Date: 13 March 2020

Dear CEO,

Observations by the IOMFSA in relation to Isle of Man Trust and Corporate Services Providers ("TCSPs") compliance with regulatory and financial crime requirements

As part of its supervisory programme the Isle of Man Financial Services Authority ("the Authority") undertook a number of inspections of class 4 and 5 licenceholders during 2018 and 2019. These inspections were focussed on individual licenceholders' compliance with their regulatory and financial crime obligations and did not form part of a specific thematic review. In addition to the inspections the Authority has numerous other touch-points with class 4 and 5 licenceholders as part of on-going supervision including but not limited to material consent matters.

The purpose of this letter is to bring to the sector's attention areas where observance of requirements, either identified by the Authority through its inspection programme or through more general supervision, was lacking or ineffective and where practices should be improved.

Risk Management

The Financial Services Rule Book 2016 ("Rule Book") requires each licenceholder to establish and maintain comprehensive policies, appropriate to the nature and scale of its business, for managing its material risks, including financial, legal, regulatory, group risk, operational risk and risks to the licenceholder associated with the activities of its clients.

It is the board's responsibility to ensure that it has an effective risk management framework in place and that front-line staff, as well as risk and compliance functions, are aware of what risks are acceptable and not acceptable. Licenceholders need to be able to demonstrate that all material risks are considered and are adequately monitored and controlled. Simply having detailed policies and procedures is not sufficient. Licenceholders must be able to demonstrate oversight of risk and that policies and procedures are implemented, understood and effective. This includes a clear articulation of the key risks and the nature and effectiveness of the controls that are employed to mitigate these risks. Licenceholders should continue to develop risk management frameworks, in a manner proportionate to the nature and scale of their business, in order to demonstrate same.

The Authority has observed that compliance frameworks tend to be more mature in licenceholders but that broader risk management frameworks are less mature. This means that aspects of risk management are only considered in a very generic, high–level manner without sufficient consideration of the specificities of the actual business and operations. Areas where we observed weakness in risk management include operational risk, financial resources and reliance on group (including operational, staffing and financial resources). Risk management in relation to the threat of money laundering and terrorist financing is specifically addressed later in this letter.

The Rule Book does not require the appointment of a Head of Risk but does require the appointment of Head of Compliance, whose responsibilities are outlined. Compliance is part of an effective risk management framework, it is not the entirety. Where we are seeing deficiencies in risk management we are seeing a lack of risk expertise within the licenceholder and a lack of clarity of ownership of aspects of risk management.

Risk Appetite

Risk appetite follows on from the broader consideration of risk management. The Authority recognises that the current operating environment is leading to changes within the TCSP sector. In some instances this will have led or will lead to changes to licenceholders' business strategies and plans. Whilst the Rule Book does not specifically stipulate that Class 4 and 5 licenceholders maintain a documented risk appetite, it is none the less important that licenceholders are clear as to the amount and type of risk that they are willing to pursue, retain or take. This risk appetite should be appropriately cascaded to staff and the amount and type of risk within the business should be monitored and controlled. The consideration of risk appetite should be clear in the decision making processes of the licenceholder.

Where licenceholders are changing strategies, for example, significant growth strategies or targeting different customer types the Authority expects licenceholders to have assessed (and be able to demonstrate this assessment) matters such as but not limited to:

- Whether this introduces greater or new risks;
- How these risk will be mitigated and whether changes are required to the internal control and risk management frameworks, resourcing and operating model etc. to ensure that they remain adequate;
- If changes are required when and how will they be implemented; and
- Whether risks will continue to be within existing appetite or is there an agreed change in appetite.

<u>Compliance with Anti-Money Laundering and Combating Financial Terrorism ("AML/CFT") requirements</u>

The following observations relate specifically to compliance with AML/CFT requirements.

Business Risk Assessments ("BRAs")

As per Part 3 paragraph 5 of the Code licenceholders are required to carry out a BRA that estimates the risk of ML/FT posed by a licenceholder's business and customers.

A licenceholder must document the consideration of its ML/FT risks pertaining to the licenceholder's services / products, customers, jurisdictions and distribution channels, mindful of the nature scale and complexity of the licenceholder's business model. This risk assessment must have regard to the specificities of the licenceholder's business and be kept up to date to reflect any changes in the business.

The Authority has observed repeated instances of BRAs where the AML/CFT risks are identified at a generic level but with little or no qualitative assessment of ML/FT threats specific to a licenceholder's business and their customers. Where we have seen this approach to risk in BRAs we have observed that the mitigating factors and controls tend also to be addressed in a generic manner and are not sufficiently focussed on the licenceholder's own control framework or the potential risks posed.

Failure to adequately consider the specificities of actual business models and operations potentially leaves a licenceholder more susceptible to the risks of ML/FT. A generic BRA of itself does not demonstrate a clear understanding by the licenceholder of the ML/FT risks within the business.

