FINANCIAL SUPERVISION COMMISSION

DEPOSIT TAKING (BANKS)

THEMED VISIT PROGRAMME 2012-13:
AML / CFT – SUMMARY FINDINGS, ISSUED SEPTEMBER 2014

CONTENTS

Glossary of terms

AML	Anti-Money Laundering
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
EDD	Enhanced Due Diligence
HNW	High Net Worth
PEP	Politically Exposed Person
SOF	Source of Funds
SOW	Source of Wealth
UHNW	Ultra-High Net Worth

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 banks during 2012-2013 with a focus on anti-money laundering and countering the financing of terrorism ("AML & CFT") processes and controls.

The Commission does not enforce the Money Laundering and Terrorist Financing Code 2013[1] ("Code"); however, compliance with this Code is a "regulatory requirement" under rule 8.2 (c) (iv) & (v) of the Financial Services Rule Book. The responsible officers of a licenceholder 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 licenceholders.

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

- Identification of, and procedures relating to, high risk customers and accounts
- Transaction monitoring
- Ongoing customer / account reviews and screening of existing customers
- Prohibited persons, business activities and countries
- Sanctions / terrorist suspects / PEPs

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 2012 and April 2013.

2. Key findings

2.1 General observations

It was clear from the on-site reviews that progress had been made in improving customer records, the risk assessment of customers, and the monitoring of

[1] This Code came into effect from 1 May 2013 (and was amended with effect from 1 July 2013) and replaced the Proceeds of Crime (Money Laundering) Code 2010 and the Prevention of Terrorist Financing Code 2011.

transactions; and that there was an increased focus on high risk customers and activities.

However, in some cases where the Commission's officers considered that customers appeared to be higher risk, they found inadequate records of customer information and documentary verification, and insufficient further levels of enquiry undertaken. In particular, details of source of wealth ("SOW") were missing from files.

A number of banks had recognised that a significant proportion of their business was higher risk, but had not always allocated sufficient resource to deal with the associated checks and enquiries.

The risk categorisation of customers was sometimes incomplete, and in some cases, where a category had been assigned, it was difficult to see how it had been determined. Without such explanation, it was not clear how the risk was being managed or mitigated.

2.2 Business risk assessment

2.2.1 Overview

Under Paragraph 4 of the Code, every bank must carry out a risk assessment for the purpose of determining CDD measures to be applied. This assessment must be documented, and regularly reviewed and amended so as to keep it up to date.

All banks that were part of the review had undertaken a risk assessment, and this assessment had been reviewed and approved by senior management. In each case a process had been formulated to categorise new business and existing clients, according to the perceived level of AML & CFT risk. However, in some instances, banks had not linked the risk assessment to the wider strategy and objectives of the business (***see 2.2.2 below***).

2.2.2 Statement of risk appetite

The above over-arching assessment of AML & CFT risk should include a statement of a bank's appetite for risk, identifying those markets that may contribute to increased risk, and considering the cost / benefits of these markets.

Where a bank's business strategy targets specific markets or sectors (e.g. e-gaming, UK non-domicile, residents of specific high risk countries, etc.) the potential risks for each sector should be broken down.

Explicit hazards and areas of concern, and the actions that should be taken to protect it against possible involvement in money laundering or the financing of terrorism, should be documented.

2.2.3 Break down of customer book

It is recommended that banks set a maximum number or percentage of high risk customers (compared to overall customer base) that they are willing to deal with, and that they specify the actions that will enforce this maximum. The assessment should state explicitly the types of new business that are unacceptable in any circumstances due to the level of risk (by cumulative scoring or by individual risk factor). Where it is identified that any existing customers fall within this category, the assessment should make it clear what action should be taken.

2.2.4 Focus of resources

The aim of (risk) assessing a business in such a way is to focus resources appropriately, recognising the increased compliance cost of targeting high risk business, the possibility that such business could subsequently result in financial loss, and the potential for a bank's reputation to be brought into disrepute. The assessment should set clear parameters for the identification of higher risk customers and the operation of services to those customers.

Where there are large volumes of higher risk customers, it may be more difficult to distinguish those with particularly high risk attributes and commit an appropriate level of attention to them. It is also possible that a proportion of the business categorised as high risk is debatable, does not warrant the additional burden on a bank's resources, and dilutes the focus on true high risk.

It is recognised that a bank may have an appetite for high risk business but, if so, it must allocate sufficient resources and put in place satisfactory controls to meet the requirements of the Code and Handbook. Alternatively, a bank may decide to exit or reduce its reliance on such business.

2.2.5 Culture of risk

Within the business risk assessment, it should be recognised that it is the responsibility of the board or senior management to ensure that effective checks do take place to identify possible criminal activity, and to ensure that where there is suspicion or knowledge of such, it is managed and reported in accordance with the Code.

2.3 Risk assessment of customers

2.3.1 Overview

Every bank had developed a process to allocate a risk category to individual customers. In some cases, a scoring mechanism was used (a 'risk matrix'), where individual risk factors (such as country of residence, net worth of client, etc.) were allocated a numeric value. If the sum of these values exceeded a predetermined floor limit, the customer was considered to be higher risk. In some cases, each risk factor could generate the higher risk category itself e.g. a customer that was a non-resident trading company might be considered higher risk, regardless of any other factors. Some banks had marked all corporate relationships as higher risk.

Risk assessment processes often included prohibited activities, and applications from customers undertaking such activities would be declined. Other banks did not have blanket prohibitions, but would make a decision based on a number of factors.

