FINANCIAL SUPERVISION COMMISSION

DEPOSIT TAKING (BANKS)

THEMED VISIT PROGRAMME 2014-15:
AML / CFT – SUMMARY FINDINGS, ISSUED JULY 2015

CONTENTS

Glossary of terms

AML	Anti-Money Laundering
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
EDD	Enhanced Due Diligence
MLRO	Money Laundering Reporting Officer
PEP	Politically Exposed Person
SAR	Suspicious Activity Report

1. Introduction

Under the Financial Services Act 2008 the Commission has a regulatory objective for the reduction of financial crime. In order to help fulfil this regulatory objective the Commission carried out themed on-site reviews at certain banks between April 2014 and March 2015 with a focus on Anti-money Laundering and Countering the Financing of Terrorism ("AML & CFT") processes and controls.

The Commission does not enforce the Anti-Money Laundering and Countering the Financing of Terrorism Code 2015[1] ("Code"); however, compliance with this Code is a "regulatory requirement" under rule 8.2 (c) (iv) & (v). The responsible officers[2] of a bank are responsible under rule 8.3 (1) for compliance with the regulatory requirements. Under rule 8.4 (2) (e), the responsible officers must establish and maintain appropriate safeguards to prevent and detect any abuse of the licenceholder's services for money laundering, financial crime or the financing of terrorism.

The Anti-Money Laundering and Countering the Financing of Terrorism Handbook ("Handbook") articulates the Commission's expectations of banks. The Commission however recognises that banks may have systems and procedures in place which, whilst not identical to those in the Handbook, nevertheless impose controls and procedures which are at least equal to if not higher than those in the Handbook.

The Commission's visit teams reviewed banks' internal and operational controls, systems, policies and procedures, with a particular focus on the following areas:-

- Suspicious transaction / activity reporting
- High-risk review processes
- Remediation of back-book clients (where relevant)
- Customer screening techniques[3] (*for PEPs, sanctions and other adverse information*)

The purpose of this feedback is to highlight the Commission's key findings from the AML / CFT on-site reviews that took place between April 2014 and March 2015.

[1] This Code was introduced with effect from 1 April 2015 and references in this document refer to the relevant provisions under this Code. However, the relevant piece of legislation at the time of the visits was the Money Laundering and Terrorist Financing Code 2013.

[2] For a bank incorporated in the Island, "responsible officers" means its directors. For a branch, "responsible officers" means senior management which includes Isle of Man resident officers.

[3] The Commission provided a list of test names to banks in advance of visits, for the banks to run through their screening systems as though those clients were being taken-on, periodically screened, or if a payment was being made.

2. Key findings

2.1 Suspicious transaction / activity reporting

2.1.1 Reporting procedures and suspicious activity report ("SAR") reporting forms

- In a number of banks the internal disclosure reporting form used by staff to report suspicions to the MLRO did not require (or include) sufficient detail to be provided to the MLRO to enable them to conduct a full investigation. This can result in the MLRO having to undertake additional work that should already have been documented as part of the internal disclosure.

  There was also found to be a lack of consistency within some banks in respect of the review of internal disclosures undertaken by the MLRO. In the majority of cases where information was lacking, this was attributed to the form being used by the MLRO to undertake the review. There was insufficient space to record any additional checks undertaken, the conclusions of the MLRO's investigation, and reason for reporting onwards to the Financial Crime Unit or not, as appropriate.

  The Commission did, however, see some very good examples of forms used and also shared a 'best practice' template for the MLRO evaluation with some banks. Based on these findings, a template form covering the internal disclosure and the MLRO evaluation is attached at ***appendix 1***, and the Commission will consider if this should be incorporated in the Handbook in due course.

- In some banks, there were no, or only limited, formal procedures in place which covered the review undertaken by the MLRO of any SARs received (refer paragraph 26 of the Code). It is important that banks have clear documented procedures in place, to ensure reviews are undertaken on a consistent basis. The procedures should detail any additional enquiries to be made by the MLRO and, if not a requirement as part of the pre-submission of the SAR, should also include a requirement to ensure CDD is adequate (or updated information obtained) as required by section 7.2.4 of the Handbook.

