Chapter 16

How small banks manage money laundering and sanctions risk – update (2014)

16.3 Themes

Management information (MI)

16.3.1 Useful MI provides senior management with the information they need to ensure that the firm effectively manages the money laundering and sanctions risks to which it is exposed. MI should be provided regularly, including as part of the MLRO report, and ad hoc, as risk dictates.

Examples of useful MI include:

- an overview of the money laundering and sanctions risks to which the bank is exposed, including information about emerging risks and any changes to the bank's risk assessment
- an overview of the systems and controls to mitigate those risks, including information about the effectiveness of these systems and controls and any changes to the bank's control environment
- legal and regulatory developments and the impact these have on the bank's approach
- relevant information about individual business relationships, for example:
  - the number and nature of new accounts opened, in particular where these are high risk
  - the number and nature of accounts closed, in particular where these have been closed for financial crime reasons
  - the number of dormant accounts and re-activated dormant accounts, and
  - the number of transaction monitoring alerts and suspicious activity reports, including where the processing of these has fallen outside of agreed service level agreements.

16

Governance structures

16.3.2 Banks should have a governance structure that is appropriate to the size and nature of their business.

To be effective, a governance structure should enable the firm to:

- clearly allocate responsibilities for financial crime issues
- establish clear reporting lines and escalation paths

•identify and manage conflicts of interest, in particular where staff hold several functions cumulatively, and

•record and retain key decisions relating to the management of money laundering and sanctions risks, including, where appropriate, decisions resulting from informal conversations.

Culture and tone from the top

16.3.3 An effective AML and sanctions control framework depends on senior management setting and enforcing a clear level of risk appetite, and embedding a culture of compliance where financial crime is not acceptable.

Examples of good practice include:

•senior management taking leadership on AML and sanctions issues, for example through everyday decision-making and staff communications

•clearly articulating and enforcing the bank's risk appetite – this includes rejecting individual business relationships where the bank is not satisfied that it can manage the risk effectively

•allocating sufficient resources to the bank's compliance function

•ensuring that the bank's culture enables it to comply with the UK's legal and regulatory AML framework, and

•considering whether incentives reward unacceptable risk-taking or compliance breaches and, if they do, removing them.

Risk assessment

16.3.4 Banks must identify and assess the money laundering risk to which they are exposed. This will help them understand which parts of their business are most vulnerable to money laundering and which parts they should prioritise in their fight against financial crime. It will also help banks decide on the appropriate level of CDD and monitoring for individual business relationships.

A business-wide risk assessment:

•must be comprehensive, meaning that it should consider a wide range of factors, including the risk associated with the bank's customers, products, and services – it is not normally enough to consider just one factor

•should draw on a wide range of relevant information – it is not normally enough to consider just one source, and

•must be proportionate to the nature, scale and complexity of the bank's activities.

Banks should build on their business-wide risk assessment to determine the level of CDD they should apply to individual business relationships or occasional transactions. CDD will help banks refine their assessment of risk associated with individual business relationships or occasional transactions and will determine whether additional CDD measures should be applied and

the extent of monitoring that is required to mitigate that risk. An individual assessment of risk associated with a business relationship or occasional transaction can inform, but is no substitute for, a business-wide risk assessment.

A customer risk assessment:

- should enable banks to take a holistic view of the risk associated with a business relationship or occasional transaction by considering all relevant risk factors, and

- should be recorded – where the risk is high, banks should include the reason why they are content to accept the risk associated with the business relationship or occasional transaction and details of any steps the bank will take to mitigate the risks, such as restrictions on the account or enhanced monitoring.

See regulation 20 of the *Money Laundering Regulations* and ■ SYSC 6.3.1R

Enhanced due diligence (EDD)

16.3.5 The central objective of EDD is to enable a bank to better understand the risks associated with a high-risk customer and make an informed decision about whether to on-board or continue the business relationship or carry out the occasional transaction. It also helps the bank to manage the increased risk by deepening its understanding of the customer, the beneficial owner, and the nature and purpose of the relationship.

The extent of EDD must be commensurate with the risk associated with the business relationship or occasional transaction but banks can decide, in most cases, which aspects of CDD they should enhance.