Where a PEP was the account holder or related to an account, banks recorded the details in a PEP register and flagged the accounts as such. Most banks subjected PEP relationships to monitoring and review in the same way as high risk customers, although some undertook more in depth checks for any classified as "sensitive". Some banks had different categories of PEP, dependent on factors such as location etc. A higher risk (or more sensitive) PEP category then drove a more frequent review cycle, with an annual review as the minimum for all PEP customers.

The risk category of a customer was normally recorded on a bank's banking systems or customer relationship management systems. However, there were instances where these systems did not include a field to record the risk category, and higher risk customers were listed on a separate spreadsheet.

2.3.2 Best practice

One bank had developed a process to risk assess new business that included additional risk investigation activities. That is, where certain high risk factors were identified (e.g. high risk country of residence), the bank would undertake further checks, rather than automatically categorise the client as high risk. The result of these checks could be that the customer was declined, was categorised as high risk going forward (formal EDD would then be obtained), or the additional information and documentation that was obtained could give the bank sufficient reassurance, so that the specific high risk factor could be discounted, and the customer was then categorised as standard risk going forward.

There were restrictions as to which risk factors could be discounted in this way; some risk factors would always generate a higher risk category or decline. (Note

that this was not considered to be risk mitigation; the risk had actually been discounted. Risk mitigation constitutes the activities that are needed to protect the bank where customers are categorised as high risk.)

2.3.3 Risk ratings

The Handbook sets out risk categories of 'standard risk' and 'higher risk', with guidance in section 4.4.3 listing the types of customers that may be considered to be 'less than standard risk', and section 2.4.5 giving guidance around the types of products and services that constitute a 'lower risk'.

Some banks were using a risk assessment process that generated a 'low / lower risk' category. Instances were seen where a wider range of customers had been assessed as 'low / lower risk' than would be expected to fall into this category when following the Handbook.

In some cases where shortcomings were identified, the risk assessment process had been developed at group or sister company level.

The risk assessment process should follow the Handbook to determine those customers that are less than standard risk. If a risk assessment process ***that does not fully follow the Handbook*** is used, it may be necessary to reposition all or some of the customers assessed as 'lower' risk into the 'standard risk' category.

In some instances, the risk assessment process had generated a rating that was deemed inappropriate by the Commission's officers, i.e. a customer was categorised as lower or standard risk, but the client relationship included significant high risk factors that could not be discounted or mitigated (***see section 2.3.6 below re customer activity, and section 2.3.15 complex structures***). As categorising a customer as higher risk was the prompt to instigate further checks (EDD, focused transaction monitoring, more rigorous transaction checks etc.), it was possible that information had been missed that should have been part of the customer approval process.

It was also discovered that records for customers with multiple accounts had sometimes been categorised with different risk ratings, although they were part of the same relationship. Accounts that are connected should be identified as such and allocated the same risk category, so that ongoing monitoring encompasses a complete picture of the risk position.

2.3.4 Records of customer risk rating / score / category

Although every bank was risk rating new customers, and had commenced the risk assessment of all existing customers, instances were seen where there was no

record of a customer's risk rating or evidence that any assessment of risk had taken place.

There were also cases where the risk rating that had been recorded against a customer did not correspond with the rating that a bank's risk assessment processes (current or historic) should have generated. If a manual override to the rating had taken place, the rationale for this was not always documented.

In some instances, a risk category had been assigned to a customer, but there was no record of the factors that had been used in the assessment, or details of what additional enquiries had been made. Where the factors raising risk concerns were not identified, it was not possible to gauge how a bank's controls could take effect, or what considerations had been taken into account by the person signing off on a new account or ongoing monitoring. Where a checklist is used, it should be fully completed. Where any non-standard information has been provided, or where standard information has not been available but the risk category has been approved, the rationale should be recorded.

Where the risk category is not recorded on the banking system, but on a separate spreadsheet, the risk category records should be clear. It should be possible to differentiate the high risk customer records for monitoring and control purposes.

Where an override of the risk assessment process had taken place, if the Compliance function has not been involved in the approval process, it should be possible for Compliance to sample check such override cases to ensure that they fit within a bank's parameters. It may be helpful if such overrides are flagged on a banks' records for the purpose of identifying these cases.

2.3.5 Existing customers

There were instances where different risk assessment processes had been applied to the existing client base, from those that were applied to new business. Each new business case was risk assessed individually, but the back-book had been assessed in bulk using a simpler formula or approach.

The main reason for doing this was that the banks' electronic records did not catalogue all of the factors that would be applied by the current risk assessment process (e.g. it was rare for the expected turnover or type of business activity to be electronically recorded), and the large volumes of customers would make it difficult to manually assess the back-book in a timely manner. These existing customers had been assigned risk categories based on the information that could be extracted electronically.

However, existing clients were subject to manual re-assessment on a trigger event basis, and the re-assessment would be performed using the new business process. This situation is not considered ideal, as factors such as sensitive business activities may not be identified unless a trigger event takes place.

Where there were significant differences between the process to assess new business and that to assess existing business, there were instances where the Commission requested banks to undertake an exercise to re-assess all existing customers using the new process. Where the current risk assessment process had significant omissions, the Commission requested that the back book was re-assessed using a revised, improved, risk assessment process. In cases where there were very large volumes of customers, and specific risk factor information could not be extracted electronically (but the key high risk factors had been identified, and there was robust transaction monitoring processes in place), the detailed re-assessment could be done on a trigger event basis.

2.3.6 Nature of customers' business / activity

Some banks' current risk assessment processes did not encompass all of the factors specified in section 2.4 of the Handbook, e.g. 2.4.6 the risk inherent in the nature of activity of the account holder.

