in alerting the board of directors and/or senior management if there is any reason to believe that the company's officers, employees or financial adviser representatives are failing or have failed to adequately address financial crime risks and there are concerns that PIAS had breached the applicable ML/TF laws and regulations.

While the other support functions also play a role in mitigating financial crime risks, the Financial Crime function is typically the contact point regarding all financial crime related issues for domestic and foreign authorities, including supervisory authorities and law enforcement authorities.
The Group Head of Legal & Compliance is responsible for escalating any material financial crime related risks or regulatory breaches to the Group CEO and to the Board Risk Committee.

Third line of defence (3rd LOD)
- Internal Audit

The Internal Audit function is responsible for undertaking periodic evaluation of the financial crime risk management framework and controls for the purpose of reporting to the Audit Committee. Such evaluations should at minimum cover ML/TF risks to assess:

a) the adequacy of ML/TF policies, procedures and controls in place for identifying ML/TF risks, addressing the identified risks and complying with laws, regulations and notices;

b) the level of compliance and effectiveness of the employees, officers and agents in implementing the policies, procedures and controls;

c) the effectiveness of the compliance oversight and quality control measures including parameters and criteria for transaction alerts; and

d) the effectiveness of the training of relevant employees, officers and financial adviser representatives.

Roles and responsibilities include

- Design, implement and maintain an audit plan to evaluate and provide independent assurance on the appropriateness, effectiveness and adequacy of financial crime policies, procedures, standards and financial crime risk management systems and controls
- Maintain the Whistleblowing communication channels
- Provide independent oversight and challenge of 1st LOD and 2nd LOD financial crime risk management control activities

2.4 Financial Crime Programme

The designated individual shall put in place an appropriate Financial Crime Programme and ensure compliance with applicable regulatory requirements and Group Financial Crime Policy.

Financial Crime Prevention Programme

- Financial Crime Business Standard Attestation for PIAS (MetricStream or equivalent)
- Annual Financial Crime Risk Assessment using the Group FC template
- Implementation of the Group Financial Crime Policy and Group Risk Assessment action plans
- Review of PIAS Gifts and Hospitality Register and Conflicts of Interest entries
- Bribery and Corruption Detection Checks – Review of Gifts and Hospitality expenses (including sponsorships and donations) in Finance
- Annual reminder to all staff on registering Gifts & Hospitality and Conflict of Interest
- Annual PIAS staff training
- Regular Tone from the Top emails on Financial Crime
- 'Speak Out Charter' whistleblowing in place
- Reporting of fraud incidents in PIAS to Group
- Business Ethics Code (annual staff sign-off)
- Timely resolution of any Financial Crime related audit issues
- Quarterly MI updates for PIAS Risk Committee
- Monthly Financial Crime Management Information submission for PIAS.
- Investigation and reporting of any instances of fraud, bribery & corruption, sanctions, money laundering or facilitation of tax evasion related issues to PIAS and where required escalation to Group Financial Crime.
- Perform risk assessment and report any true matches for Global Name Screening (GNS) for all categories (i.e. sanctions, Politically Exposed Persons) and High Risk Countries Jurisdiction Index to Group Financial Crime via monthly MI Reporting.

Financial Crime Oversight Activities with Business Units

- Monthly Financial Crime Training to New Representatives during Induction Training

- Facilitate/ follow up on issues relating to Global Name Screening (GNS), Fraud and Suspicious Transactions Reporting MI review
- Attend to Law Enforcement enquiries, where required

2.5 Review of Financial Crime Risk Management Programme

PIAS will review its financial crime risk management programme on a regular basis (at least annually), to ensure they are fit for purpose and reflect any changes to PIAS risk profile. Additional reviews will be instigated where there are significant changes to the business, such as a merger, acquisition, disposal, major new product line/customer proposition, business transfer/reorganisation, new geographical market, new or revised legislation and/or regulation etc. At a minimum, the review process will be documented at PIAS Risk Committee.

2.6 Notification of Appointments

PIAS will provide to Group Financial Crime details of the individuals appointed as the Designated individual, MLROs (or equivalent) and Nominated Officer (or equivalent).

Details will include the name of the individual(s); the names of the business areas for which they are responsible; date of appointment; confirmation of any regulatory approval required; confirmation of any regulatory notification required.

Notification to Group Financial Crime will occur on any subsequent change to the appointed individuals or their scope of responsibility.

2.7 Appointment of a Designated Individual

The PIAS Risk Committee must identify and appoint a member of the Senior Management as the Designated Individual, who will ultimately be accountable for financial crime risk management in PIAS. For PIAS, the Designated Individual is the Head of Risk Management & Compliance.

Where appropriate, PIAS may appoint additional designated individuals, provided that it is clear who has ultimate accountability for financial crime. All appointments must be approved by the PIAS Risk Committee.

To be able to adequately fulfil the role, the appointed person must:

a) understand the market/business/cell to which they have been appointed and how the financial crime legal, regulatory and internal policy requirements apply
b) understand the level of financial crime risk exposure within their market/business/cell

c) have an appropriate level of seniority, skills, knowledge and experience in implementing, maintaining and monitoring compliance with financial crime standards
d) have sufficient standing to act independently under his/her own authority

All appointments (including delegations) must be fully documented including details of accountabilities and responsibilities and must be agreed on at least an annual basis by the PIAS Risk Committee.

The CEO (or equivalent) must ensure that the role of 'Designated Individual' is covered at all times. Any gaps in coverage of over 1 month must be reported to the PIAS Risk Committee and Group Financial Crime, together with a plan for resolution.

