Monetary Authority of Singapore

GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM -

DIRECT GENERAL INSURANCE BUSINESS, REINSURANCE BUSINESS, AND DIRECT LIFE INSURANCE BUSINESS (ACCIDENT & HEALTH POLICIES)

13 MAY 2019

TABLE OF CONTENTS

1 INTRODUCTION

1.1 These Guidelines apply to all insurers licensed under section 8 of the Insurance Act (Cap. 142) ("the Act") and to all foreign insurers operating in Singapore under a foreign insurer scheme established under Part IIA of the Act[1].

1.2 Direct life insurers writing life policies should refer to MAS Notice 314 on "Prevention of Money Laundering and Countering the Financing of Terrorism – Direct Life Insurers" and the accompanying guidelines in relation to direct life insurance business. For all other insurers, including foreign insurers operating in Singapore under a foreign insurer scheme and direct life insurers writing accident and health policies, these Guidelines are intended to provide guidance on the prevention of money laundering and countering the financing of terrorism.

1.3 For the purposes of these Guidelines, the licensed insurers and foreign insurers operating in Singapore under a foreign insurer scheme as defined in paragraph 1.1 will be collectively known as "insurers".

1.4 Singapore's primary legislations to combat money laundering ("ML") and terrorism financing ("TF") are the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A) ("CDSA") and the Terrorism (Suppression of Financing) Act ("TSOFA") respectively. Insurers may refer to the Inter-Ministry Committee on Terrorist Designation's website for more information[2] in relation to the TSOFA, and the Commercial Affairs Department's website[3] for more information on the CDSA and the reporting of suspicious transactions.

1.5 ML is a process[4] intended to mask the benefits derived from criminal conduct so that they appear to have originated from a legitimate source.

1.6 TF refers to the financing of terrorist acts, and of terrorists and terrorist organisations.

---

[1] This includes Lloyd's service companies registered under regulation 6 of the Insurance (Lloyd's Asia Scheme) Regulations.

[2] https://www.mha.gov.sg/Pages/Inter-Ministerial-Committee---Terrorist-Designation-%28IMC-TD%29-.aspx

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

[4] Generally, the process of ML comprises three stages:
Placement – the physical or financial disposal of the benefits derived from criminal conduct;
Layering – The separation of these benefits from their original source to disguise the ultimate source and transfer of these benefits;
Integration – The provision of apparent legitimacy to the benefits derived from 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 funds.

1.7 Proliferation financing ("PF") refers to the act of providing funds or financial services which are used, in whole or in part, 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 materiels (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

1.8 In addition, targeted financial sanctions ("TFS") relate to specific sanctions imposed in relation to both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities[5]. TFS include the following components:

(a) Sanctions relating to TF (i.e. the lists indicated under the First Schedule of the TSOFA and any other lists or information provided by the Monetary Authority of Singapore ("the Authority") or other relevant authorities in Singapore regarding sanctions relating to TF);
(b) Sanctions relating to PF that make reference to resolutions effected by the United Nations Security Council ("UNSC")[6]; and
(c) Sanctions relating to resolutions effected by the UNSC on undesirable persons[7].

In these Guidelines, regulations issued by the Authority in relation to paragraphs 1.8(b) and 1.8(c) will be collectively known as the "MAS TFS Regulations".

1.9 For the purposes of these Guidelines, the risks of TF, PF and non-compliance with TFS will be collectively known as "TF risks". Similarly, where the term "countering the financing of terrorism" ("CFT") is used in relation to controls, this would refer to control processes to counter both TF and PF, and to ensure compliance with TFS.

1.10 The expressions used in these Guidelines have the same meaning as those found in the Act, except where expressly defined in these Guidelines or where the context otherwise requires.

1.11 The degree of observance with these Guidelines by an insurer may have an impact on the Authority's overall risk assessment of the insurer, including the quality of its board and senior management oversight, governance, internal controls and risk management processes.