Where a customer's activity was used as a consideration, in some cases a bank's policy did not state explicitly how each type of activity should contribute to the categorisation of the customer. Banks should obtain information regarding the nature of a customer's business activity, and the risk assessment process should contain a list of customer activities that should be considered to be higher risk or prohibited.

In some banks the consideration of customer activity as a risk factor was restricted to non-personal accounts. Cases were seen where the employment of a personal customer in the arms trade had not been recognised as a high risk factor. Insufficient levels of enquiry were seen when a customer stated that they were employed as a 'consultant' in an unspecified profession. Activity risk should be applied to both personal and non-personal customers.

Some cases were seen where a (non-resident) personal customer had stated that they were employed by a company, but it was evident that the company was not a separate entity to the individual. E.g. the customer and his family were the entire owners of the company, or there was not actually any legal entity that would be recognised as such, and the customer was working for himself. There were also instances of declared self-employment. All such cases should have additional focus on the source of funds and source of wealth, and the nature of the customer's activities.

For example, a case was seen of a customer who claimed to be employed by a petro-chemical company in a high risk country. However, they appeared to be the sole owner of a company that traded in oil in Nigeria, that may or may not have been legally incorporated (as it was treated as a personal account, this had not been established). Acceptance of such business (there are major problems with illegal oil trading in Nigeria) without fully understanding the customer's activities and undertaking thorough EDD exposes a bank to a significant risk that they may be handling the proceeds of crime. This example was not unique; many similar cases relating to the circumstances of personal customers' employment were noted.

2.3.7 Definitions of sensitive activities

The range of activities categorised as sensitive did not always include some industries that can typically be regarded as having the highest level of exposure to risk of engaging in bribery including, for example: Aerospace & Defence; Electronic & Electrical Equipment; Industrial Engineering; Mobile Telecommunications; Software & Computer Services; Technology Hardware & Equipment; Drugs and Pharmaceuticals. A broader range of activities that are regarded as higher risk is published by the Industry Classification Benchmark.

There should not be any option to categorise an activity as 'miscellaneous'. Where an activity has not previously been risk categorised, there should be a provision in a bank's procedures for management to investigate the level of risk and assign a category to the activity. For high volume banks, this may include amendment of the procedures for consistency in future cases. Alternatively, a documented rationale for the activity's risk category should be appended to the customer records.

2.3.8 Scoring mechanisms

Where a scoring mechanism is used, all of the factors suggested in the Handbook should be included, and it should be possible to override the score if the mechanism is not sensitive to all details, e.g. a matrix may give a low score to a company that is resident in a standard risk country, but may not have leeway to identify that it is actually operating in / trading with a high risk country, and cannot then generate the risk score that should apply for that country. Where the ultimate beneficial owner (or other connected party to an account) is categorised as a high risk individual, the scoring mechanism should take this into consideration, or there should be a manual override to do so.

2.3.9 High risk countries

All banks had assigned risk categories against a list of countries for the purpose of assessing a customer's country of residence. In most cases, the country of

operation, nationality, source of funds, etc. were also assessed against the high risk country list. The risk assessment process should state clearly which elements of a customer profile should be considered against the list of countries.

Sometimes, the high risk country list was issued by a bank's group compliance function, whilst in other instances, the local bank had determined the list. It was not always clear how the risk categories had been decided, and whether Appendix G of the Handbook had been taken into consideration. There should be a documented methodology to show how country risk categories have been assigned and a process of regular review.

Where a customer is resident in a country that has not been individually categorised by a bank, there should be procedures in place to manually assign a risk level to that country. For consistency, consideration should be given as to whether this country should be formally risk categorised going forward.

In some instances the presence of a group entity in a country was taken into consideration, and the risk rating of that country was reduced. The Commission does not believe this is appropriate. However, where a new business applicant is an existing face-to-face customer of the foreign entity, and is being introduced by this part of the group, this may be considered to be a mitigating factor.

Where a customer's nationality is considered as a factor in the risk assessment, if dual nationality is identified, the highest risk (country) factor should be used.

Instances were seen where countries listed in Appendix G of the Handbook had not been included in the high risk country list. In such cases, banks should document why these countries are not considered to be higher risk.

2.3.10 Changes to high risk countries

It is recommended that consideration is given to Transparency International's Corruption Perceptions Index ("the Index") to help identify high risk countries. The Index is updated on an annual basis, and countries may move in and out of the higher risk range. Although the Commission would expect a bank's high risk country list to be updated on a regular basis, it does not expect banks to automatically remediate an individual customer risk assessment due to such a movement. The need for remediation would depend on the reason for the change in the Index score and the nature of a customer's connection to the country.

More urgent remediation of a risk category may be needed for customers when there is a significant event in a linked country, e.g. additional focus may be required for customers that are resident in countries where political uprisings such as the Arab Spring have taken place.

If the Index is used as a stand-alone tool to assess some factors (e.g. the location of a sensitive activity), for consistency, the same tool should be used in the formation of the high risk country list for other factors, including country of residence.

2.3.11 Products and services

Section 11 of the Code specifies matters that may pose a higher risk, including: (d) the provision of banking services for higher risk accounts or high net worth individuals. The Handbook, section 2.4.5, provides guidance to products and services that may be more vulnerable to abuse. Where banks differentiate risk according to a customer's use of products and services, there should be a clear rationale within the risk assessment. E.g. a customer holding a long term fixed term deposit account only, *may* have less associated risk than a customer operating a transactional or instant access account.