2.8 Responsibilities of a Designated Individual

At a minimum, the responsibilities of the designated individual for financial crime risk management must include:

a) any local regulatory or legal accountabilities for financial crime
b) active involvement in financial crime risk management, supervision and critical decision-making processes
c) oversight and input into the design and ongoing review of local financial crime policies, procedures, systems and controls
d) being a key member of financial crime governance forums/committees
e) oversight of and involvement in the business/market/cell financial crime risk assessment(s) and reporting process
f) ensuring adequate financial crime resources are deployed to mitigate identified risks
g) demonstrating 'tone from the top' by embedding a culture of compliance, for example, through promotion of a zero tolerance appetite to acts of bribery and corruption by any person associated with PIAS
h) assessing and reporting on the adequacy of the financial crime risk management programme through ongoing testing, management information and board/committee reporting
i) ensuring the relevant local board(s) are adequately informed of internal and external financial crime developments
j) oversight of financial crime related breaches and the provision of feedback to board or equivalent on levels of compliance

The designated individual may delegate activities to other competent persons, however, the ultimate responsibility for the management of financial crime risk will remain with the designated individual. The responsibilities of the designated individual must be documented within their role profile or job description.

2.9 Designated Individual Review Process

The on-going appropriateness of the designated individual for financial crime risk must be assessed on a regular basis to ensure they remain appropriate for the role. This must include:

a) assessment through the annual performance management process (including any ad hoc performance issues)
b) consideration of suitability against the wider team's seniority, skills, knowledge and experience
c) evidence of continued senior management financial crime training and/or attendance at relevant financial crime events.

3 Risk Assessment

3.1 General Principles and Risk Assessment

In general, PIAS shall take appropriate steps to identify, assess and understand, its money laundering and terrorism financing risks in relation to the clients, the countries and jurisdictions the clients are from or in, and the products, services, transactions and delivery channels of PIAS.

PIAS shall document the risk assessment and consider all the relevant risk factors before determining the level of overall risk and the appropriate type and extent of mitigation.

PIAS shall exercise adequate due diligence when dealing with clients, natural persons appointed to act on the clients' behalf, connected parties of the clients and beneficial owners of the clients. This includes companies with bearer shares where identities of bearer shares must be made known to PIAS, and when there are changes to the ownership of these shares or named custodian.

Policies, procedures and controls must be properly developed, implemented and approved by the Senior Management to manage and mitigate the risks identified.

Where higher risks are identified, there should be enhanced measures and controls to mitigate these risks. The performance of the controls shall be reviewed on an annual basis for its effectiveness.

3.2 Enterprise-Wide Risk Assessment ("EWRA")

PIAS takes appropriate steps to identify, assess and understand its financial crime risk (or minimally the ML/TF risks) at the enterprise-wide level. The assessments for PIAS will be consolidated by Group so that the financial crime risks exposure may be evaluated. The enterprise-wide financial crime risk assessment will enable the Group and PIAS to better

understand its overall vulnerability to financial crime and to forms the basis for the overall risk-based approach across the Group.

The results of the reviews are documented and approved by PIAS senior management even if there are no significant changes to the enterprise-wide risk assessment. PIAS must give full support and active cooperation to the Group's enterprise-wide ML/TF risk assessment.

The assessment should be kept up-to-date and re-performed at least once every two years, or when a material trigger event occurs. Such material trigger events include but are not limited to:

- the establishment or acquisition of a new subsidiary; or
- the acquisition of new customer segments or new delivery channels, or the launch of new products and services by a subsidiary.

In performing the ML/TF aspects of the risk assessment, the following should be considered:

a) the ML/TF risk environment of the countries in which we operate (e.g. this information can be obtained from the Singapore's National Risk Assessment Report and in particular, the industry sectors and the crime types that present higher ML/TF risks);

b) the inputs from the Suspicious Transactions Reporting Office ("STRO") i.e. whether there is a high incidence of cases where we are instructed to take action to freeze assets;

c) the target customer segments and customer profiles such as those identified as politically exposed persons, those from higher risk industries or countries, the value of the transactions, etc;

d) the nature of products and services, i.e. whether the products carry a cash value or not, national insurance scheme versus voluntary life insurance, etc; and

e) the channels of distribution employed including whether they are subject to equivalent AML/CFT regimes.

3.3 Product Developments, Practices, Technologies and Customer Proposition Initiatives

On a regular basis (at least annually), PIAS risk-assesses each active product and/or service offering to identify its susceptibility to financial crime. The assessment may group products/services into categories or product sets where appropriate (e.g. all pension products may be assessed together), provided the full product/service offering is included.

This assessment considers all financial crime risk types and is carried out in such a way as to facilitate the identification and implementation of suitable mitigating controls.

An assessment of the risks associated with new product developments, new business practices, including new delivery mechanisms, the use of new or developing technologies for both new and pre-existing products, amendments to existing products and customer proposition initiatives are undertaken in line with Group's requirements. As part of this, the Head of Risk Management & Compliance will ensure that consideration of financial crime risks forms part of the new product development process.

All assessments of risk required under this section is documented including all assessment steps taken. All new product types, new business practices including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products or new customer proposition initiatives assessed by the Risk & Regulatory Team are notified to Group Financial Crime as part of the 'matters for escalation' submission.

Where any new product or customer proposition initiative is outside of PIAS's existing business model/product range (e.g. introduction of life products to a GI business), or introduces significant new risks (e.g. a high risk product or a new country of operation), the Head of Risk Management & Compliance will present the proposal and the risk assessment to Group Financial Crime prior to the new product or customer proposition going live.

Where the new products, new business practises including new delivery mechanism and new or developing technologies favour anonymity, the Group Head of Legal & Compliance approval is required prior to launch.

3.4 Mergers and Acquisitions

The Head of Risk Management & Compliance will ensure that an assessment of the financial crime risks associated with mergers and acquisitions (including acquisitions of portfolios of customers from other financial services firms) is undertaken in line with the requirements of Group's mergers and acquisitions processes.

The risk assessment will be documented and consider the risks arising in both:

- **merger/acquisition process** – particularly whether there are increased bribery and corruption risks associated with the merger/acquisition (e.g. through engagement of third parties, negotiators, etc.; as a result of the jurisdiction involved; due to secrecy in the process; etc)

- **acquired business** - the extent to which the acquired customers, products, services, employees, locations, systems, data, etc. introduce additional or different financial crime risks to the acquiring Singlifebusiness especially where the firm's processes and procedures are below the requirements of Group's Standards

PIAS will consider whether any sample testing of key financial crime prevention processes and procedures (such as customer due diligence activities or sanctions name screening) needs to be undertaken as part of the risk assessment.

