Chapter 12

Banks' management of high money-laundering risk situations (2011)

12.3 Consolidated examples of good and poor practice

12.3.1 In addition to the examples of good and poor practice below, Section 6 of the report also included case studies illustrating relationships into which banks had entered which caused the *FSA* particular concern. The case studies can be accessed via the link in the paragraph above.

12.3.2 High risk customers and PEPs – AML policies and procedures

Examples of good practice	Examples of poor practice
• Senior management take money laundering risk seriously and understand what the Money Laundering Regulations 2007 are trying to achieve.	• A lack of commitment to AML risk management among senior management and key AML staff.
• Keeping AML policies and procedures up to date to ensure compliance with evolving legal and regulatory obligations.	• Failing to conduct quality assurance work to ensure AML policies and procedures are fit for purpose and working in practice.
• A clearly articulated definition of a PEP (and any relevant sub-categories) which is well understood by relevant staff.	• Informal, undocumented processes for identifying, classifying and declassifying customers as PEPs.
• Considering the risk posed by former PEPs and 'domestic PEPs' on a case-by-case basis.	• Failing to carry out enhanced due diligence on customers with political connections who, although they do not meet the legal definition of a PEP, still represent a high risk of money laundering.
• Ensuring adequate due diligence has been carried out on all customers, even if they have been referred by somebody who is powerful or influential or a senior manager.	• Giving waivers from AML policies without good reason.
• Providing good quality training to relevant staff on	• Considering the reputational risk rather than the

the risks posed by higher risk customers including PEPs and correspondent banks.	AML risk presented by customers.
• A clearly articulated definition of a PEP (and any relevant sub-categories) which is well understood by relevant staff.	• Using group policies which do not comply fully with UK AML legislation and regulatory requirements.
• Ensuring RMs (Relationship Managers) and other relevant staff understand how to manage high money laundering risk customers by training them on practical examples of risk and how to mitigate it.	• Using consultants to draw up policies which are then not implemented.
• Keeping training material comprehensive and up-to-date, and repeating training where necessary to ensure relevant staff are aware of changes to policy and emerging risks.	• Failing to allocate adequate resources to AML.
	• Failing to provide training to relevant staff on how to comply with AML policies and procedures for managing high-risk customers.
	• Failing to ensure policies and procedures are easily accessible to staff.

12.3.3 High risk customers and PEPs – Risk assessment

Examples of good practice	Examples of poor practice
• Using robust risk assessment systems and controls appropriate to the nature, scale and complexities of the bank's business.	• Allocating higher risk countries with low risk scores to avoid having to conduct EDD.
• Considering the money-laundering risk presented by customers, taking into account a variety of factors including, but not limited to, company structures; political connections; country risk; the customer's reputation; source of wealth/ funds; expected account activity; sector risk; and involvement in public contracts.	• MLROs who are too stretched or under resourced to carry out their function appropriately.
• Risk assessment policies which reflect the bank's risk assessment procedures and risk appetite.	• Failing to risk assess customers until shortly before an *FCA* visit.

• Clear understanding and awareness of risk assessment policies, procedures, systems and controls among relevant staff.	• Allowing RMs to override customer risk scores without sufficient evidence to support their decision.
• Quality assurance work to ensure risk assessment policies, procedures, systems and controls are working effectively in practice.	• Inappropriate customer classification systems which make it almost impossible for a customer to be classified as high risk.
• Appropriately-weighted scores for risk factors which feed in to the overall customer risk assessment.	
• A clear audit trail to show why customers are rated as high, medium or low risk.	

12.3.4 High risk customers and PEPs – Customer take-on

Examples of good practice	Examples of poor practice
• Ensuring files contain a customer overview covering risk assessment, documentation, verification, expected account activity, profile of customer or business relationship and ultimate beneficial owner.	• Failing to give due consideration to certain political connections which fall outside the Money Laundering Regulations 2007 definition of a PEP (eg wider family) which might mean that certain customers still need to be treated as high risk and subject to enhanced due diligence.
• The MLRO (and their team) have adequate oversight of all high-risk relationships.	• Poor quality, incomplete or inconsistent CDD.
• Clear processes for escalating the approval of high risk and all PEP customer relationships to senior management or committees which consider AML risk and give appropriate challenge to RMs and the business.	• Relying on Group introductions where overseas standards are not UK-equivalent or where CDD is inaccessible due to legal constraints.
• Using, where available, local knowledge and open source internet checks to supplement commercially available databases when researching potential high risk customers including PEPs.	• Inadequate analysis and challenge of information found in documents gathered for CDD purposes.
• Having clear risk-based policies and procedures setting out the EDD required for	• Lacking evidence of formal sign-off and approval by senior management of