2.3.12 Pooled accounts

Bank accounts holding pooled funds may be operated by local advocates, lawyers, accountants, and stockbrokers, in order to manage funds on behalf of their clients (see section 4.12 of the Handbook). As long as the applicant for business (advocate, lawyer, accountant or stockbroker) has been assessed as low risk, banks are not obliged to obtain CDD on the underlying clients. However, banks must make efforts to ensure that the funds of higher risk individuals or entities are not included in the pooled accounts.

It was not always clear that this had been checked.

Banks should obtain confirmation from the operator (e.g. the advocate) that there are no funds for higher risk individuals or entities contained in the existing pool, and that none will be put in the pool. If the definition of high risk for this purpose is that used by the operator of the account, the bank must ensure that it is satisfied with that definition. The records / information pertaining to each pooled account should include this correspondence.

The Commission's AML Unit has since undertaken further research into pooled accounts and also how certain types of intermediary relationships should be treated for AML / CFT purposes. This includes clarifying how banks should treat CSP general client accounts which are not specifically referred to in section 4.12 of the Handbook. Any changes that may be made in this area will also require amendments to the Code and in August 2014 a consultation document was issued by The Department of Home Affairs.

2.3.13 HNW / UHNW

Where the net worth of a customer is used as a factor in the risk assessment, the floor limits or definition of High Net Worth ("HNW") and / or Ultra-High Net Worth ("UNHW") should be clearly stated.

2.3.14 Bearer shares

Where a bank account is operated by a company that has bearer shares in issue, the Commission expects the bank to immobilise the bearer shares, normally by taking them into safe custody. (See section 4.7.3.1 of the Handbook and paragraph 11(2)(c) of the Code.)

Instances were seen where corporate customers of banks had issued, or had the facility to issue bearer shares, but no further enquiry (on immobilisation) had been made. However, beneficial ownership was fully established and evidenced. The risk assessment of a company should include full investigation of the ownership structure, including existing bearer shares and any circumstances where bearer shares may become available. Banks might consider checking whether this is permitted by the Memorandum and Articles of the company.

2.3.15 Trusts and complex structures

Instances were seen of complex structures including trusts and corporate shareholders, and trusts where a dummy settlor had been accepted[2], or where the only identified beneficiaries were charities (blind trusts). Although in most cases information regarding the Ultimate Beneficial Owner had been obtained and verified, the Commission does not believe that such structures can be treated as standard (or low) risk.

Such files would benefit from a structure chart or file note, with a further explanation of the background and rationale for account, details of connected parties, and full reasoning for the CDD / EDD undertaken.

Trusts where additional beneficiaries can be added should be closely monitored to ensure that payments are not made without full identification and verification of the identity of the recipient (***also see section 2.6.8***).

[2] In the matter of a dummy settlor, cases were only for older existing customers and there was no evidence of these structures being used for new clients.

2.3.16 Eligible introduced accounts

Where a customer is categorised as higher risk by a bank, the changes to the Code in 2010 removed the concession that allowed the bank to rely on an Eligible Introducer Certificate ("EIC") in place of full CDD documentation. However, a number of banks had continued to rely on EICs for higher risk customers, or had not remediated existing higher risk customer records.

Following the visit programme and consultation with banks, the Commission amended the guidance in the Handbook. It remains the case that the use of an EIC cannot replace full CDD / EDD for higher risk customers, but banks may accept copies of CDD / EDD held by Eligible Introducers in certain circumstances - see section 4.10.4 of the Handbook. Remediation of existing records to the new standards should be undertaken as soon as possible, and concluded no later than the completion date of the next customer review.

Where banks have agreed Terms of Business with introducers, to ensure clarity and consistency, they should ensure that it is clear within the agreement that where a customer or account is classified as higher risk by the bank, the eligible introducer's concession does not apply, full KYC must be supplied, and EDD is required.

2.3.17 Approval of business

Some banks did not have a specific process for the approval / sign off of higher risk customers, to ensure that all of the risks to the business had been considered. All banks had procedures for the approval of PEP relationships.

All banks maintained some form of a declined business register, however, in some cases there was no electronic register, which would have enabled a search to take place. Some paper records did not include the reason for declining the application.

2.4 Customer Due Diligence

2.4.1 Identity information and verification

Some banks were unable to confirm that they held full CDD for all existing customers, due to the volume and historic nature of their customer base. These banks were requested to put remediation programmes into place. In such cases, banks generated an electronic report from the computer systems to identify the customers that were considered to be higher risk (using such flags as were available on the systems) and these customers' records were retrieved from filing systems, reviewed, and remediated where necessary. Non-high risk customers were required to be rectified on a trigger event basis (***see section 2.8 below re trigger events***).

Where a corporate account is categorised as higher risk, it is a requirement that *all* parties linked to the entity are identified and that identity is verified (see section 4.7.3 of the Handbook). Some banks had not recognised this, and limited CDD was obtained on some parties. Where it is discovered during the customer review that *all* parties have not supplied full CDD, the bank's records should be rectified (***see section 2.7 below re customer reviews***).

In some cases it was difficult to locate full identification information for parties to non-personal accounts, e.g. company directors, signatories, beneficiaries of trusts. Banks were requested to review their application forms to ensure that they captured all of the information required, see sections 4.7.3 and 4.4.1 of the Handbook.

2.4.2 Certification

Certification did not always meet the standard specified by the Handbook, e.g. the person certifying the document did not hold a position as shown in the recommended list of suitable certifiers, or the certifier had not provided their contact details. If non-standard certification is accepted, there should be a documented rationale and sign off for the exception.

Copies of copied identification documents were sometimes seen for direct customers of the bank. Copies of copies are only acceptable where there is an Eligible Introducer Certificate or Terms of Business in place, and then only in certain circumstances - see section 4.10.4 of the Handbook.