After reviewing the risk assessment, PIAS will put in place appropriate action plans to ensure all financial crime deficiencies identified in the risk assessment are remedied and implement suitable controls to manage the financial crime risks in line with Group's financial crime risk appetite and tolerances in both the transition/acquisition process and in the 'new' business.

3.5 Risk Based Controls

The Head of Risk Management & Compliance uses EWRA and any other assessments of financial crime risk to design, implement and operate effective and proportionate controls to mitigate financial crime risks.

A risk-based approach is most likely to be taken in respect of the extent, nature and frequency of controls relating to:

- Customer due diligence (including enhanced due diligence and associated person (non-customer) due diligence)
- Screening
- Ongoing monitoring
- Compliance monitoring
- Training

The risk-based approach will be documented (either as a standalone document or incorporated in other relevant documents) and takes into account the Group Financial Crime Policy.

The approach will be reviewed at least annually to ensure continued suitability.

4 Due Diligence

4.1 Customer Due Diligence

Customer Due Diligence ("CDD"), Simplified Customer Due Diligence ("SCDD") or Enhanced Customer Due Diligence ("ECDD") is performed on all customers to the required level as determined by Group Financial Crime Policy. This is to comply with regulatory requirements to 'Know Your Customer' and to ensure that the business knows who it is dealing with. This includes customers, employees, business partners and third-party providers.

Appropriate control mechanism is in place to ensure compliance with the relevant regulatory requirements relating to CDD, SCDD, ECDD and reliance on third-party providers to conduct CDD.

Broadly, as a safeguard against establishing any business relations or undertaking any transaction, that is or may be connected with or may facilitate ML/TF, the MAS regulations require that the identities of the following persons are identified and verified:

- the customer (individuals, corporates or other body of persons)
- any beneficial owner of the customer
- any beneficiary
- any natural person appointed to act on behalf of the customer
- any connected party of the customer
- any beneficial owner of a beneficiary

When establishing business relationship with individual customers, the following personal information about the customers must be obtained:

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

CDD/SCDD/ECDD requirements include provisions for all relevant customer types and include requirements for completing CDD/SCDD/ECDD on beneficial owners where appropriate. The circumstances in which a customer should be subject to enhanced due diligence (ECDD) to reflect a risk assessment or local regulatory requirements are documented in the PIAS' FCRMP.

CDD/SCDD/ECDD will be completed at the commencement of a customer relationship and is kept up-to-date throughout customer relationship.

CDD/SCDD/ECDD evidence is retained and retrievable according to records retention requirements.

The quality, completeness and accuracy of CDD/SCDD/ECDD is subjected to a regular, on-going quality control process, and the nature, frequency and scope of this control process is documented in the FCRMP.

The results of CDD/SCDD/ECDD quality testing form part of business's compliance monitoring and reporting.

For the purposes of this document, ‘customer’ includes any party where there is regulatory obligation to complete due diligence under AML/CFT legislation and may include relationships referred to as something other than ‘customer’ (For example ‘client’, ‘insured party’, ‘policyholder’, ‘account holder’, ‘beneficiary’, ‘contract holder’, etc.).

All customers of PIAS are subjected to AML/CFT due diligence requirements.

Risk-based Application of Customer Due Diligence (CDD)

PIAS defines the nature and extent of Customer Due Diligence (CDD) applicable to the business(es).

CDD is conducted according to the level of risk posed by customers:

- Simplified Customer Due Diligence (SCDD) may be applicable in limited and pre-defined reduced risk circumstances;
- Customer Due Diligence (CDD) is applicable as the standard level of due diligence;
- Enhanced Customer Due Diligence (ECDD) is applicable in all defined higher risk circumstances, where information over and above CDD is required.

Customers are classified as either Standard Risk customers or High Risk customers. High Risk customers are reviewed annually.

Risk assessment on individual customers ensure that the risks a customer relationship brings to PIAS are duly captured and that an appropriate classification for the customer is established. This will ensure due diligence measures and ongoing monitoring are effective and proportionate.

Timing of Initial Customer Due Diligence Activities

PIAS has procedures in place to complete the initial Customer Due Diligence (CDD) activities for customers before establishing the business relationship.

The approach to local exceptions for timing of CDD are documented and regularly reviewed to ensure compliance with local legislation and regulatory guidance.

Ongoing Customer Due Diligence

PIAS determines the appropriate level of ongoing Customer Due Diligence appropriate for its customers and products, ensuring that the approach taken aligns to its risk appetite and is fully documented as part of the Financial Crime Risk Management Programme.

On-going Customer Due Diligence activities are considered on a risk-based approach, with the extent, frequency and nature of due diligence reviews or refresh driven by the risk posed by the customer in order to:

- ensure the Customer Due Diligence information is kept up to date and reflects any changes to the customer's details
- ensure it continues to meet legal or regulatory requirements
- ensure the appropriate classification is assigned to the customer
- ensure that the customer and their activities remain within Group's risk appetite

On-going Customer Due Diligence is done on a periodic basis and on a trigger event basis.

Periodic Reviews

High Risk Customers

All customers identified as 'high-risk' are reviewed on an annual basis.

Corporate Customers

Periodic reviews are done every 5 years for corporate customers as their beneficial ownership, corporate structure and key personnel are more likely to change over time than is the case for individual customers.

Trigger Reviews

Trigger reviews on customers shall be performed for cases/or instances where there is:

- identification of a credible involvement in financial crime
- increased risk of customer being involved in ML/TF or other financial crime (e.g. through relevant alerts from the transaction monitoring system, court production order or unexplained wealth orders)
- where a suspicious activity report relating to the customer has been filed
- becoming aware of facts or information which leads to doubt over the veracity or adequacy of the due diligence previously obtained
- becoming aware of a change in the individual customer's country of residence
- becoming aware of a change in beneficial ownership of a corporate customer
- becoming aware of a change in the customer's nature of business;
- identification of a PEP, or an increase in the risk rating of an existing PEP
- becoming aware that the customer no longer qualifies for Simplified Customer Due Diligence (e.g. through the loss of regulatory or listed status or selection of a new product)

The nature of ongoing due diligence is proportionate to the risk, taking into account the frequency of customer contact/interaction, the longevity of our products, the length of the customer

relationship, etc. For example, a customer is paying regular premiums over 20 years, from the same account, responding to documentation sent to their address, with a low value product and no unusual activity, is unlikely to require frequent intrusive CDD.