Senior management should be provided with all relevant information (eg, source of wealth, source of funds, potential risks, adverse information and red flags) before approving PEP relationships to ensure they understand the nature of, and the risks posed by, the relationship they are approving.

Examples of effective EDD measures we observed included:

- obtaining more information about the customer's or beneficial owner's business

- obtaining more robust verification of the beneficial owner's identity on the basis of information obtained from a reliable and independent source

- carrying out searches on a corporate customer's directors (or individuals exercising control) to understand whether their business or integrity affects the level of risk associated with the business relationship, for example because they also hold a public function

- using open source websites to gain a better understanding of the customer or beneficial owner, their reputation and their role in public life – where banks find information containing allegations of wrongdoing or court judgments, they should assess how this affects the level of risk associated with the business relationship

- establishing the source of wealth to be satisfied that this is legitimate – banks can establish the source of wealth through a

combination of customer-provided information, open source information and documents such as evidence of title, copies of trust deeds and audited accounts (detailing dividends)

•establishing the source of funds used in the business relationship to be satisfied they do not constitute the proceeds of crime

•commissioning external third-party intelligence reports where it is not possible for the bank to easily obtain information through open source searches or there are doubts about the reliability of open source information, and

•where the bank considers whether to rely on another firm for EDD purposes, it ensures that the extent of EDD measures is commensurate with the risk it has identified and that it holds enough information about the customer to carry out meaningful enhanced ongoing monitoring of the business relationship – the bank must also be satisfied that the quality of EDD is sufficient to satisfy the UK's legal and regulatory requirements.

See regulation 7 of the *Money Laundering Regulations*.

Enhanced ongoing monitoring

16.3.6 In addition to guidance contained in ■ FCG 3.2.9G:

•compliance has adequate oversight over the quality and effectiveness of periodic and event-driven reviews, and

•the firm does not place reliance only on identifying large transactions and makes use of other 'red flags'.

Transaction monitoring

Examples of red flags in transaction monitoring can include (this list is not exhaustive):

•third parties making repayments on behalf of the customer, particularly when this is unexpected

•repayments being made from multiple bank accounts held by the customer

•transactions that are inconsistent with the business activities of the customer

•the purpose of the customer account changing without adequate explanation or oversight

•transactions unexpectedly involving high-risk jurisdictions, sectors or individuals

•early repayment of loans or increased frequency/size of repayments

•accounts with low balances but a high volume of large debits and credits

- cumulative turnover significantly exceeding the customer's income/ expected activity
- debits being made shortly after credits of the same value are received
- the customer making frequent transactions just below transaction monitoring alert thresholds
- debits to and credits from third parties where there is no obvious explanation for the transaction, and
- the customer providing insufficient or misleading information when asked about a transaction, or being otherwise evasive.

Customer reviews

Banks must keep the documents, data or information obtained as part of the CDD process up to date. This will help banks ascertain that the level of risk associated with the business relationship has not changed, or enable them to take appropriate steps where it has changed.

Examples of factors which banks may consider when conducting periodic reviews.

- Has the nature of the business relationship changed?
- Does the risk rating remain appropriate in the light of any changes to the business relationship since the last review?
- Does the business relationship remain within the firm's risk appetite?
- Does the actual account activity match the expected activity indicated at the start of the relationship? If it does not, what does this mean?

Examples of measures banks may take when reviewing business relationships:

- assessing the transactions flowing through the customer's accounts at a business relationship level rather than at an individual transaction level to identify any trends
- repeating screening for sanctions, PEPs and adverse media, and
- refreshing customer due diligence documentation, in particular where this is not in line with legal and regulatory standards.

See regulation 8 of the *Money Laundering Regulations*.

Sanctions

16.3.7 In addition to guidance contained in FCG 7, examples of good practice include:

- firms carrying out 'four-eye' checks on sanctions alerts before closing an alert or conducting quality assurance on sanctions alert closure on a sample basis

- firms regularly screening their customer database (including, where appropriate, associated persons, eg, directors) against sanctions lists using systems with fuzzy matching capabilities, and

- specified individuals having access to CDD information held on each of the bank's customers to enable adequate discounting of sanctions alerts.