2.4.3 Acceptable Applicants

In some cases banks had classified corporate entities as higher risk, but had also used the "Acceptable Applicant" concession. This concession cannot be used for higher risk entities, see section 4.9 of the Handbook and paragraph 11 (1A) of the Code.

2.4.4 Relationship information

Some banks did not collect full relationship information at account take on, e.g. expected account turnover for transactional accounts, purpose and intended nature of relationship etc. (see section 3.3 of the Handbook). Without this information, a bank cannot compare actual transactions against those expected, to help identify unusual or suspicious activity.

Some banks, however, did not have fields in their computer systems to record this information, so even where the information had been obtained, it could not be used for automated transaction monitoring purposes.

2.4.5 Background financial information for corporate entities

There were cases where banks had not requested or been supplied with a copy of the annual financial statements for (higher risk) trading entities. Although it is not a regulatory requirement to obtain these, the availability and content of financial statements should be considered as factors in the risk assessment of the customer at account take on and during customer reviews, and as an aspect of EDD (for higher risk accounts) as appropriate.

2.4.6 Eligible introducers

Where Terms of Business are in place, these must be kept up to date, ensuring that any changes to an introducer's regulated status are discerned, and maintained in line with any changes in the Code and Handbook. Where a bank undertakes a risk assessment of introducers, this must also be documented and kept up to date (***see also section 2.3.16 re eligibly introduced accounts***).

2.4.7 PEPs

Where PEPs were linked to an account, but were not the primary customer, there were instances where insufficient enquiry had been made, or CDD/EDD documentation could not be found. Where a PEP is a director, signatory, or minor party to a client, full CDD and EDD must be obtained.

2.5 Enhanced Customer Due Diligence ("EDD")

2.5.1 Defining EDD

A number of banks had not defined EDD in procedures, or described how to distinguish CDD from EDD. Procedures did not include what would prompt a request for EDD, the methods by which EDD should be obtained, or the extent to which enquiries should be made and verified.

It was difficult to identify from some customer files which documents and information were standard CDD, and which were considered to be EDD. EDD should be formally documented as such, including an explanation as to how the EDD supports a bank's understanding of the customer / business e.g. print outs of internet searches that verify a certifier's details should be dated and annotated to explain what it is that they are confirming.

In some cases, where funds are received from third parties, banks should consider amending their procedures to include a request for EDD on the third parties, e.g. when the third party is a trading company resident in a high risk country and / or

undertaking a high risk activity it may be advisable to obtain reassurance that the funds are from a legitimate source by requesting copies of contracts, identity documents etc.

2.5.2 EDD for legal persons

For standard risk corporate entities and trusts etc., banks must obtain identification information and verification documents for at least two signatories/directors etc. Obtaining CDD on *all* persons related to a company (as required by the Handbook for higher risk customers) does broaden the scope of enquiry beyond the CDD requirements for standard risk customers, however, this in itself does not comprise comprehensive EDD.

2.5.3 Source of Wealth ("SOW")

The Code requires that SOW is established for higher risk customers as part of EDD.

In some cases, SOW information and additional supporting documentation (as appropriate) had not been obtained for higher risk customers (especially those with older relationships). SOW should be obtained as part of the account opening process for higher risk applicants, retained on the customer records, checked during the customer review, and remediated where necessary.

Where a person's wealth was derived from their own business, it was not always clear that an appropriate level of enquiry had taken place to confirm this (***see also section 2.3.6 re risk associated with customers' business***).

Where SOW information and verification had been obtained, there was not always a file note to explain why it was acceptable, where this was not obvious. Procedures should include explicit requirements to explain the SOW and state how this has been corroborated.

2.5.4 Lack of EDD

In a number of cases where a customer had been assessed as higher risk, there was no evidence that any of the EDD requirements had been considered or obtained. This included cases where the customer had been subject to a formal ongoing business review. The review should include an assessment of EDD and remediation, as required (***see also section 2.7 re customer reviews***).

2.5.5 Outstanding EDD

Where a customer had been requested to provide information as part of EDD, some banks did not have a diary system to follow up on outstanding requests, did not have the facility to flag accounts or a policy regarding the activity that could be permitted on the account while the request was pending. Further, there was not a policy to define what action should be taken if the request was not complied with, within a reasonable time limit.

2.6 Transaction monitoring

2.6.1 Overview

All banks undertook some form of post-event transaction monitoring. At a minimum, an exception report was produced to identify individual transactions that exceeded pre-determined floor limits. Such transactions were then manually checked against the banks' records to ensure that the Source of Funds ("SOF") and nature of activity was in accordance with expectations. A bank's expectations should be driven by the information obtained at account take on, and updated on a regular basis, in line with section 3.3 of the Handbook: Collecting Relationship Information.

In most instances, the checks were undertaken independently by a member of staff who was not party to the keying, checking and authorisation of the transactions.

Where a bank's records did not provide an adequate explanation, i.e. the transaction was unusual, further information and / or documentation was requested. Where these checks resulted in a transaction being identified as suspicious, a Suspicious Transaction Report was submitted to the MLRO. This process met the requirements of part (c) of section 5.1 of the Handbook, possible characteristics to monitor: the amount of any transactions, paying particular attention to particularly large transactions.

Most banks were aware of the need to have live transaction screening systems in place for sanctions purposes.

