CAYMAN ISLANDS
MONETARY AUTHORITY

To: All Licensees

From: Cayman Islands Monetary Authority

Date: 9 February 2016

Supervisory Issues and Information Circular

We are pleased to introduce the first edition of the Cayman Islands Monetary Authority's (the "Authority") *Supervisory Issues & Information Circular,* which will be issued bi-annually. The document aims to raise awareness, in the industry, of common regulatory and thematic issues identified through our off-site and on-site supervisory practices and highlight regulatory developments for the financial sector.

As a secondary objective, the circular also aims to emphasize regulatory matters which might not be particularly problematic at this time but are important to our regulatory objectives.

Regulatory Highlights

Below are a number of regulatory initiatives and regulatory matters that we wish to bring to your attention at this time. We expect that all licensees will be mindful of the matters below in the normal course of conducting business and in the development of new business strategies, plans and ventures in the future.

De-risking

"De-risking" refers to financial institutions exiting relationships with and closing the accounts of clients considered "high risk." Over the past nine months this issue became quite topical locally as money service businesses ("MSBs") in the Cayman Island, as in other parts of the world, were faced with the withdrawal of banking services. A key factor in de-risking is the dependence on both local and foreign correspondence banking relationships, which provide access to the global financial system. As the primary financial services regulator in the Cayman Islands, the Authority continues to be very much engaged, locally and internationally, as de-risking poses a potential threat to other segments of the financial services industry. The Authority strongly encourages financial institutions to implement a risk based approach, and only terminate customer relationships on a case-by-case basis, where the money laundering and terrorist financing risks cannot be mitigated.

CFATF Review – Q2 2017

During the second quarter of 2017, the Cayman Islands is scheduled to be reviewed by the Caribbean Financial Action Task Force, a regional organization that is an associate member of the Financial Action Task Force. The CFTAF members have agreed to implement common counter measures to address the problems of criminal money laundering and terrorism financing by adopting the FATF 40 Recommendations for combating money laundering and the financing of terrorism and proliferation. The last assessment of the Cayman Islands took place in 2007 and preparations for the 2017 review are in process. Many of you may be aware that a National AML/CFT Risk Assessment exercise (NRA) was launched by the Government in October 2014, which included representatives from both the Authority and the financial services industry along with other Governmental agencies and private sector industries. The object of the NRA was to identify threats and vulnerabilities and identify strategic actions to mitigate the risks identified. The Government is in the process of finalizing the NRA Report. At the same time, the Authority and the Government continue to work to address any known or identified areas of weakness.

The Authority will keep you apprised of developments, particularly as the industry will be engaged in various capacities as we work to prepare for the assessment.

Outsourcing

We understand that our licensees will continue to look for opportunities to reduce costs by outsourcing key operational functions. The Authority wishes to remind licensees of the importance of due diligence and risk assessment of providers of outsourced services as well as the importance of proper supervision of those services in accordance with the *Statement of Guidance on Outsourcing* released in August 2015. The Authority also wishes to emphasize that while it is acceptable for certain tasks to be performed by a third-party provider, the responsibility to supervise covered activities for compliance with applicable laws and regulations, as well as self-regulatory organizational rules, remains with the governing body and senior management of the licensee. This concern is also applicable to employees of affiliates conducting certain functions on behalf of the licensee.

Data Security

Licensees should remain focused on their organisation's data security given the persistence of threats as cybersecurity issues continue to rise globally. As entities in an International Financial Centre, Cayman Islands based firms are exceptionally vulnerable to data breaches. Thus, the Authority sees this issue as important and one that requires ongoing attention. While we recognise that many of our licensees have robust data security systems, we also recognise that there may be others that simply do not, or may have systems that are improper or inadequate. Going forward, the Authority will review licensees' approaches to data security risk management. Depending on a licensee's business and risk profile, we will examine one or more of the following areas: technical controls, incident response, and staff training. As part of our reviews, the Authority will also consider licensees' ability to protect the confidentiality, integrity and availability of sensitive customer and other information.