- Section 7.2.4 of the Handbook states that the MLRO must acknowledge receipt of a SAR and at the same time provide a reminder (to the reporter) of the obligation to do nothing that may prejudice enquiries i.e. tipping off the customer or any other third party. This was not being undertaken in full by all MLROs.

2.1.2 Other issues

- In some banks, only a very small number of SARs were being made to the MLRO, which was unusual given the both the type of business undertaken, and in comparison to peers. Banks are reminded of the importance of ensuring staff are aware of their legislative responsibilities in respect of reporting suspicions.

- In a small number of cases there was a delay in reporting SARs onwards to the Financial Crime Unit due to secondary checking processes within licenceholders (particularly in times of absence of a second party to undertake such a check). Banks are reminded that any suspicions of money laundering or terrorist financing (whether actual or suspected) must be disclosed to the Financial Crime Unit without undue delay.

2.2 High risk review processes

The Code requires banks to have particular regard to whether a business relationship poses a higher risk. High risk relationships will generally require more frequent intensive monitoring.

Section 3.3 states that the customer risk assessment should be reviewed at least annually for higher risk relationships and Section 3.4.4 of the Handbook states that CDD information held for higher risk customers should be reviewed at least annually. It also suggests that in order to monitor higher risk situations, a bank must consider conducting an annual independent review of CDD information, activity and transactions.

2.2.1 Annual reviews: timeliness

- Whilst most banks were conducting ongoing reviews of higher risk customers, not all banks were conducting them on an annual basis, and there was not always a system in place to ensure these were conducted on a timely basis.

- In some cases, it was difficult for Commission Officers to determine how often reviews were being conducted as the recording systems used did not include the date of any previous review.

- Where annual reviews are behind schedule, the Commission believes it is important that the backlog position is reported outside the team conducting the review so the risk can be monitored (i.e. to a risk committee or board).

2.2.2 Procedures and recording (of annual) reviews

- Not all banks had a procedure for undertaking annual reviews of higher risk clients, or a standard recording form, which meant that some reviews were being conducted on an inconsistent basis.

- In some cases where there were documented procedures, these were conflicting as to how the review should be undertaken, particularly where different departments within a bank were performing the review.

- The Commission believes it is important that reviews are conducted consistently to ensure that an independent review of CDD information, activity and transactions is carried out in accordance with section 3.4.4 of the Handbook for all higher risk customers (and that the customer risk assessment is reviewed as suggested in section 3.3).

  It is also important that full details of the independent review are documented on a consistent basis. Some banks were using a standard annual review checklist/form to document details of their annual review; however, some of these forms did not capture all information expected in accordance with section 3.4.4 of the Handbook. The Commission considers the independent annual review should stand up on its own as a complete but concise summary of the client relationship.

- It is recognised that for some (potentially more complex) customers additional checks/information will be required. Any additional information should be formally documented as appropriate and included within the annual review pack.

- ***The Commission will prepare a best practice template annual review form and this will be included within the sector specific guidance for banks within the new Handbook in due course, to supplement the general guidance for annual reviews contained in section 3.4.4***.

- Within some banks there seemed to be confusion as to what information was classified as standard CDD (which would be expected to be gathered for all clients) and what was classified as enhanced due diligence ("EDD"). Banks should ensure within both their account opening and high risk account review procedures that the difference between CDD and EDD is clear, to ensure that EDD is being obtained for all higher risk relationships. The difference between CDD and EDD is covered in section 4.1.1 of the Handbook.

2.2.3 Trigger events (including CDD at annual reviews)

- In most banks an annual review is classed as a 'trigger event', as a point in time to check the adequacy of CDD information held for clients. However, in a number of banks, where CDD was found to be inadequate and an update was requested from the customer, there was not a robust process in place to ensure this information was received.

  Banks should ensure that where updated CDD is requested from customers as part of a 'trigger event' check (including at the annual review), there is a follow up procedure in place to ensure this is received, and that appropriate action is taken if the information is not received.

2.2.4 Classification as higher risk

- The numbers of accounts risk rated as 'higher' in some banks has increased significantly over the past number of years. Due to the additional sign off and ongoing monitoring processes for higher risk customers, this also has an impact on the resources required to conduct effective ongoing monitoring.