2.6.2 Source of Funds and relationship information

Where banks did not hold sufficient information regarding the customer activity under review, or the source of funds of a deposit, or documentary verification was thought necessary, banks normally reverted to the customer to request this. However, some banks did not have a diary system to follow up on outstanding requests, did not have the facility to flag accounts, or a policy regarding the activity that could be permitted on the account while the request was pending. Further, there was not always a

policy to define what action should be taken if the request was not complied with within a reasonable time limit. The same issue arose with requests for CDD/EDD arising from account applications, and customer reviews, ***see sections 2.7.10 and 2.5.5***.

Banks should have procedures in place to define the information or documents that may be considered satisfactory according to the various circumstances that may occur. There should also be procedures for following up and closing off such requests. Where a checklist is used, there should be procedures to define how and when it is used. Procedures should also state who has authority to approve or reject transactions, and what decision process is used.

2.6.3 Turnover

Not all banks had an automated facility to compare the actual turnover (by value and volume) of a transactional account to the turnover that the customer had predicted. Such a facility would assist banks to identify potential unusual activity. For long-standing customers, it is recommended that actual turnover is compared against customers' historic, 'normal' activity. If an automated facility compares activity against out of date records, it may miss significant events, or generate an unnecessarily large number of exceptions, and dilute the focus of the checks. See section 5.1 of the Handbook, possible characteristics to monitor: (f) the customer's normal activity or turnover.

2.6.4 Patterns of activity

Not all banks had an automated facility to identify aggregate amounts within a time period, where an individual transaction may not appear unusual, but the combined amounts could show an unusual pattern of activity that should be investigated further. Such banks were reliant on manual checks by operations staff, which was not always possible given the large numbers of clients.

Where an automated system is used, if this has been obtained from an external supplier or group entity, the bank should be aware of the specific rules within the system, and have the authority to request changes to the parameters. The rules should be documented to demonstrate how all account entries are considered. Full testing should be undertaken to ensure that the automated system picks up the correct transactions in a consistent manner. See section 5.1 of the Handbook, possible characteristics to monitor: (b) the frequency and nature of a series or pattern of transactions.

2.6.5 Transactions from / to high risk countries

Most banks did not have the facility to automatically identify receipts originating from high risk countries, and were unable to target such transactions for monitoring purposes. (It was also noted that some banks did not have additional pre-event checks in place for payments to high risk countries). See section 5.1 of the Handbook, possible characteristics to monitor: (d) the geographical origin / destination of a payment or receipt. It should be noted this is separate from the issue of payments to / from sanctioned countries or individuals where facilities (sanctions screening) were in place.

2.6.6 Activity on higher risk accounts

For higher risk accounts, banks generally undertook post event monitoring that included *all* activity that had taken place.

2.6.7 Internet banking

Most banks' internet banking offerings did not include the facility for customers to make direct payments without the intervention of staff. However, if fully automated internet banking is available to customers, floor limits should be in place so that any large transactions are halted to be reviewed by bank staff prior to release into the system. If possible, this should also apply to all payments being sent to high risk countries.

If internet banking is provided to customers that have been categorised as high risk or PEPs, consideration should be given to interrupting all internet banking payment instructions to allow manual checks to take place.

Where online banking is offered to a trust or foundation, the bank must ensure that full CDD is held for the beneficiaries before any payment is made to them. Where the account is operated by an introducer, it still remains the responsibility of the bank to ensure that CDD is held.

2.6.8 Trusts and foundations

There were cases identified where distributions had been made to the beneficiaries of trusts and foundations, where banks did not hold full CDD on the beneficiary. It was noted that a bank may not be easily able to distinguish a payment to a beneficiary from a payment made as an investment or expense incurred by the trust. In some instances, the beneficiary was a charity, and obtaining full corporate and personal CDD would be onerous (taking into account the nature of the charity and its location).

Basic plausibility checks may be sufficient where the recipient of a payment is not thought to be a beneficiary. However, procedures must be in place to undertake additional identity and verification checks when distribution payments are being made to beneficiaries or less well known organisations, as required by paragraph 6 (4) of the Code. This also extends to cases where loans or payments are made arising as a result of powers of revocation being exercised in respect of a trust, as described in section 4.6.2 of the Handbook. Although this latter point was not identified from visits to banks, the Commission has observed failings in the trust service sector whereby the identity of (higher risk) beneficiaries was not verified because such loans or payments were not treated as distributions for the purpose of AML / CFT.

2.6.9 Wire transfers

All banks confirmed that they included full details of the remitter in outgoing wire transfers. Most banks undertook sample checks on incoming wire transfers, and would request any missing information. Where the information was not provided, the payment was returned. Banks did not always have any automated facilities to check all incoming wire transfers for remitters' details.

2.6.10 Evidence of monitoring

Insufficient narrative was sometimes provided within the review records, making it difficult to see what factors had been considered, and how it had been determined that a transaction was in line with a customer's normal activity. Some transaction monitoring reports reviewed were not dated by either the reviewer or the Compliance oversight process, so Commission Officers could not determine whether the reviews were taking place on a timely basis. Reviews should be prioritised, completed in a timely manner and fully documented, including the date of review.

Where checklists are used for pre-event checks or post-event monitoring, they should be fully completed, especially where the checklist documents the reason for the transaction, and the rationale for believing that this is within the range of normal activity for that customer.

2.7 Ongoing customer reviews

2.7.1 Overview

Section 5.1 of the Handbook details the required frequency of customer reviews, based on the risk category of the customer.[3]

[3] Section 5.1.1 of the Handbook was amended in May 2013 to require all licenceholders' customers to be reviewed every 3 years as a minimum. However, the sector specific guidance for banks in section 9.2.4 was also

Most banks undertook some form of over-arching regular review on higher risk customers.