Where possible, CDD reviews are to be completed from existing business information and public source data. PIAS only considers obtaining additional information direct from the customer if no other means of re-confirming CDD information is possible.

PIAS considers also that although keeping customer information up to date is required under AML/CFT legislation, it is also often a requirement of data protection legislation in respect of personal data.

4.2 Associated Persons and Non-Customer Due Diligence

PIAS completes risk-based Due Diligence ("DD") on non-customer relationships to the required level as determined by Group Financial Crime Policy and FCRMP. This includes employees, third-parties, intermediaries, suppliers and other relevant parties (e.g. Joint Venture Partners). This is to ensure that the business knows with whom it is dealing, particularly to mitigate sanctions and bribery risks.

- the nature, extent and format of DD will be risk-based to reflect the level of financial crime risk. This will take into account the role the associated person is undertaking for PIAS and the jurisdiction involved
- the nature, extent and format of DD will be documented, communicated and accessible to relevant parties
- the circumstances in which an associated person should be subject to additional due diligence to reflect a risk assessment or local regulatory requirements will be documented in PIAS' FCRMP
- DD will initially be completed at the commencement of a relationship and will be kept up to date throughout the relationship according to a schedule determined in PIAS' FCRMP.
- DD evidence will be retained and will be retrievable
- quality, completeness and accuracy of DD will be subject to a quality control process, the nature, frequency and scope of this control process will be documented in the FCRMP
- Results of DD quality testing will form part of PIAS' Compliance monitoring and reporting

4.3 Employees - Recruitment

Singlife's People Function oversees hiring for PIAS. PIAS' new employees (both permanent and temporary, including contractors) are hired objectively and thoroughly screened prior to employment in line with Pre-Employment Screening Guidelines.

This includes an interview process as well as obtaining and verifying any references given and analysing any gaps in employment history in line with the Group Fit and Proper Minimum Requirements. Where declared in the employment application, People Function ascertains whether the candidate has any conflicts of interest and/or been referred by a public official. Where there is a conflict as a result of referral from a public official, this will be escalated to the 2nd line of defence, the Risk & Regulatory Team.

After onboarding the employee, the individual is subjected to appropriate pre-employment name screening by Singlife which will include Sanctions, Politically Exposed Persons ("PEPs") and Special Interest Persons (SIPs) screening using Group Name Screening tool ("GNS").

4.4 Employees – Post Recruitment

PIAS ensures that the compensation structure for all employees does not create incentives for inappropriate behaviour that is not aligned to Group's values.

Employees name-screening are screened daily in GNS to detect for PEP, sanctions and adverse news.

PIAS identifies all roles where there is a higher exposure to financial crime risks and where appropriate apply additional controls in relation to them and the activities undertaken, such as, broader background check, increased supervision, enhanced training, additional compliance monitoring.

PIAS will consider whether on-going due diligence activities are required for employees where their roles have a higher exposure to financial crime risks.
PIAS requires that all employees attest annually to Group's Code of Business Ethics.

4.5 Non-Employee Associated Persons and Third Party Risk Management Framework

PIAS ensures that employees responsible for engaging and dealing with non-employee associated persons and third parties (e.g. suppliers of services or intermediaries) are aware of the requirements set out and that accountabilities for compliance with them are clearly documented and understood.

- There will be a Group-led risk-rating policy applied to non-employee associated persons and third party relationships, which records the status of the relationship, assesses and records the risk of bribery and corruption associated to each relationship. For associated persons providing services "for or on behalf" of Singlife, this data must be stored within an associated person register which records relevant details and establishes appropriate levels of due diligence.

4.6 Non-Employee Associated Persons and Other Third-Party Due Diligence

Non-employee associated persons and third party due diligence takes place prior to the receipt of goods or services from them. They are screened using GNS before a business relationship is established. Status of the relationship is ascertained and documented.

Where the non-employee associated person is an entity other than a natural person, for example a company, the key corporate personnel and beneficial owners are identified. The key corporate personnel and beneficial owners subject to identification procedures are equivalent to the identification (but not verification) requirements required for a similar entity under the relevant local AML requirements.

4.7 Third Party Screening

Screening of third parties (including non-employee associated persons and identified key corporate personnel and beneficial owners follows the screening requirements of the relevant.

Confirmed true matches as a result of name screening are escalated to Risk & Regulatory Team for advice as to the materiality of the issue and whether the business should proceed with the relationship.

4.8 High Risk Third Parties and High Risk Non-Employee Associated Persons – Financial Crime Review and Approval

The Risk & Regulatory Team reviews and assesses the following relationships:

- all ‘high risk’ non-employee associated persons
- any non-employee associated person or third party which has been linked to bribery and/or corruption

The nature and scope of the non-employee associated person or third party business relationship are reviewed by Risk & Regulatory Team who will recommend to the CEO whether to enter into the relationship or not, and where necessary determine any additional controls required to mitigate the bribery and corruption risks associated with the third-party are documented.

PIAS will not enter into a business relationship with a high-risk third-party unless it has been approved by the Head of Risk Management & Compliance or PIAS CEO. In addition, PIAS Risk Committee must approve the business relationship prior to its commencement

The decision whether to enter into the business relationship with the non-employee associated person or third party concerned will be documented and include an assessment of the bribery and corruption risks associated with the business relationship and the detailed rationale behind the decision made.

Where a non-employee associated person or third-party relationship is rejected for financial crime-related reasons, the market must ensure that the name of that third party is added to any relevant internal watchlist.