Customer Risk Assessments ("CRAs")

Part 3 Paragraph 6 of the Code requires licenceholders to carry out a CRA prior to the establishment of a business relationship. A CRA should be based on a model which reflects all relevant factors. It should include up to date and relevant information. It should be applied diligently, with effective follow-up where risks are identified or more information is needed. In many of the inspected CRAs the Authority observed one or more of the following deficiencies:

- CRA forms utilised were not compliant with the requirements of the Code with important risk factors not being considered;
- Information contained in CRAs and used to assess the risk rating was inconsistent with information retained on file and did not always accurately reflect the reason for establishing the structure, the underlying activity and customer associated risks;
- There was a lack of financial and transactional information on file for customer entities including intended volume, frequency and value of transactions. Where this information was on file at the outset there were numerous instances where this information was not maintained. In the absence of financial and transactional information it was not evident how the licenceholder could identify, assess and appropriately report any unusual or suspicious activity;
- Limited or no documented consideration of complex structures;
- There were significant examples of deficiencies in source of funds and source of wealth information/verification;
- The basis of the risk rating was insufficiently clear and / or insufficiently documented both on inception of the client relationship and on an ongoing basis;
- The risk rating did not appear consistent with the actual money laundering risk associated with customers and their structures.

Complex corporate structures by their very nature are open to misuse and may therefore pose a higher ML/FT risk. Complex structures may have a number of layers across multiple jurisdictions, which can make it more challenging to identify the ultimate beneficial owner. It is therefore essential that when accepting or establishing complex structures on behalf of customers that licenceholders conduct the appropriate level of due diligence in order to be able to assess and evidence that the structure is appropriate to be on-boarded.

The customer must be able to provide the relevant documentation and provide a robust explanation for the use of the structure. Typically this will require licenceholders to obtain Customer Due Diligence ("CDD") appropriate to specific Complex structures rather than generic information. It is the Authority's expectation that staff of the licenceholder fully understand and document their understanding of the structure and an explanation why it is acceptable and within stated risk appetite to accept the customer. The Authority expects the licenceholder to be able to evidence and articulate this on an ongoing basis.

Related to the above deficiencies the Authority also observed instances where follow-up actions record on the CRA were either not followed-up in a timely manner or not followed up at all. This is indicative of weaknesses in internal control frameworks and potentially a lack of clarity for front-line staff as to what is acceptable from a risk perspective.

Enhanced Due Diligence

Part 5 paragraph 15 of the Code requires licenceholders to establish, record, maintain and operate appropriate procedures and controls in relation to undertaking enhanced customer due diligence.

In some instances where licenceholders had identified customers as being higher risk and therefore subject to enhanced due diligence there was a lack of clarity to what this entailed and the consistency of the application. Enhanced Due Diligence should be undertaken at the time of on-boarding the customer.

Board Responsibility and Oversight

The board of a licenceholder is ultimately responsible for ensuring that the licenceholder conducts its affairs in an appropriate manner and meets its regulatory obligations. It follows that where we identify inappropriate practices and / or material deficiencies in compliance with regulatory obligations we will hold the board accountable for its oversight of the licenceholder's affairs.

It is the board's responsibility to ensure that there is adequate four eyes oversight applied within the business, that key function holders are competent for their roles and that there is sufficient breadth of relevant experience, adequate levels of resource and expertise across the business as a whole. It is also open to the board to obtain additional opinion or quality assurance from suitable third parties should that be considered necessary. It is not sufficient to simply attribute blame to an individual whether that individual be a controlled function holder

We have observed instances where licenceholders have failed to adequately address non-compliance previously identified by the Authority. In these circumstance it is likely that the Authority will take more significant action. Similarly the Authority is also likely to take more significant action where licenceholders have failed to adequately address non-compliance highlighted by its staff. It is the board's responsibility to ensure that these matters are addressed in a timely manner and that it has satisfied itself that appropriate action has been taken or resolution achieved.

As a CEO, we ask you to consider this letter carefully and to discuss it with your board. The board should seek to understand whether any of the matters identified in this letter are applicable to the licenceholder and to take appropriate action to address any deficiencies in a timely manner. The supervisory teams will follow-up in 2021 with a sample of licenceholders as to the board's consideration of the matters outlined in this letter, including:

- What enquiries the board has made to understand whether any of the deficiencies outlined in this letter are present in the licenceholder;
- The outcome of these enquiries;
- What action has been undertaken / will be undertaken to address identified deficiencies.

Please be advised that, where there is non-compliance with the relevant requirements, the Authority will have regard to the consideration given by licenceholders to this correspondence, when exercising its regulatory and enforcement powers.

Yours faithfully,

Colin Manley

Head of Insurance, Pensions and Fiduciary Services