Section 5.1.1 of the Handbook includes the requirements for higher risk customers: that the review should take place on an annual basis as a minimum, that the process should be independent; that it should consider the accuracy and completeness of CDD records held by the bank; and that it should review the activity and transactions undertaken in the period against expectations.

The Commission considers that banks should include within the review any other information that may be easily available, such as media comments, and changes to a customer's status e.g. changes in employment, income, geographic location. Even if CDD records are comprehensive and up to date and no financial activity has taken place on the customer's account (e.g. the product is a fixed deposit), the level of risk associated with a customer may have changed. See section 5.1.1 of the Handbook, part (b): '…changes in circumstances…'

Some banks undertook higher risk customer reviews on a more frequent basis, where specific risk factors were causing concern.

As part of the customer review, banks undertook a re-assessment of the assigned risk category. Where it appeared to the reviewer that a customer could be down-graded to a lower risk category (e.g. a customer had moved back to the UK), this was subject to management sign-off. Where a customer's risk category was to be increased (e.g. it was discovered that the customer was working or trading in a high risk country), in most instances the approval of the board or senior management was required to continue to operate accounts for the customer.

Procedures should be in place to ensure that a robust review is performed, significant transactions and changes are identified and reviewed, and the outcome recorded.

2.7.2 Procedures

Some banks did not have formal procedures for performing ongoing reviews. Further, procedures and / or checklists did not always distinguish between personal and corporate relationships, or provide enough guidance to staff.

amended to include a dispensation for banks (due to the volume of clients) allowing them to review non-high risk customers on a trigger event basis.

2.7.3 Execution of reviews

There were instances where no formal customer reviews had taken place since account opening. This was considered to be a breach of the Code.

In some cases, banks had been unable to record the risk category on their mainframe systems, or other database, and therefore could not accurately identify the customers that should have been subject to formal ongoing reviews. In these circumstances, banks used the only fields on the system that were available to record information, but these fields did not match all parameters that had been used for the initial assessment. As a result, some customers that had been identified as posing a higher risk of money laundering and financing of terrorism at account take on had not been subject to a regular review.

Finally, some banks had a larger number of higher risk customers to review than their resources could cope with but were reviewing how to address such issues (***see the comments in section 2.2.4 regarding the Business Risk Assessment***).

2.7.4 Independence of reviews

In some cases, banks did not have an independent review process. If a review is undertaken solely by a customer's relationship manager, there is a danger that there may not be sufficient focus on the potential AML and CFT risks of the customer.

2.7.5 Frequency of reviews

Some banks did not undertake a review of higher risk customers at least annually. To comply with the Handbook, a review should take place before the anniversary of the last review, *not* after. The date that a review takes place should always be recorded, and used to establish when the next review is due. Banks should also record the date when any outstanding actions are due, and this should be monitored to ensure that they are completed in a timely manner. It is not anticipated that any actions should still be outstanding when the next review falls due.

2.7.6 Scope of reviews

The Commission's sample review of customer files found cases where insufficient CDD and EDD had been obtained initially, to show a full and complete understanding of a customer. This was not, in all cases, rectified at the regular review. A lack of Source of Wealth ("SOW") information was widespread (especially for clients that had been on the books for a longer time), and cases were also seen where the Commission's officers would have expected to find documentary

verification of SOW. Where the bank had intimated that they had reviewed and remediated the customer files, this was of particular concern.

There were also instances where the scope of the review was not sufficiently comprehensive, i.e. the review did not encompass customers' business activity, transaction history, changes in circumstances of the customer, and other connected relationships.

2.7.7 Out of date CDD

If the certified copy of an original valid passport is no longer in date at the customer review stage, it is not an automatic requirement for banks to obtain an updated copy passport. However, it was noted that some banks do request this as part of EDD for higher risk customers, or as part of the general CDD update process. Where it is a bank's policy to request replacements for out of date CDD documents, this should be undertaken consistently.

2.7.8 CDD that does not meet current standards

Where CDD is held, but does not meet current standards (e.g. the certification is incorrectly worded) consideration should be given to addressing any discrepancies. For non-high risk customers, it may be concluded that the CDD remains adequate for the purpose, and an exception documented and signed off. Some banks had not recorded any evaluation of such CDD.

2.7.9 Action following review

In some instances a review had identified that the CDD records were inadequate, but no further action had taken place. Accounts had not been flagged or frozen pending remediation, and no contact had been made with the customer. This was considered to be a breach of the Code.

2.7.10 Requests for CDD

Where a request was sent to a customer for updated CDD / EDD, some banks did not have a diary system to follow up on outstanding requests, did not have the facility to flag accounts or a policy regarding the activity that could be permitted on the account while the request was pending. Further, there was not a policy to define what action should be taken if the request was not complied with within a reasonable time limit (the same issue arose with SOF requests, ***see section 2.6.2, transaction monitoring - SOF***).

If customers fail to comply with requests, procedures should be in place to restrict activity on accounts.

Banks should have a policy in place regarding the continuation of accounts that have been blocked pending receipt of CDD / EDD.

2.7.11 Records of reviews

Where CDD had been reviewed (in a scheduled review or due to a trigger event), there were instances where it was not possible to see what had been included in the review, what deficiencies had been identified, and what additional enquiries had been made. A checklist or a formal file note should be produced and retained with the CDD records.

There were cases where there was insufficient narrative to demonstrate how significant transactions in the period fitted with a customer's profile.

Where an exception to current CDD standards has been agreed, the rationale and approval should be documented and retained with the CDD records.

