Annex A

Summary of Observations made by the Insurance Authority ("IA") in Inspections of Insurance Institutions ("IIs")[1] under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) ("AMLO") from June 2018 to December 2024

INTRODUCTION

During the period since June 2018, the IA carried out inspections under section 9 of AMLO on more than 70 IIs. The objective of these inspections is to ascertain their compliance with obligations under Schedule 2 of AMLO. In broad terms, these obligations require an II to:

- comply with customer due diligence ("CDD") and record-keeping requirements specified in Schedule 2 to AMLO;

- establish effective procedures for the purposes of complying with such requirements (section 19 of Schedule 2 to AMLO) and take all reasonable measures to ensure that proper safeguards exist to prevent their contravention (section 23 of Schedule 2 to AMLO); and

- take all reasonable measures to mitigate money laundering and terrorist financing ("ML/TF") risks (section 23 of Schedule 2 to AMLO).

These obligations are supplemented by the Guideline on Anti-Money Laundering and Counter-Terrorist Financing ("Guideline") promulgated by the IA under AMLO and the Insurance Ordinance ("IO").

The inspections serve to ensure that anti-money laundering ("AML") and counter-financing of terrorism ("CFT") standards are maintained and kept up-to-date in line with international standards and in the context of technology advancement. We would like to share some key findings that will inform our general inspection approach.

GENERAL OBSERVATIONS

1) Oversight by senior management

a) Understanding and mitigation of risks

As a prerequisite to establishing effective AML/CFT procedures for complying with the requirements in Schedule 2 to AMLO and taking all reasonable measures

[1] The definition of IIs should be construed in conjunction with the Guideline on Anti-Money Laundering and Counter-Terrorist Financing ("GL3"), i.e. authorized insurers and reinsurers carrying on long term business, licensed individual insurance agents, licensed insurance agencies and licensed insurance broker companies carrying on regulated activities in respect of long term business.

to mitigate ML/TF risks, senior management of an II is expected to have a clear understanding of and adequately manage such risks. Accordingly, our inspections focused on whether the information regarding ML/TF risks and related controls is communicated to senior management of an II in a timely, complete, understandable and accurate manner.

The institutional ML/TF risk assessment ("IRA") which an II should conduct to identify, assess and understand the ML/TF risks to which it is exposed is crucial to this process. The Guideline requires that senior management of an II approve the results of the IRA. The following examples were observed in our inspections:

EXAMPLES

i. There are examples of not insignificant delays in (or complete absence of) submission of the IRA to senior management for approval. In some cases, approval was not obtained even where the IRA was presented at senior management meetings. Granting of approval is an important step for senior management to take accountability for the IRA and its results, ensuring that results therein have been duly considered and scrutinized. This process should be substantive and evidenced, for example, by minutes or e-mails.

ii. In one case, ambiguity existed regarding which member of senior management was responsible, thereby causing approval of the IRA results to be delayed for several years.

iii. A matter to which senior management should give attention is where an II seeks to change internal control that would materially affect its exposure to ML/TF risks. This includes significant increase in the thresholds for income or asset proof accompanying large payments and the thresholds for proof that large payments are not coming from unrelated third parties. If there is no evidence of such changes having been discussed by senior management, for example in meetings of the governance committees tasked with overseeing AML/CFT compliance, it would fall short of the standards for meeting its obligations under AMLO as supplemented by the Guideline. In one case, an II introduced a materially higher threshold for internal controls without documenting the justification or obtaining approval from senior management, thus deviating from its AML Policy and attracting compliance risks.

To maintain robust ML/TF risk management, it is essential for senior management of an II to understand its risk exposure. It follows that senior management should approve the IRA and be informed of potential impact arising from and the risk mitigating measure of significant changes made to the AML/CFT systems.

b) Implementation of AML/CFT systems

Having identified the ML/TF risks to which it is exposed through the IRA process, senior management of an II should implement effective AML/CFT systems that can adequately manage and mitigate those risks. The following examples were observed in our inspections:

EXAMPLES

i. In one case, senior management of an II failed to detect lack of rigor in which compliance reviews on AML/CFT matters were being conducted, leading to non-compliant practices going undetected.

ii. In another case, compliance reviews were adequately conducted and identified significant deficiencies, which were not rectified in a timely manner due to insufficient follow-up on the progress of planned actions. Eventually the deficiencies appeared to fall off the radar screen altogether.

iii. In some other cases, lack of resources for the AML/CFT function resulted in sloppiness when carrying out essential duties. To enable the Compliance Officer ("CO") and Money Laundering Reporting Officer ("MLRO") of an II to discharge their responsibilities fully and effectively, senior management should ensure that they and the functions supporting them are allocated with adequate resources.