4.9 Non-Employee Associated Person and Third-Party Documentation

Contracts with all non-employee associated persons and third parties will contain relevant anti-bribery and corruption representations and warranties as determined by the relevant legal counsel. The legal counsel will ensure that the contract clauses, terms and conditions, statements of work, or other formal communication with those individuals or businesses acting on behalf of PIAS, includes references to Group's approach to financial crime.

All non-employee associated persons and third parties receive Singlife's Supplier Code of Behaviour and all relationships that are determined to be Medium- or High-risk rated sign up to and undertake to comply with the Code.

Copies of due diligence materials, including risk assessments, the results of screening, and any referrals to Risk & Regulatory Team or governance committees are retained and are retrievable. If a non-employee associated person or third party refuses to sign up to ABC contract clauses or the Supplier Code, any proposal for their engagement must be submitted to the Risk & Regulatory Team for review, risk assessment and escalation for approval (if necessary) to PIAS Risk Committee.

5 Screening

5.1 Sanctions Screening

PIAS screens names (customers, employees, third parties etc.), using GNS as the global screening tool to check against sanctions lists.

All customers (including where appropriate, directors, controllers and beneficial owners), counterparties, associated persons (including employees and any other relevant parties identified by PIAS (e.g. Joint Venture partners), are screened using GNS.

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.

To ensure that the PIAS does not deal with any sanctioned individuals and entities, PIAS screens the following persons using the Group-approved name screening tool (GNS) at onboarding and regularly:

- its customers;
- any beneficial owner(s) of the customer;
- any beneficiary;
- any natural person appointed to act on behalf of the customer;
- any connected party of the customer;
- any beneficial owner(s) of a beneficiary;
- any third party the company engages in business with;
- any insured person;
- the company's directors, representatives and employees

The screening is conducted against the financial crime watchlists and sanctions lists including but not limited to those issued by:

- US Office of Foreign Assets Control (US OFAC),
- HM Treasury,
- United Nations Security Council,
- the European Union,
- Monetary Authority of Singapore and
- Singapore Ministry of Home Affairs

If any sanctioned individual or entity is identified, PIAS will action on the following:

a) immediately freeze funds, other financial assets or economic resources of the designated individual and entity;
b) abort entering into any financial transactions or provide financial assistance or services in relation to: (i) designated individuals, entities or items; or (ii) proliferation and nuclear, or other sanctioned activities;
c) inform MAS of any fact or information relating to the funds, other financial assets or economic resources owned or controlled, directly or indirectly, by a designated individual or entity; and
d) file a suspicious transaction report ("STR") and extend a copy to MAS

PIAS clears sanction alerts within 2 business days and ensures the appropriate actions are taken.

5.2 PEP Screening

PIAS identifies Politically Exposed Persons ("PEPs") relationships in order to appropriately manage the potentially increased money laundering, bribery and tax evasion risks.

Customers (including identified controllers and beneficial owners), counterparties, associated persons (including employees) and any other relevant parties identified by PIAS (e.g. Joint Venture partners) are screened to identify association to financial crime.

Customers (including identified controllers and beneficial owners) and counterparties may be screened to identify association to financial crime. (Note: Any decision not to screen customers/ counterparties/clients are documented and agreed by PIAS Risk Committee).

PIAS clears PEP alerts within 10 business days and ensures the appropriate actions are taken.

All PEPs are classified as high-risk customers. Prior to forming any business relationships with the PEPs, approval is sought from the CEO. Thereafter, they are monitored as part of PIAS' High-Risk Customers list.

5.3 Additional Screening

PIAS identifies and manage the financial crime risk inherent in entities and individuals with which PIAS may have dealings.

PIAS screen customers (including where appropriate their key corporate personnel and beneficial owners), counterparties, associated persons (including employees) and any other relevant parties identified by PIAS (e.g. Joint Venture Partners), to identify exposure to:

- jurisdictions with an increased financial crime risk.
- parties identified as linked to financial crime

PIAS uses the Jurisdictional Index published by Group Financial Crime to assess the jurisdictional risk of customers (e.g. for customer acceptance, associated person due diligence, etc.). Further details are available in the Jurisdictional Index.

5.4 State Owned Companies (SOC) Screening

Being able to identify a connection or relationship with a state-owned company, or a state-owned company executive, will help inform the financial crime risk assessment for existing and potential new relationships. In particular, it will assist in identifying bribery and corruption risk and PEP (AML) risk exposure. An entity is considered 'state owned' where the government or state (or their representative bodies) own or control 50% or more of the entity. However, entities with lower levels of state ownership may still introduce risk to PIAS, for example where public officials represent the entity or otherwise interact with PIAS (bribery risk); where the state concerned is subject to sanctions; or where the state concerned is otherwise considered high-risk.

Screening of SOC is performed using GNS and identification of a connection to a SOC will contribute to an assessment of the financial crime risk of that relationship and a documented decision of whether to commence, retain, reject or end the relationship. The results of SOC screening will be included within the relevant enhanced due diligence records.

5.5 Special Interest Person/Entity (SIPs and SIEs) Screening

PIAS uses GNS as the standardized screening tool. Dow Jones also provides media reports to identify individuals and entities with a documented implication of relevant criminal activity including corruption, financial crime, trafficking, organised crime, terror and tax crime. Where considered necessary (e.g. when completing enhanced due diligence), additional supplemental resources may be used, such as internet media searches or specialist external due diligence reports.

6 Ongoing Monitoring

6.1 Transaction Monitoring

PIAS is responsible for monitoring transactions related to that market's activities on an ongoing basis to help identify unusual activity which may be connected to financial crime.

PIAS has a risk-based transaction monitoring framework that documents relevant financial crime scenarios, identifies transactions to be monitored and establishes the type and frequency of transaction monitoring required for each in accordance with guidance from Group Financial Crime.

The transaction monitoring framework will be documented as part of the financial crime operating model, be approved by the Designated individual and PIAS Risk Committee and reviewed at least annually.

Transactions identified as unusual or potentially suspicious through transaction monitoring controls will be reviewed, investigated and concluded in a timely manner.

6.2 Monitoring and Review Scenarios

PIAS identify and document scenarios that may be indicative of fraud. These scenarios may inform the extent and nature of the transaction activity.