2.7.12 Management oversight

Some banks did not have a formal process for approval / sign off of a change to the risk category of a customer, to ensure that all of the risks had been considered for the continuation of the relationship or to flag the account for future monitoring.

The status of reviews should be monitored independently to ensure that they are being undertaken on time and there are no backlogs. Sufficient resource should be made available for reviews to be undertaken in the right way and to allow any necessary remediation to be completed in a timely manner.

2.8 Ongoing reviews - trigger events

2.8.1 Overview

Most banks had procedures to define a 'trigger event', when activity on a customer's account, the take up of additional services, or changes to a customer's profile occurred. When a trigger event was identified, the customer's CDD records were subject to review, risk assessed and updated as appropriate. For standard and lower risk customers, however, instances were seen of events that fitted a bank's definition of a trigger event, but had not been identified as such, and no review had taken place.

2.8.2 Large transactions

It is recommended that large outward payments should be considered as trigger events, where they exceed a pre-determined threshold (for customer segments). This can be particularly important where it is known that a tranche of customers may not have been assigned a risk rating or the risk assessment process for existing customers was limited (banks generally undertook more thorough checks on transactions for higher risk customers).

2.9 Customer screening

2.9.1 Screening of new customers

All banks undertook the screening of new customers against some form of 'blacklist' databases. The screening process was used to attempt to discover if the applicant was a known high risk individual or entity and the 'blacklists' included some or all of the following: PEPs, subject to sanctions, criminals, terrorists, adverse media etc. There was a manual process in each case to investigate the match and either discount it or take the appropriate action.

In some cases, it was not clear that all parties to an application had been screened.

2.9.2 Screening of existing customers

A number of banks had an automated screening process for their entire banking / customer information systems on a regular basis e.g. daily (overnight), monthly, etc. Where a customer review was performed (e.g. at a trigger event or scheduled higher risk review), in general banks would also undertake the manual screening of the customer against blacklists at the same time.

The level of automated screening varied, with some checks run against the full scope of the 'blacklist', and others against a selective range of factors, e.g. just PEPs and sanctions.

Where banks did not have automated screening processes, or where screening was not undertaken against all available factors, there is a risk that the bank may not have full information regarding its customers. This is especially pertinent for customers currently classified as standard risk (including more historic customers) which, if adverse information was known, may now pose a higher risk and would therefore be subject to more intense review and monitoring processes. Where they were not already in place, banks were requested to consider installing full automated customer screening systems.

For a bank to be able to electronically screen all parties to an account (e.g. directors, shareholders, beneficiaries, settlor, signatories etc. as well as the named account holder), it was necessary for that information to be recorded on the systems. In some cases, these records had not been fully completed, and therefore these parties could not be adequately screened. All such banks were requested to add the missing data to an electronic system for screening purposes.

2.9.3 Screening procedures

In some cases where screening had taken place, and a potential match had been identified, it was not clear whether any investigation had taken place and what factors had determined that it was not a match. There were also cases where the record had not been annotated to show that the match had been discounted. Some banks did not have formally documented procedures for undertaking customer screening.

Procedures should be put in place to describe how to undertake the screening, how to investigate potential matches, what records to keep, and what action to take where the hit is believed to be a true match.

2.9.4 Sanctions

Some banks were reliant on the providers of their payment systems to screen payments against sanction lists. Where this is the case, a bank should ascertain what screening the provider undertakes for any payments it processes and ensure that this is satisfactory. Although the process for screening payments can be "outsourced", the ultimate responsibility remains with the bank.

When Isle of Man Customs and Excise issues updated notices, if there is no automated screening of the existing customer base (***see 2.9.2 above***), banks undertake a manual search of their systems to check for any true matches. When parties to an account had not been recorded on the computer systems, banks were reliant on staff knowledge and the checks undertaken as part of file reviews to ascertain whether there were any matches. This was not considered to be a robust process.

2.10 Record keeping

Where checklists were used for account opening, periodic account reviews, trigger events, and risk assessments, (and to summarise details for senior management consideration and approval), they were not always fully completed.

There were some instances where an account review, or transaction monitoring, had taken place, but the bank was unable to provide any evidence as to what had been reviewed or what action had subsequently occurred.

2.11 Compliance monitoring

2.11.1 Transactions

The Compliance monitoring programme should include random manual examinations of a day's work to ensure that all entries over a certain limit are captured, and ensure that these have been properly investigated.

2.11.2 Customer reviews

Scheduled customer reviews and trigger event reviews should be included in the Compliance monitoring programme to ensure that they are carried out in accordance with internal procedures, i.e. they are accurate, comprehensive and timely, and any actions have been completed.

The level, intensity and frequency of monitoring of higher risk reviews should ensure that expected standards are maintained. Where issues are identified, feedback should be provided to the staff undertaking the reviews.

3. Action taken by the Commission

Visit reports were issued to participating banks, and included breaches and best practice points, relating to the above sections. Timeframes for remedial action were agreed in all cases, sometimes for periods of 6 to 12 months, and a few further bespoke visits were undertaken to monitor progress during 2013 / 2014.

There were files reviewed where there was not sufficient information on the file to determine whether the use of the bank's services was legitimate or suspicious. In these cases, a schedule of queries was provided to the bank, so that they could check whether they did actually hold information, or could pursue the enquiry.

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

4. Our priorities for 2014 / 2015

AML / CFT will continue to be a key focus of the banking supervision team's visit process on a rolling basis and forms part of the 2014 / 2015 plan. The banking supervision team is also working with the Commission's AML Unit and the Isle of

Man Bankers' Association on any AML / CFT related matters that arise, including amendments to the Handbook and Code.