Above all, senior management should ensure that adequate resources are allocated for effective functioning of AML/CFT systems and establish a robust oversight mechanism to ensure that the systems are able to meet the relevant statutory and regulatory requirements.

2) Compliance functions

The AML/CFT regulatory regime relies on an II to develop compliance controls and procedures to address the risks to which it is exposed. This places responsibility on (and gives autonomy to) the IIs in designing the systems for specific operations, in which the compliance function has a crucial role to play.

The CO in an II and the compliance function which he/she leads is the focal point for oversight of ML/TF prevention and detection, providing support and guidance to senior management so that risks are identified, understood and managed. Specifically, the CO should be responsible for the following:

a. developing and continuously reviewing the AML/CFT systems to ensure that they remain up-to-date, can meet prevailing statutory and regulatory requirements, and are effective in managing ML/TF risks arising from the business of an II;

b. overseeing the AML/CFT systems of an II which include general monitoring and enhancement of the controls and procedures where necessary; and

c. communicating key AML/CFT issues with senior management, including any significant deficiencies identified.

Some examples were observed in our inspections:

EXAMPLES

a) Development and review of AML/CFT systems

i. In one case, the compliance function was required to certify at regular intervals that an AML/CFT control had been carried out effectively and in line with prescribed timelines. However, the staff concerned did not undertake any robust checking before granting certification, relegating it to a "tick-box" mechanism that gave a false sense of assurance.

ii. In the second case, after certain AML/CFT processes were found inadequate, the compliance function procrastinated on remediation measures until finally nothing was done.

iii. In the third case, an II procured a new technology-based AML/CFT system and assigned the compliance function to commission it but the staff responsible were not familiar with the system functionalities and limitations, impact on workflow, system coordination and resource implications. In the end, poor calibrations resulted in unsatisfactory outcomes.

These examples reinforce the high integrity that compliance personnel must bear, never allowing assurances to be reduced to tick-box exercises and be determined in rectifying deficiencies. The senior management must also acknowledge that no matter how comprehensive the skill set is, gaps still exist. The compliance function should be properly resourced and able to gain access to, and obtain cooperation and accountability from, other operating units.

b) Monitoring effectiveness of AML/CFT systems

i. There were instances where the compliance function did not conduct sample tests on a sufficiently regular or extensive basis to ensure early detection of control weaknesses. As a result, deficiencies in certain AML/CFT controls and processes went undetected for prolonged periods.

ii. This problem was exacerbated when the II placed heavy reliance on incident reporting protocols to assess the adequacy of regulatory compliance and the effectiveness of AML/CFT systems, leading to flaws being kept away from senior management.

A fundamental role of the compliance function is to make vigorous and continued assessment on adequacy of the AML/CFT systems installed by an II, with sample testing commonly used for this purpose. The compliance function should ensure that any weaknesses identified are drawn to the attention of relevant operating units in the II and to that of the senior management where appropriate, and follow up with a proper remediation plan.

c) Communication with senior management

Some isolated cases revealed an absence of records on discussion or reporting about AML/CFT matters at senior management meetings, on top of instances where defects in the AML/CFT controls were not escalated to senior management or played down. In other isolated cases, progress was not followed up after deficiencies were reported to senior management.

Although senior management do not want surprises, this should not be mistaken as a call on the compliance function against filing timely reports. A CO with strong integrity will champion his/her transparency and proactiveness by escalating issues which deserve rectifying to senior management in a prompt and accurate manner. Failure to do so may result, for extreme cases, in significant AML/CFT risks being ignored, jeopardizing the AML/CFT system of an II and its reputation.

3) Customer risk assessment ("CRA")

As part of the CDD obligations under AMLO, an II is required to assess the ML/TF risk associated with a business relationship. This process is usually referred to as a CRA which determines the extent of CDD measures to be applied. The following examples were observed in our inspections:

EXAMPLES

a) Lack of risk assessments

In one case, the AML/CFT policy of an II required, as part of the CRA process, for risk profile of the customer to be assessed by relevant risk factors and scores. Despite this, the II was unable to produce documentary evidence that such assessments were being conducted in practice. In another case, while the II was assigning risk ratings to some customers sporadically, it was not doing it consistently for all customers.

b) Risk assessment before formation of business relationship

In one case, the outcome of ML/TF risk assessment for customers produced by the AML/CFT system of an II was not available prior to business relationships with the customers being formed due to system limitations. As a result, customers were not assigned with correct risk levels nor subjected to appropriate CDD measures, with some

high-risk customers not being subject to enhanced due diligence ("EDD").

c) No risk assessment for change of policy ownership

In one case, CRAs (and hence CDD measures) were carried out by the II on insurance policy applications, not for new customers upon change of policy ownership.