As a minimum, PIAS considers the following scenarios and identify what (if any) transactional activity may be monitored to detect these scenarios:

<u>External Fraud - All Businesses</u>

- payments to customers, representatives, nominees or beneficiaries with links to multiple policies/products/payments (often an indicator of links to organised crime syndicates)
- application fraud, deliberate non-disclosure
- unusual or inflated payment requests for goods and services

- fraud typologies and examples identified in local national risk assessments, law enforcement publications or regulatory guidance
- fraud typologies identified by international organisations, such as Financial Action Task Force
- abuse of PIAS brand

External Fraud - General Insurance (including Health)

- claims fraud
- underwriting fraud
- policy churning (typically a process where a policy is replaced to generate additional income) by associated parties
- reopening of claims to facilitate fraudulent payments

External Fraud - Life Insurance

- surrender fraud, e.g. account takeover/identity fraud (particularly high risk for vulnerable customers)
- policyholder impersonation
- claims fraud
- underwriting fraud
- withdrawal of funds/policy surrender requests made immediately after changing material customer account information, e.g. bank account, beneficiary, address, etc.
- reopening of claims to facilitate fraudulent payments

Internal Fraud – All Businesses

- expense reimbursement payments in breach of the Group expense policy:
- personal spend
- duplicate expense claims
- weekend spending
- inflated mileage claims
- trend in business and staff entertaining
- payments to factitious employees
- abuse of employee incentive schemes
- abuse of position, e.g. making payments to suspicious bank accounts
- abuse of PIAS bank accounts
- unusual or inflated payment requests for goods and services
- mis-selling of products to meet targets
- fraud typologies and examples identified in local national risk assessments, law enforcement publications or regulatory guidance
- fraud typologies identified by international organisations, such as Financial Action Task Force
- abuse of PIAS brand
- human resources fraud, e.g. false employment credentials

Scenarios are based on PIAS risk profile, considering the output from relevant financial crime risk assessment, and the above only act as an aide memoire to assist in documenting the transaction monitoring framework.

6.3 Identifying Relevant Activity

PIAS uses identified fraud scenarios to identify and document transactions for monitoring.

PIAS seek to identify transactions that are deemed to pose a higher risk of fraud and introduce suitable monitoring, including special consideration of abnormal trend transactions when compared to historic activity.

As a minimum, PIAS consider the following transactions and identify what (if any) activity may be monitored to detect these transactions:

External Fraud

- supplier bordereau payments
- large claim payments exceeding a defined threshold
- duplicate claims
- request payment paid into bank account other than the nominated account
- commission payments
- irregular underwriting payments
- irregular premium refunds
- payments of travel or subsistence for non-PIAS employees
- payments to/from jurisdictions deemed to be high risk of fraud
- payments to/from named on or connected to individuals on fraud watchlists, i.e. hunter
- repetitive/duplicative payments
- payments to/from unconnected or unnecessary third parties

Internal Fraud

- payments over employee expense threshold
- reimbursement of employee expenses
- payment of employee incentives and bonuses above threshold
- manual payments
- multiple expense requests without supporting evidence
- payments of travel or subsistence for non- PIAS employees
- payments made to fictitious suppliers

The above are only examples of potentially higher risk transactions and must not be considered as the only examples relevant for each market. An assessment must be undertaken locally to determine the relevant transactions.

Monitoring transaction activity for fraud forms part of the transaction monitoring framework which must be approved by the PIAS Risk Committee.

7 Risk Reporting

7.1 Reporting and Investigation - Internal / External Fraud

This section relates to any incident of potential internal/ external fraud under local legislation, with direct or indirect links to PIAS, including its employees, agents, suppliers, business partners, intermediaries, etc. It does not include suspected internal/ external fraud unrelated to PIAS.

Procedures for reporting internal/ external fraud concerns for all employees and relevant third parties include documented roles, responsibilities and procedures for designated fraud investigation teams and where relevant documented operating models for larger markets. Red flags, including data analytics tools, are consistently updated to reflect emerging fraud trends and typologies.

PIAS will undertake a root cause analysis of internal/ external fraud incidents to identify weaknesses in controls, such as training, red flags, data analytics, investigation methods, etc. Policies, procedures and training where changes are required, will be updated to reflect these control changes.

The procedures for internal/ external reporting make it clear that there is no requirement for an incident to be proven before it is escalated internally. The threshold for internal reporting will be where there is either knowledge, suspicion or reasonable grounds for knowing or suspecting. In cases of doubt, the presumption must be to report, rather than not report.

To comply with MAS Insurance Fraud Risk Guidelines 2012, the following details are required to be furnished to the Authority for any suspected or confirmed fraud cases

- Date of incident
- Type of insurance policies/products (if applicable)
- Name of reported fraudster(s)
- NRIC/FIN or Passport No. of individual fraudster(s)
- Legal Status of fraudsters in Singapore
- Country/ies of Citizenship
- Relationship of fraudsters with insurer (i.e. policyholder, claimant, administrative staff, distributor etc.)
- Dollar Amount involved, if any
- Status of Case or Legal Proceedings, if any
- Whether Police Report has been made and who made the Police Report, if applicable

Examples of activities to be shared:

- New-to-insurer customer making a claim on medical insurance policy shortly after policy inception for bills incurred overseas;
- A website set up by unknown parties, which shows different insurers' products with very high guaranteed returns and instant online sign-up and payment facilities.

7.2 Reporting the Proceeds of Crime Arising from Fraud

In respect of any external or internal fraud incidents where an individual (including employees) or entity has benefited from criminal behaviours or actions (e.g. life insurance claim paid and subsequently established the customers death was faked) the benefit would be deemed to be criminal property and the individual or entity may have committed a money laundering offence.

Therefore, if at any time during an investigation of a fraud incident it is determined that an individual has benefited from inappropriate criminal behaviours or actions, a suspicious activity report must be submitted according to local procedures.

Internal reports must be submitted directly to the relevant appointed nominated officer. The reporting process must be appropriately documented as part of the financial crime risk management programme and communicated to all relevant employees.