  It was not wholly evident that the impact on resources had been properly considered by some banks, and the Commission suggested to individual banks that their business risk assessment or strategy document should better address the links between higher risk business and availability of resources.

2.3 Remediation of back-book

- It is recognised that varying projects have been, and continue to be, undertaken by banks to remediate their 'back-book' of customers and these are at different stages. This has meant in some situations that not all customers of the bank have been formally risk-assessed to banks' current standards. There could, therefore, in theory be some higher risk customers that are have not been identified as such. However, taking into account the regular screening that banks undertake (see section 2.4 below), the likelihood of a material number of higher risk customers not having been classified as such is considered to be relatively low.

2.4 Customer screening *(for PEPs, sanctions and other adverse information)*

During the Commission's visits all banks were provided with a list of names and asked to run them through any databases used in the following situations:-

a) Take-on of a new client
b) A periodic re-screening of the client base (e.g. overnight sweeps)
c) Inward or outward payments (for sanctions only)

2.4.1 Screening results

- Most banks screened clients manually at account take on, and therefore the names the Commission expected to be highlighted were picked up correctly.

- There were no material issues in respect of inward or outward payment screening, and all banks picked up the expected sanctioned individuals within the list via their payments systems. Some smaller banks, who use other banks to process payments on their behalf, will rely on the payment processing bank for parts of this function.

- Banks screen their general client database(s) on a frequent basis, and in some cases (particularly with the larger institutions) on a daily basis. This screening did, within the majority of banks, identify PEPs and sanctioned individuals/companies (*although see section 2.4.2 below*).

  There were however issues with some banks not picking up clients subject to other adverse information, e.g. disqualified directors, financial crime/narcotics convictions etc. This is particularly relevant for non-higher risk clients who may not be subject to other periodic checks, e.g. high risk annual reviews and trigger events (when searches for adverse information would be undertaken).

  The Handbook, section 3.4.3, now provides more information in respect of customer screening for adverse information / negative press.

2.4.2 Connected parties

Not all banks had loaded all parties connected to an account into their systems, to which screening was linked (e.g. directors, trustees etc). Therefore, when the periodic screening of the computer systems is conducted, not all parties are screened. This leads to the risk that some banks may have unknown higher risk parties connected to their non-personal accounts, including PEPs. It was however evident that, where this issue still existed, banks were in the process of taking steps to remedy the shortcomings.

3. Action to be taken by the Commission

Further sector specific guidance will be developed and incorporated into the Handbook in respect of the Commission's expectations of banks' independent annual review of higher risk clients, to supplement the high level statements in section 3.4.4 and 3.3.

Consideration as to whether to include the template form in ***appendix 1*** in the Handbook will also be made.

The Commission has already provided this feedback to banks and expects banks to take note of the findings and good practice points explained herein.

Appendix 1 - Suspicious Activity and Evaluation Record Sheet

SAR reference number	

Account Name	
Account Number(s)	
Relationship Manager (where applicable)	
Member of staff reporting	
Date of report	

Description of suspicious transaction or activity including dates (please use separate sheet for further details if needed)	
Risk rating of customer	
Details of any contact with customer to seek explanation and response provided (as	

appropriate)	
Reason for suspicion (please use separate sheet for further details if needed)	
Details of any supporting documentation attached	

MLRO review

Date report received	
Date acknowledgement sent to submitter (attach copy)	
Logged on SAR register	

Is consent required from authorities prior to transaction taking place?	Yes/No
Provide reasons for above	

Is CDD in place? If not what attempts have been made to obtain?	

Internet searches undertaken	
Additional MLRO enquiries undertaken (including dates, specific questions asked, responses received, staff interviewed, documents reviewed)	
Documents attached (e.g. screen prints, copy correspondence)	
Date Investigation complete	
Disclosed to authorities	Yes/No
Reason for decision	

Date disclosure made to authorities (attach copy)	
Request for consent (where appropriate)	
SAR spreadsheet updated with decision	

Outcome

Response received from the FCU	
SAR register updated	
Consent received	Yes/No/N/a
Strategy for customer	
Date complete	
MLRO sign off	