[5] This refers to designated individuals and entities as defined in the respective regulations promulgated under the MAS Act, the United Nations Act and the Terrorism (Suppression of Financing) Act.

[6] As a member state of the United Nations ("UN"), Singapore is committed to implementing the UN Security Council Resolutions ("UNSCRs"). The Authority gives effect to targeted financial sanctions under the UNSCRs through MAS Regulations issued under section 27A of the MAS Act.

[7] Such sanctions are typically effected due to acts against humanity or war crimes.

2 MONEY LAUNDERING AND TERRORISM FINANCING

2.1 Insurers should be cognisant of their exposure to ML/TF risks. Payments originating from insurers are viewed as commonplace, with the money assumed to be clean. If money launderers are able to successfully place funds into an insurance policy, they would have made significant steps in layering and integrating such funds into the financial system.

2.2 Funds for TF may be derived from criminal activities such as robbery, drug-trafficking, kidnapping, extortion, fraud or hacking of online accounts. In such cases, there may also be an element of money laundering involved to disguise the source of such funds.

2.3 Terrorist acts and organisations may also be financed from legitimate sources such as donations from charities, legitimate business operations and self-funding by individuals. In addition, considering the fact that TF does not always need to involve large sums of money, TF can be hard to detect and insurers should remain vigilant.

2.4 In the case of direct insurance business, ML/TF activity could occur within the context of, and as the motive behind, insurance fraud. For example, exaggerated or false claims could be made to recover part of invested illegitimate funds. Other examples could include the refund of premiums, by an insurer's cheque, for overpaid or cancelled policies.

2.5 In the case of reinsurance business, ML/TF activity could occur through the establishment of fictitious fronting arrangements and captives, or by the misuse of normal reinsurance transactions. Examples include dealing with bogus insurers or receiving tainted premiums from insurers which have weak anti-money laundering ("AML") controls that allow illicit funds or funds from unclear or dubious sources to pass through.

3 THE THREE LINES OF DEFENCE

3.1 Insurers are reminded that the ultimate responsibility and accountability for ensuring compliance with AML and CFT ("AML/CFT")-related laws and regulations rest with their board of directors and senior management[8].

3.2 An insurer's board of directors and senior management are responsible for ensuring strong governance and sound risk management and controls in relation to AML/CFT within the insurer. While certain responsibilities can be delegated to senior employees responsible

[8] All references to an insurer's "board of directors and senior management" henceforth apply to insurers incorporated in Singapore. For an insurer incorporated outside of Singapore, this should refer to its local senior management, its Head Office, and the Head Office's board of directors.

for AML/CFT, the final accountability rests with an insurer's board of directors and senior management. The insurer should ensure a strong compliance culture throughout the organisation, where the board of directors and senior management set the right tone from the top. The board of directors and senior management should also set a clear risk appetite and establish a compliance culture whereby financial crime is not tolerated.

3.3 Business units (e.g. front office, customer-facing functions) constitute the first line of defence in identifying, assessing and mitigating the ML/TF risks faced by an insurer. As part of the first line of defence, business units require robust controls to detect illicit activities and should be allocated sufficient resources to perform this function effectively. The insurer's policies, procedures and controls on AML/CFT should be clearly documented in writing, and communicated to all relevant officers, employees and agents in the various business units. The insurer should also ensure that its officers, employees and agents are adequately trained to be aware of their AML/CFT-related obligations, so that the insurer is in compliance with prevailing AML/CFT laws and regulations.

3.4 The second line of defence includes an insurer's compliance function[9], and other support functions such as operations, human resource or technology that work together with the compliance function to identify ML/TF risks. The compliance function is typically responsible for the screening of new and existing business relations and their ongoing monitoring. The compliance function should alert the board of directors or senior management if it has reason to believe that the insurer's officers, employees or agents are failing or have failed to adequately address ML/TF risks and concerns or have breached applicable AML/CFT laws and regulations. While the other support functions also play a role in mitigating ML/TF risks that an insurer faces, the compliance function will usually be the main contact point in relation to all AML/CFT-related issues for domestic and foreign authorities, including supervisory authorities, law enforcement authorities and financial intelligence units.