The Risk & Regulatory Team shall evaluate and document the basis of their determination in the Suspicious Transactions Register whether the matter should be referred to STRO within 15 business days, unless the circumstances are exceptional or extraordinary. Any exception (i.e. exceed 15 business days) shall be explained and documented in the Suspicious Transactions Register. The MLRO or Nominated Officer will review the report before it is submitted to the Singapore Police Force via STRO Online Notices and Reporting Platform (SONAR).

Reporting is done concurrently to local authorities as well as Group Financial Crime.

7.3 "Tipping Off" Offence

PIAS has appropriate procedures, systems and controls to ensure that employees do not do or say anything that might "tip off" another person that an internal or external report of (suspected or actual) money laundering or terrorist financing has been made. Additionally, PIAS must have appropriate procedures to ensure employees do not otherwise prejudice a money laundering/terrorist financing investigation, even when an internal or external report has not been made.

This must include consideration of the following:

- suitable training and awareness for all relevant employees
- controls over access to internal and external reports

- specific reminders to employees at the time of submission of an internal report
- prepared statements/scripts for customer communication
- handling of customer contact by specialist employees

"Tipping off" does not include disclosures to regulators/supervisors, other PIAS/Group employees and in certain circumstances other financial institutions that are connected to the customer/transaction/activity. In any cases of doubt, the matter must be referred to local nominated officer who may then escalate to Group Financial Crime team, where appropriate.

7.4 Fraud Loss Reporting

Material External Fraud Loss Reporting

PIAS has a responsibility to prevent, detect, report and investigate all instances of external fraud in accordance with Group's approach to financial crime. This will be reported as part of Management Information. As part of the investigation process all fraud losses must be quantified to enable the reporting of material losses.

Where the investigation of a suspected external fraud incident indicates that PIAS's liability may exceed SGD 50,000 the case must be referred to the Risk & Regulatory Team who must consider whether further action is appropriate. Considerations may include, but are not limited to:

- root cause analysis
- adapting or implementing new prevention techniques
- reviewing the current detection controls (i.e. red flags, data analytics, transaction monitoring, etc.) to ensure they are set up to appropriately identify such risks and revise controls where appropriate
- assessing whether the loss is subject to new and/or emerging fraud trends or typologies and implement new control techniques to prevent and detect where appropriate
- assesses whether the loss is connected to organised crime or part of a wider fraud scam (either internal or industry wide)
- investigations suggest potential impact to other Singlife businesses across the Group,
- e.g. claimant has multiple claims across different product types
- assess whether the recovery of assets/monies has been fully considered
- external reporting obligations, including registering loss on local fraud prevention databases, including non-material losses

Escalation will be made to the Group Head of Legal & Compliance particularly where there may be wider implications across the Group or there are potential external reporting requirements.

Material Internal Fraud Loss Reporting

PIAS has a responsibility to prevent, detect and report all instances of internal fraud in accordance with Group's approach to financial crime.

Proven instances of internal fraud may prompt markets, in conjunction with Group Investigations, to consider, but are not limited to:

- root cause analysis
- adapting or implementing new prevention techniques
- reviewing the current detection controls (i.e. red flags, data analytics, transaction monitoring, etc.) to ensure they are set up to appropriately identify such risks and revise controls where appropriate
- assesses whether the loss is connected to organised crime or part of a wider fraud scam (either internal or industry wide)
- assess whether the recovery of assets/monies has been fully considered
- external reporting obligations, including registering loss on local fraud prevention databases, including non-material losses

All proven instances of internal fraud must be reported to the Group Head of Legal & Compliance. No external reporting (including to regulators or law enforcement) of proven or suspected internal fraud may occur without first liaising with the Group Head of Legal & Compliance

Reporting is done concurrently to local authorities as well as Group Financial Crime.

7.5 Incident Reporting (Internal Audit)

In order for Internal Audit to investigate incidents in an effective and timely manner, PIAS reports using any available channel (e.g. direct to Internal Audit or using Speak Out (by email, telephone or mobile application)), suspicions or alleged instances of internal and non-customer malpractice or financial crime, including possible breaches of the Business Ethics Code.

In order to achieve this, PIAS reports such incidents to Internal Audit within 2 business days.

7.6 'Speak Out Charter'

"Speak Out Charter" is a confidential reporting process to enable employees, contractors, outsource providers and other third parties to report behaviour in the workplace (by Singlife or Third Parties) that may be a breach of Singlife Business Ethics Code; may be illegal, criminal, or unethical; or may be an abuse of our systems, abuse of any processes or policies.

"Speak Out Charter" provides a confidential, reliable, credible and secure reporting mechanism. PIAS sends active reminders to all management and staff of this service, including ensuring that

management and staff understand their obligation to report in accordance with Group's Business Ethics Code.

8 Compliance Monitoring

PIAS has a risk-based compliance monitoring plan annually to assess compliance with relevant financial crime regulations and related financial crime procedures.

The scope, nature and frequency of monitoring will be documented as part of the Financial Crime Work Plan, considering any local regulatory requirements for regular independent assurance. At minimum, compliance testing will include the following key risk areas for Financial Crime:

- Financial Crime training and awareness
- Financial Crime responsibility/ownership
- Financial Crime risk assessment – market risk assessment and product/services risk assessments
- Management information (including completeness, accuracy and analysis)
- Governance, reporting (both internal and external) and escalation
- Review of associated person due diligence (including employees)
- Procurement activities
- Adequacy of red flags and other detection systems
- Responding to law enforcement and incidents
- Governance, reporting and escalation
- Investigation procedures
- Financial Crime record keeping

The monitoring programme is in addition to quality control activities conducted as part of normal business operations to confirm that controls are being operated (e.g. ongoing checks on the completeness of CDD).

PIAS ensures that the compliance monitoring function has the appropriate resource and capability (knowledge, skills and independence) to effectively oversee and challenge the business in relation to financial crime issues.

The findings of the monitoring programme will be reported to the Head of Risk & Compliance ["RM&C"], and PIAS Risk Committee.