Complete, accurate and timely CRAs are essential to calibrate the CDD measures applicable to individual customers. The lack of an effective framework will have a cascading effect on the ability of an II to comply with other AML/CFT obligations, including the requisite EDD measures and annual reviews of high-risk customers.

4) Customer due diligence

When IIs detect high ML/TF risk concerning a business relationship, they should apply EDD measures to mitigate the risk and obtain approval from senior management before establishing or continuing the business relationship. The following examples were observed in our inspections:

EXAMPLES

a) In some cases, EDD measures were not carried out on policyholders classified as high risk by the II and approvals were not obtained from senior management. Sometimes it was attributed to failure of the system to screen out persons classified as high risk.

b) In one case, while internal approvals were obtained before establishing business relationship with high-risk customers, the responsible personnel were not part of senior management as required by the Guideline.

There is a strict legal obligation to apply EDD measures and obtain approval from senior management before establishing or continuing a business relationship with customers classified as having high ML/TF risk. The IIs should implement robust controls to ensure compliance with this obligation.

5) Politically exposed persons ("PEPs"), terrorists and sanction designations

AMLO places specific obligations on IIs with regard to customers and beneficial owners who are PEPs as well as situations presenting high ML/TF risk that might involve PEPs. The IIs are expected to establish and maintain effective procedures for determining whether a customer or a beneficial owner is a PEP and for the purpose of carrying out its obligations in relation to high ML/TF situations. Most IIs have installed screening systems for this purpose. The following examples were observed in our inspections:

EXAMPLES

a) Algorithm design and system calibration

Many IIs customized AML/CFT screening systems procured off the shelf by adding algorithms, scoring parameters and system settings.

Examples were observed where responsibility for calibrating the scoring parameters in such algorithms and for selecting system settings was assigned to the compliance function of an II. Due to lack of technical knowledge and understanding of the algorithms being used, system functionalities and interaction of the system with screening databases, scoring parameters and selection setting caused the system to become ineffective in generating alerts for customers. In other words, whilst the compliance function had attempted to produce accurate screening alerts, inability to master the algorithm, systems and databases (and their interaction) resulted in alerts not being generated for genuine hits.

b) Wrongful clearance of alerts

In one case, certain alerts generated by the screening system were dismissed by the II as false positives without documented review. Some of these alerts were later found to be associated with PEPs that should not have been missed.

In another case, alerts relating to PEPs were taken by the compliance function as being false positives based solely on comments from the referring departments without conducting the requisite due diligence or providing sound justification.

c) Screening of beneficial owners

Some IIs did not screen beneficial owners on an ongoing basis because information was not captured by the policy administration system.

Screening systems and other technological applications are integral to the AML/CFT controls and processes of an II. However, it is imperative that proper and robust governance, testing and change management is followed throughout the system life-cycle by qualified personnel equipped with requisite skills. It is worth reiterating that the compliance function should always act with integrity, courage and diligence when discharging its role.

6) Premium collection

When a policy holder uses an unrelated third party to pay premiums, the beneficial owner or source of funds may be obscured. This raises a red flag which section 23 of Schedule 2 to the AMLO compels an II to address using a risk-based approach ("RBA") by putting in place controls and processes to identify premiums paid by a third party, validate the

relationship between the policy holder and the payor, and ascertain underlying reasons for the arrangement.

For premiums paid by cashier order, it was not uncommon for IIs to set a threshold in determining whether proof of payment coming from the policy holder (as opposed to a third party) should be sought, below which additional control was necessary, complemented in certain cases by sample testing or self-declaration by the customer with his/her insurance agent acting as a witness.

Competitive tension drove up the threshold in some IIs to inordinately high levels that this risk had become so manifest as to undermine the AML/CFT controls altogether. Examples of policy holders signing declarations to say that they had purchased the cashier order were found to be false. In reality, many cashier orders had been purchased by the insurance agent who witnessed the signing off of self-declaration.

We have made reference to the requisite skill set of contemporary compliance personnel, but the most important attribute which the compliance function and senior management of an II must possess is common sense. Even after the inordinately high thresholds had been revealed, there was reluctance by some IIs to act for fear of losing market share, compelling the IA to promulgate a circular on 9 April 2024 announcing prescriptive controls that reduce the discretion enjoyed by IIs and hampers flexibility to cater for the diversity among market participants.