3.5 The third line of defence is an insurer's internal audit function, which plays a key role in independently evaluating the insurer's AML/CFT risk management framework and controls. This independent assessment is achieved through internal audits (or an equivalent function's periodic evaluations) of the insurer's compliance with AML/CFT laws and regulations, as well as policies, procedures and controls. An insurer should establish policies for periodic AML/CFT internal audits, covering areas such as –

(a) adequacy of the insurer's AML/CFT policies, procedures and controls in identifying ML/TF risks, addressing the identified risks and complying with laws, regulations and notices;

[9] For insurers without a compliance function, the second line of defence should be carried out by a person of sufficient seniority with the necessary competency.

(b) effectiveness of the insurer's officers, employees and agents in implementing the insurer's policies, procedures and controls;
(c) effectiveness of the compliance oversight and quality control including parameters and criteria for transaction alerts; and
(d) adequacy and effectiveness of the insurer's AML/CFT training of relevant officers, employees and agents.

The results of these assessments should be reported to either the Audit or Risk Committee of the insurer, or a similar body of oversight, on a regular basis. Significant AML/CFT issues should be escalated to the Board. Any deficiencies identified should be promptly addressed to mitigate risks, including legal and reputational risks, to the insurer.

3.6 The board of directors and senior management should understand the ML/TF risks that the insurer is exposed to and how the insurer's AML/CFT control framework operates to mitigate those risks. The AML/CFT controls put in place by an insurer should commensurate with the scale, complexity and inherent risk of the insurer, and may be broadly categorised into the following 4 categories, which will be elaborated on within these Guidelines:

(a) Management Oversight, Policies and Training;
(b) Customer Due Diligence and Screening Procedures;
(c) Record Keeping and Documentation; and
(d) Assessment and Reporting of Suspicious Transactions.

4 MANAGEMENT OVERSIGHT, POLICIES AND TRAINING

4.1 The roles and responsibilities of the board of directors and senior management in relation to AML/CFT should be clearly set out.

4.2 There should be a formalised process in place to keep the board of directors and senior management informed regularly of compliance and risk management efforts, audit reports, identified compliance and risk management deficiencies, and corrective actions taken in relation to AML/CFT. Examples of such reports may include statistics on the number of Suspicious Transaction Reports ("STRs") filed, sanctions hits, outstanding transaction monitoring alerts and/or sanctions alerts including aging reports and resource issues.

4.3 Senior management are reminded to take prompt corrective actions to ensure the proper and timely remediation of deficiencies in AML/CFT controls and risk management.

4.4 There should be adequate processes in place for updating senior management and any other relevant personnel of AML/CFT-related updates issued by the Authority or other relevant authorities in Singapore. There should also be a designated employee (e.g. Head of

Compliance) responsible for providing such updates to management and other relevant personnel.

4.5 There should be a clear and detailed set of documented AML/CFT policies and procedures in place that incorporate, at a minimum, the following elements:

(a) Customer due diligence and screening procedures;
(b) Documentation of screening results;
(c) Assessment, escalation and reporting of suspicious transactions; and
(d) Frequency and recipients of AML/CFT-related training.

4.6 AML/CFT policies and procedures should be reviewed regularly by the board of directors and/or senior management. At a minimum, these policies should be reviewed whenever there are changes in regulations or if there is a significant change in the insurer's business strategies.

4.7 Regular AML/CFT-related training[10] should be conducted for the board of directors, employees and agents (where applicable) of the insurer. Such training may take the form of seminars, e-learning modules, etc.

5 CUSTOMER DUE DILIGENCE AND SCREENING PROCEDURES

5.1 Screening of customers[11] should be carried out against relevant ML/TF information sources, which include designated names of individuals and/or entities within:

(a) the lists and information provided by the Authority or other relevant authorities in Singapore in relation to ML/TF risks;
(b) the First Schedule of the TSOFA; and
(c) the MAS TFS Regulations.