PIAS also ensures that prompt remedial action is taken to resolve identified financial crime control weaknesses.

Compliance Monitoring – Resources

The Risk & Regulatory Team must have the appropriate resource and capability (knowledge, skills and independence) to effectively oversee and challenge the market in relation to financial crime issues.

The Risk & Regulatory Team must have full, free and unrestricted access to all business activities, records, data, property and personnel necessary to complete their work.

The Risk & Regulatory Team is specifically responsible to oversee compliance of the market's financial crime activities.

Any identified gaps in capacity, capability or access will be referred to the PIAS Risk Committee and notified to the Group Head of Legal & Compliance.

In the absence of suitable internal resource, or if otherwise considered necessary by the designated individual or Group Head of Legal & Compliance, PIAS may seek external verification or assurance of the effectiveness of AML/CTF procedures.

Compliance Monitoring - Findings and Remediation

The findings from any financial crime compliance monitoring review are fully documented and reported to the Designated Individual(s) and PIAS Risk Committee.

Both 1st and 2nd LODs are expected to take all appropriate action to remedy any deficiencies identified through compliance monitoring reviews and report on the progress of such activities to PIAS Risk Committee.

9 Response to Financial Crime

In order to be able to manage financial crime incidents in a coordinated and informed manner, PIAS documents the actions that will be taken in response to specified financial crime events. This will include documented procedures for the receipt, review and response to requests, enquires or notices from law enforcement agencies and relevant regulatory/governmental authorities.

The plan (or the components that make up the plan) is the responsibility of the designated individual and will be approved by the designated individual and PIAS Risk Committee on an annual basis (or more frequently if any changes are made to the plan). It is reviewed and, if necessary updated, in the event of any changes to process following a financial crime incidents or relevant changes to the financial crime risk assessments.

The scope and nature of the procedures, including any specific legal or regulatory requirements, will be included as part of the Financial Crime Risk Management Policy and be proportionate to the volume, frequency and nature of financial crime incidents and requests received.

PIAS also complies with the Section 35 of the Criminal Procedure Code 2010 on 'Powers to seize property in certain circumstances' when responding to financial crimes.

10 Training

The Head of Risk Management & Compliance will ensure that all employees acknowledge and commit to Group's approach to financial crime risks. Training is provided (as part of their induction) through the Essential Learning / Learning Management System existing and new employees, permanent or temporary contract workers, including contractors are tested yearly. PIAS employees are reminded any financial crime related incident involving an employee will be considered gross misconduct and dealt with accordingly.

Where additional training is required for department at high risk of financial crime, tailored training will be provided.

On an annual basis, Financial Crime training materials are reviewed and update to reflect any local regulatory/legislative or market changes.

The Risk and Regulatory team (with the support of People Function) will monitor the completion of AML/CFT training within the stipulated timeline. Risk Management & Compliance will take appropriate action against those who are unable to complete the AML/CFT training without a reasonable cause.

11 Management Information

PIAS follows the Group required suite of key risk indicators and information to monitor the changing financial crime risk profile of the business. This includes but is not limited to information on number and nature of transaction alerts flagged for review/investigations, number of fraud incidents reported, CDD backlog (if any), trends observed from transaction monitoring etc.

The Management Information is presented to Group Financial Crime Team monthly, using the Group Financial Crime MI pack conforming to the format, template and requirements set by the Group Financial Crime Team.

12 Board and Management Reporting

The Risk and Regulatory team will prepare and present a quarterly financial crime report to the business entity's Operational Risk Committee and to the Board Risk Committee. The report must provide information on the financial crime risk profile of the company, performance against each of the 6 Group's Financial Crime preference statements, the effectiveness of risk mitigating controls and any material matters such as regulatory violation together with the remediation actions.

13 Record Keeping

Record Retention and Retrieval

PIAS has implemented procedures, systems and controls to enable relevant financial crime records to be retained, retrieved and if necessary, deleted to comply with local legislation and Group's Financial Crime Policy. All financial crime related records will be accurate, legible, auditable and retrievable including:

- documents and information obtained to satisfy CDD requirements (e.g. identification documents/certificates, proof of address, ECDD documents etc.)
- records relating to customer transactions
- documents relating to the review/investigation of potentially suspicious or unusual activity
- records relating to training (i.e. date of completion, nature of training, attendance records etc.) and compliance monitoring (i.e. reports to senior management)
- records of screening and potential match investigation
- risk assessments and FCRMP documents
- incident investigation reports

PIAS shall ensure compliance with the record retention period as set out in paragraph 10.3 of the MAS FAA Notice 06 on Prevention of Money Laundering and Countering the Financing of Terrorism -Financial Advisers ("FAA-N06")

- For customer due diligence information relating to the business relations and transactions undertaken in the course of business relations, as well as policy files, business correspondence and results of any analysis undertaken, a period of 7 years following the termination of such business relations; and

- For data, documents and information relating to a transaction undertaken in the course of business relations, including any information needed to explain and reconstruct the transaction, a period of 7 years following the completion of the transaction.

PIAS may retain data, documents and information as originals or copies in paper or electronic form or on microfilm, provided that they are compliant with the requirements of the Evidence Act 1893 and Electronic Transactions Act 2010 and are admissible as evidence in a Singapore court of law.

PIAS shall retain records of data, documents and information on all its business relations with, or transactions undertaken in the course of business relations for, a customer pertaining to a matter which is under investigation, or which has been the subject of a Suspicious Transaction Reporting ("STR"), in accordance with any request or order from Suspicious Transaction Reporting Office or other relevant authorities in Singapore.

In such cases, all relevant records should be retained such that:

a) any individual transaction undertaken in the course of business relations can be reconstructed (including the amount and type of currency involved) so as to provide, if necessary, evidence for prosecution of criminal activity.

b) the Authority or other relevant authorities in Singapore and the internal and external auditors are able to review business relations, transactions undertaken in the course of business relations, records and CDD information; and

c) the Group or relevant business entity can satisfy, within a reasonable time or any more specific time period imposed by law or by the requesting authority, any enquiry or order from the relevant authorities in Singapore for information.