7) Ongoing monitoring

Since ongoing monitoring is essential to the effectiveness of AML/CFT systems, an II should continuously assess its business relationship with a customer through CDD and transaction monitoring as per section 5 of Schedule 2 to AMLO. The former involves periodic review of documents, data and information about the customer to ensure that they are up-to-date and relevant, the latter entails identifying suspicious transactions. The following examples were observed in our inspections:

EXAMPLES

a) <u>Annual review of high-risk customers</u>

In one case, an II was using pre-defined criteria that filtered out most of its high-risk customers, causing less than 10% of them being subject to annual review. In another case, an II failed to perform annual review on certain high-risk customers because of deficiencies in its database and data extraction process. In the third case, an II did not perform annual review on high-risk customers necessary to verify and update CDD information.

b) Inadequacy of transaction monitoring

In one case, the II with a sizeable portfolio performed transaction monitoring using only two sets of exception reports. In a second case, the II did not generate exception reports at all. In a third case, issues with the data extraction process resulted in alerts not being generated despite that the II had adequate transaction monitoring reports in place.

c) Duplicated internal customer identity ("ID") number

Most IIs make use of ID numbers to facilitate administration of customer accounts and policy management, as well as to monitor and detect the pattern of suspicious transactions. However, duplicated ID numbers were occasionally created due to human errors in the data capture process or multiple travel or identification documents provided by the customers. Conversely, there were instances where one ID number was assigned to several customers. These errors will have a knock-on impact on integrity of the monitoring mechanism.

d) Monitoring system alerts resolution

Effective policies and procedures should be available to resolve alerts and adequate manpower should be deployed by IIs to address alerts generated by their transaction monitoring system. An II suffered from significant delay in clearing the backlog of alerts due to manpower shortage, while another II resolved alerts without preserving evidence that profile of the customers and related transactions had been examined or justification for the resolution, suggesting that less than 10% of the alerts had in fact been reviewed.

Since the business relationship between an II and its policyholders typically lasts for years if not decades, it is essential to have in place robust monitoring measures so that the II can keep abreast of change in circumstances.

8) Suspicious transaction reporting

When the transaction entered into by a customer appears unusual or is inconsistent with the knowledge on that customer, an II should take further steps to ascertain if there is suspicion in accordance with the obligations set out in section 5 of Schedule 2 to AMLO. The following examples were observed in our inspections:

EXAMPLES

a) In one case, suspicions were raised about the sources of wealth and/or income which did not align with the profile of several customers. The MLRO decided not to report them to the Joint Financial Intelligence Unit ("JFIU") on the ground that payments were made via regulated financial institutions.

b) In another case, despite being presented with multiple red flags including splitting of cash payments, undisclosed third-party payments and making of false declarations, the MLRO still concluded that the case was not suspicious.

c) In the third case, an II simply failed to recognize red flags that demonstrated a lack of vigilance in monitoring suspicious transactions.

d) In the final case, the MLRO spotted irregular premium payments made by a person not known to the policyholder for years and undertook further investigation, but did not record the findings or the justification for not reporting to the JFIU.

Since IIs are expected to exercise maximum vigilance on suspicious transactions, the MLRO should be objective and impartial when evaluating whether a transaction needs to be reported to the JFIU. Inclination against reporting and recording the deliberations made should be avoided at all costs.

UPDATE ON APPROACH TO AML/CFT INSPECTIONS

The AML/CFT inspections are meant to ascertain that IIs are in compliance with their obligations under Schedule 2 to AMLO supplemented by the Guideline. The IA will draw attention of IIs to weakness in the way that they comply with these obligations via the following three communication tools:

a) **Management Letter** - issued where divergence from the regulatory requirements is minor but nonetheless needs to be addressed.

b) **Compliance Advice Letter** - issued where divergence from the regulatory requirements constitutes non-compliance of a less serious nature, admonishing the II to effect rectification within a short and realistic time frame.

c) **Letter of Concern –** issued where divergence from the regulatory requirements constitutes non-compliance of immediate concern that comes close to triggering disciplinary sanctions. It demands cease and desist, the failure of which will be taken into account in determining the sanctions to be imposed in the future.

Regardless of the communication tool chosen, the II will have an opportunity to outline the remedial actions to be taken within a reasonable timeframe and be invited to conduct an independent review by internal or external auditors. This allows the II to vindicate its compliance culture and its desire to achieve continual improvement.

In certain instances, the IA spotted non-compliances so blatant and serious as to make disciplinary sanctions inevitable. This includes cases where non-compliances are obvious and pervasive, of a systemic nature, expose weaknesses in governance, widely known within the II and not rectified for a prolonged period of time. Even when the

disciplinary process is initiated, the IA will ensure that it is expeditious and take into account the response, cooperation and contrition showed by the II as mitigating factors.