5.2 In the context of direct insurance business, the screening of customers should include the screening of policy owners, insureds and claimants. In cases where an insurer has assessed the policy owner or insured to be of a higher ML/TF risk, the insurer should also screen the substantial shareholders (direct and indirect), beneficial owners, natural persons

[10] There should minimally be some form of regularity with regard to such training, as opposed to the conduct of a one-off training.

[11] For the purposes of these Guidelines, the definition of the term "customers" will vary depending on the type of insurance business (e.g. direct insurance business, reinsurance business), and is elaborated on in paragraphs 5.2 and 5.3 of these Guidelines.

appointed to act on behalf of the customer and directors, if any, of the policy owner or insured.

5.3 In the context of reinsurance business, the screening of customers should include the screening of cedants and claimants[12]. Underlying insureds should also be screened in cases where they are made known to the reinsurers. In cases where a reinsurer has assessed the cedant or underlying insured to be of a higher ML/TF risk, the reinsurer should also screen the substantial shareholders (direct and indirect), beneficial owners and directors, if any, of the cedant or underlying insured.

5.4 Screening of customers should be conducted at the following points in time:

(a) before establishing business relations for new customers, otherwise as soon as reasonably practicable thereafter;
(b) prior to renewing business relations with existing customers;
(c) on a regular basis after the establishment of business relations[13];
(d) when there are changes made to the lists[14] mentioned in paragraph 5.1 above; and
(e) before making claim payments to claimants[15].

5.5 For the purposes of screening, the insurer should minimally, either:

(a) subscribe to a commercial sanctions database; or
(b) maintain an internal database containing the names of designated individuals and entities.

5.6 The screening database(s) (i.e. commercial sanctions database and/or internally-maintained database) and procedures adopted by an insurer should be effective in identifying individuals and entities with adverse information, as well as designated individuals and entities as defined in the First Schedule of the TSOFA and the MAS TFS Regulations, or as informed by the relevant authorities in Singapore.

[12] Claimants, in the perspective of a reinsurer, may refer to parties to which claim payments are made (i.e. cedants/brokers).

[13] In determining the frequency of regular screening, the insurer should consider (i) duration of the policy, and (ii) customer risk profile. Given that most direct general insurance and reinsurance policies are relatively short-term in nature (e.g. 1 year), the insurer should conduct such ongoing screening minimally at a frequency of once every 6 months, or upon the occurrence of a trigger event as deemed necessary by the insurer, whichever is earlier. Higher risk customers should be subject to screening at a higher frequency.

[14] It is not necessary to screen customers with whom the insurer no longer has business relations with, on or after the effective date of the change.

[15] Where the claimant is not the customer, the insurer shall first identify the payee and verify his identity before making the payment.

5.7 In view of system limitations in screening capability, some insurers may not be able to effectively detect designated individuals or entities if they were to perform screening based on a full/exact match logic instead of a partial/fuzzy[16] match logic for name searches. A full/exact name match for screening should not be used, as this will likely result in missed sanctions or adverse comments hits. In addition, the screening filters used by the insurer should not be limiting[17] and should take into account the various permutations of a person's first and last names.

5.8 Insurers are reminded that where screening results in a positive hit against the lists mentioned in paragraph 5.1, an insurer shall freeze without delay and without prior notice, the funds or other assets of designated persons and entities that it has control over, so as to comply with applicable laws and regulations in Singapore. This would include both the TSOFA and the MAS TFS Regulations relating to sanctions and freezing of assets of persons. Any such assets shall be reported promptly to the relevant authorities and an STR shall be filed.

5.9 Insurers should also have in place screening procedures when hiring employees, officers[18] and agents[19], and when establishing business relationships with offshore intermediaries. This should include, where applicable:

(a) background checks with past employers;
(b) credit history checks;
(c) screening against ML/TF information sources; and
(d) bankruptcy searches.