Risk Registers

Through our recent off-site reviews we have observed that a small number of larger licensees have successfully developed and implemented "living" registers, as a part of their risk framework, to identify, capture, monitor and mitigate key risks specific to their business activities and operations. These risk registers – which are widely used by institutions in all major financial centres – provide senior management and the Board with a key tool to (i) assess how the business environment is changing, (ii) evaluate the probability and impact of changes to a licensee's business and risk environment and (ii) put in place mitigating actions and controls to eliminate or at least minimise its risks. Over the past year we have seen a rapidly changing market environment that has given rise to new business, management and operational risks. Going forward, licensees need to be highly vigilant as to how they manage these new developments – to this end, putting in place a dynamic risk register is a vital management tool. During the course of the year, the Authority will be making further enquires as to the steps being taken by licensees to improve the way they monitor and manage emerging risks.

Fraud Prevention and AML Convergence

In recent years, regulators and industry participants worldwide have seen great benefit in converging AML and fraud prevention initiatives. With the appropriate systems and internal controls, holistic approaches to suspicious customer behaviour, inclusive of AML and fraud indicators, allow licensees to more effectively and efficiently prevent financial crime as a whole, especially in cases where AML/CFT risk is low. The inclusion of fraud detection and prevention within a robust AML regime can also help licensees manage AML risk better as the proceeds of fraud quite often become the subject of money-laundering offences. As such, licensees should review their current AML and fraud regimes and begin to streamline their approaches, or at minimum expand their AML regimes to include some guidance on fraud prevention. Firms currently without fraud regimes should look to develop a programme robust enough to identify and

deter potential cases of fraud, based on the nature, scale and complexity of their business. This fraud policy can be included in the licensee's current AML manual.

Regulatory Issues

Our supervisory work over the last year brought to our attention a few regulatory issues which at times contributed to licensees compromising the quality of service provided to customers, as well as compliance and supervisory breakdowns. Most prevalent of the issues identified was the inconsistency with which licensees implemented their Anti-money Laundering and Countering Terrorist Financing (AML/CFT) regimes. Notable inconsistencies were evident even among licensees within the same peer group.

As such, we have provided a summary of the minimum elements we expect to see in a well-functioning AML/CFT programme.

Anti-Money Laundering and Countering Terrorist Financing

Overall AML Programme

Given the jurisdiction's susceptibility to reputational risk, we wish to remind licensees of the importance of robust due diligence and AML/CFT regimes. Overall we expect licensees to have in place AML/CFT programmes that:

1. Use a risk assessment process to identify the products, services, customers, third parties, and locations that are more vulnerable to money laundering and financing of terrorism.
2. Assign responsibility for AML compliance to an appropriate person who will keep senior management and the Board informed.
3. Implement risk-based Customer Due Diligence (CDD) policies to help identify and monitor vulnerable accounts and relationships.
4. Identify reportable transactions and comply with reporting requirements.
5. Provide dual control and segregation of duties as appropriate.
6. Train and supervise employees to be aware of and compliant with AML/CFT regulations.
7. Report and maintain records as required.

Client Risk Rating

Our supervisory work over the last year has revealed various weaknesses associated with client risk rating. The application of risk rating to clients and related monitoring was not consistently observed amongst licensees. Licensees are required to conduct a risk assessment of their clients, and make a distinction between high and low risk cases in accordance with section *3.109* of the Guidance Notes on the Prevention and Detection of Money Laundering and Terrorist Financing in the Cayman Islands, which was updated in August 2015.

As guidance, here are some of the basic elements licensees may wish to include in their respective client rating methodologies:

1. Identification of AML/CFT Risk

The licensee should have a clearly documented methodology for identifying risk factors specific to its customers. The methodology should identify the main risks, given the nature of the business. Some risk factors include, but are not limited to:

- *Type of Customer* (organisation, individual, PEPs, NGO, etc.)

- *Account Types*
- *Product Types*
- *Types/Volume of Activity*
- *Other Risk Factors*
  - Type of business
  - Occupation (for individuals)
  - Length of relationship
  - Relationship history, i.e. Previous subject of SAR filing, subject of subpoena, subject of negative press
  - Country of residency
  - Country of incorporation
  - Country of operation

2. Analysis of AML/CFT Risks

The licensee's risk methodology should include guidelines for determining clients' risk level or risk score.

Options

Licensees can decide whether to (1) apply an initial/default rating to their clients at on-boarding subject to a subsequent risk assessment at a later date or (2) conduct a full risk assessment at on-boarding. Whether the licensee applies a default rating or a full risk assessment at on-boarding will depend on the information available to the licensee at the time, sophistication of their systems or risk models, availability of trend data etc. Clients given a default rating should be reviewed under a full risk assessment methodology within a year after on-boarding at most.