6 RECORD KEEPING AND DOCUMENTATION

6.1 There should be adequate documentation by the insurer of the basis for clearing or dismissing hits arising from its screening procedures (i.e. false positive hits). As a good practice, additional parameters such as date of birth and nationality should minimally be used to establish and dismiss false hits.

[16] A partial/fuzzy match logic allows for different permutations of a customer's name to be screened by the system.

[17] Certain systems may require two separate fields to be entered (e.g. name and nationality) before screening can be carried out. The system should not reject a potential hit solely due to an incorrect field match (e.g. nationality) since there may be different definitions with regard to the nationality field (e.g. country of citizenship vs. country of residence etc.). For such cases, further assessment should be carried out by the insurer.

[18] "Officer" means any director or any member of the committee of management of the insurer.

[19] "Agents" refer to underwriting agents and sales agents.

6.2 There should be documentation and maintenance of proper records by the insurer as to when screening was performed, the results of the screening and the assessment of screening results for all policies.

6.3 A record of all transactions referred to the Suspicious Transaction Reporting Office ("STRO") should be maintained by an insurer, including the relevant internal findings and analysis.

6.4 In cases where an insurer maintains an internal database containing the list of designated individuals and entities for the purpose of screening, there should be clear documentation of when the internal database was most recently updated, as well as of the name of the person who carried out the update.

7 REPORTING OF SUSPICIOUS TRANSACTIONS

7.1 Clear guidance should be provided to all officers, employees and agents as to what constitutes a "suspicious transaction" that warrants escalation and reporting.

7.2 There should be well-defined guidelines and procedures in place for escalating, investigating, reporting and acting on suspicious transactions. The channels for reporting suspicious transactions should be clearly specified in writing and communicated to all personnel.

7.3 A clear internal reporting channel should be set up for the escalation of suspicious transaction reports from the officer, employee or agent making the report. The insurer should establish a single reference point (e.g. Chief Executive, Head of Compliance) within the organisation to whom all transactions suspected of being connected to ML/TF activity should be referred to.

7.4 The onus is on the insurer to identify and assess red flag indicators of suspicious transactions. The insurer should determine what constitutes a suspicious transaction which warrants escalation and reporting based on the scale, complexity, and inherent risk of its business. In terms of determining and assessing suspicious activity exhibited by customers, examples of suspicious circumstances that may warrant the filing of an STR may include the following:

(a) where the customer is reluctant, unable or unwilling to provide any information requested by the insurer;
(b) where the customer, without reasonable grounds, decides to withdraw a pending application to establish business relations with the insurer;

(c) where the customer, without reasonable grounds, decides to suddenly terminate existing business relations with the insurer;
(d) abnormal settlement instructions, including payment to apparently unconnected parties; or
(e) frequent changes to the customer's address or to authorised signatories.

7.5 STRs should be filed on all suspicious transactions and cases. Where an insurer decides not to file an STR for a case that was initially thought to be suspicious, the basis for doing so should be documented, and the decision made by the initial assessor of the case should be raised to a higher authority for review and approval.

7.6 An STR should be filed within 15 business days of the case being referred by the relevant officer, employee or agent, if the insurer has assessed that the matter should be referred to the STRO, unless the circumstances are exceptional or extraordinary. The decision as to whether to refer the matter to the STRO should be regardless of the amount of the transaction, if any.

7.7 STR reporting templates are available on the Commercial Affairs Department's website. However, insurers are strongly encouraged to use the online system provided by STRO to lodge STRs, as this also enables reporting entities to be kept apprised of STRO's advisories. In the event that an insurer is of the view that STRO should be informed on an urgent basis, including where a transaction is known to be part of an ongoing investigation by the relevant authorities, the insurer should give initial notification to STRO by telephone or email and follow up with such other means of reporting as STRO may direct.

7.8 Under exceptional circumstances, (e.g. if the online system is down) and the insurer files an STR manually with the STRO (i.e. not through the STRO Online Notices and Reporting Platform ("SONAR")), a copy of the report should be extended to the Authority for information.