Default Risk Rating At On-boarding

- One option is the application of a default risk rating, which automatically flags the new customer for a probationary period during which the customer is subjected to closer scrutiny until a risk rating is applied under the licensee's risk based framework.
- If the customer's profile highlights any of the indicators conventionally associated with the heightened risk of money laundering exposure, the licensee should apply a higher risk rating initially as a default for specified customer types.

Full Risk Assessment

Another option is to conduct a full risk rating of the client. The risk assessment should identify risks inherent to the client and determine the overall risk score. The methodology for calibrating individual risk factors into a single rating risk score should be clearly documented. This may be qualitative, mathematical or a combination of both.

Risk Classes

Clients should be categorized into risk groups or risk classes. Risk classes may be simple in development, such as low, medium, and high, or they can be more elaborate, such as low, medium, medium-high, high, and very high. Smaller licensees with simpler business profiles can apply a simple risk classification schematic, whereas more complex institutions may opt for a more expansive risk classification schematic. Criteria for risk groups or classes should be clear and well documented.

3. Client Rating Reviews and Monitoring

The development and implementation of a monitoring regime is vital to the overall client rating process. The licensee should have well documented policies which outline frequency for review, treatment of high risk customers, etc.

Frequency of Client Reviews

The licensee should have procedures that outline the frequency of reviewing the risk ratings assigned to clients. It should also include procedures for moving clients from one risk band to another. The following timelines are generally applied:

- High-risk clients: periodic AML KYC reviews every 6-12 months
- Medium-risk clients: periodic AML KYC reviews every 12-24 months
- Low-risk clients: reviews every 24-36 months

In general, when conducting periodic AML KYC reviews, AML/compliance or assigned officers should normally review the elements below:

- Review each customer's information: name, address, ID number, certificate of good standing (if applicable), and the customer's original information to determine if there are any material changes
- Rescreen each customer's information against specially designated and country-based sanctions lists. In instances where there is a substantive change (i.e., a different country of residence), the compliance staff needs to reassess and reapply the risk rating for that customer
- Review the types of transactions performed by each client and compare against the forecasted or anticipated account activity (normally performed via automated transaction screening tools)
- Determine any potentially suspicious activities that were not detected by the firm's real-time transaction monitoring platforms or systems.

4. Treatment of High Risk Clients

The licensee should have documented procedures that outline how clients will be treated once they have been assessed as high, medium or low risk. The treatment of clients in various risk classes should aim to manage the risks identified and assessed in the previous process. The licensee's methodology should clearly document strategies, policies and procedures that help to reduce the risk identified.

Examples of strategies, policies or procedures that will help mitigate risk are:

- Applying enhanced monitoring to high risk clients
- Having different identification and verification methods for higher risk clients
- Having a management approval processes in place for higher risk clients

5. Recording Client Risk Classifications

Clients' risk ratings should be clearly recorded and accessible to all relevant personnel. The licensee should also be able to generate useful reports for their own use and for regulatory review if necessary. For example, reports showing only clients rated as high or reports that list all clients by risk classification etc.

AML Monitoring Regimes

The Authority continues to assess the adequacy of licensees' monitoring for suspicious activity, including their transactional activity, trading activity and products and services. Licensees should routinely test their systems and verify the accuracy of data submitted to them to ensure that all risks are properly identified and assessed. In situations where a risk-based decision is made to exclude certain customer transactions from one or more aspects of AML surveillance, the rationale for the decisions should be documented.

The Authority makes it a priority to assess the adequacy of licensees' monitoring of high-risk customers and transactions. When monitoring customer transactional activity, firms should ensure that the business purpose of higher risk transactions is understood to enable the firm to assess whether the transactions are suspicious, considering what the firm knows or should know about the customer and the customer's anticipated activity. The Authority also wishes to remind licensees to consider reviewing customers' activity over a period of time sufficient to identify patterns and ensure they assess the full picture of activity. When firms delegate the monitoring of suspicious activity to personnel outside of the AML function, firms should ensure that appropriate delegation has been made, and that the AML function has an open line of communication with the personnel conducting reviews of the activity.