higher risk and PEP customers, particularly in relation to source of wealth.	high-risk and PEP customers and failure to document appropriately why the customer was within AML risk appetite.
• Effective challenge of RMs and business units by banks' AML and compliance teams, and senior management.	• Failing to record adequately face-to-face meetings that form part of CDD.
• Reward structures for RMs which take into account good AML/compliance practice rather than simply the amount of profit generated.	• Failing to carry out EDD for high risk/PEP customers.
• Clearly establishing and documenting PEP and other high-risk customers' source of wealth.	• Failing to conduct adequate CDD before customer relationships are approved.
• Where money laundering risk is very high, supplementing CDD with independent intelligence reports and fully exploring and reviewing any credible allegations of criminal conduct by the customer.	• Over-reliance on undocumented 'staff knowledge' during the CDD process.
• Understanding and documenting complex or opaque ownership and corporate structures and the reasons for them.	• Granting waivers from establishing a customer's source of funds, source of wealth and other CDD without good reason.
• Face-to-face meetings and discussions with high-risk and PEP prospects before accepting them as a customer.	• Discouraging business units from carrying out adequate CDD, for example by charging them for intelligence reports.
• Making clear judgements on money-laundering risk which are not compromised by the potential profitability of new or existing relationships.	• Failing to carry out CDD on customers because they were referred by senior managers.
• Recognising and mitigating the risk arising from RMs becoming too close to customers and conflicts of interest arising from RMs' remuneration structures.	• Failing to ensure CDD for high-risk and PEP customers is kept up-to-date in line with current standards.
	• Allowing 'cultural difficulties' to get in the way of proper questioning to establish required CDD records.

- Holding information about customers of their UK operations in foreign countries with banking secrecy laws if, as a result the firm's ability to access or share CDD is restricted.
- Allowing accounts to be used for purposes inconsistent with the expected activity on the account (e.g. personal accounts being used for business) without enquiry.
- Insufficient information on source of wealth with little or no evidence to verify that the wealth is not linked to crime or corruption.
- Failing to distinguish between source of funds and source of wealth.
- Relying exclusively on commercially-available PEP databases and failure to make use of available open source information on a risk-based approach.
- Failing to understand the reasons for complex and opaque offshore company structures.
- Failing to ensure papers considered by approval committees present a balanced view of money laundering risk.
- No formal procedure for escalating prospective customers to committees and senior management on a risk based approach.
- Failing to take account of credible allegations of criminal activity from reputable sources.
- Concluding that adverse allegations against customers can be disregarded simply because they hold an investment visa.
- Accepting regulatory and/or reputational risk where there is a high risk of money laundering.

12.3.5 High risk customers and PEPs – Enhanced monitoring of high risk relationships

Examples of good practice	Examples of poor practice
• Transaction monitoring which takes account of up-to-date CDD information including expected activity, source of wealth and source of funds.	• Failing to carry out regular reviews of high-risk and PEP customers in order to update CDD.
• Regularly reviewing PEP relationships at a senior level based on a full and balanced assessment of the source of wealth of the PEP.	• Reviews carried out by RMs with no independent assessment by money laundering or compliance professionals of the quality or validity of the review.
• Monitoring new clients more closely to confirm or amend the expected account activity.	• Failing to disclose suspicious transactions to SOCA.
• A risk-based framework for assessing the necessary frequency of relationship reviews and the degree of scrutiny required for transaction monitoring.	• No formal procedure for escalating prospective customers to committees and senior management on a risk based approach.
• Proactively following up gaps in, and updating, CDD during the course of a relationship.	• Failing to seek consent from SOCA on suspicious transactions before processing them.
• Ensuring transaction monitoring systems are properly calibrated to identify higher risk transactions and reduce false positives.	• Unwarranted delay between identifying suspicious transactions and disclosure to SOCA.
• Keeping good records and a clear audit trail of internal suspicion reports sent to the MLRO, whether or not they are finally disclosed to SOCA.	• Treating annual reviews as a tick-box exercise and copying information from the previous review.
• A good knowledge among key AML staff of a bank's highest risk/PEP customers.	• Annual reviews which fail to assess AML risk and instead focus on business issues such as sales or debt repayment.
• More senior involvement in resolving alerts raised for transactions on higher risk or PEP customer accounts, including ensuring adequate explanation and, where necessary, corroboration of unusual transactions from RMs and/or customers.	• Failing to apply enhanced ongoing monitoring techniques to high-risk clients and PEPs.

• Global consistency when deciding whether to keep or exit relationships with high-risk customers and PEPs.	• Failing to update CDD based on actual transactional experience.
• Assessing RMs' performance on ongoing monitoring and feeding this into their annual performance assessment and pay review.	• Allowing junior or inexperienced staff to play a key role in ongoing monitoring of high-risk and PEP customers.
• Lower transaction monitoring alert thresholds for higher risk customers.	• Failing to apply sufficient challenge to explanations from RMs and customers about unusual transactions.
	• RMs failing to provide timely responses to alerts raised on transaction monitoring systems.

12.3.6 Correspondent banking – Risk assessment of respondent banks

Examples of good practice	Examples of poor practice
• Regular assessments of correspondent banking risks taking into account various money laundering risk factors such as the country (and its AML regime); ownership/management structure (including the possible impact/influence that ultimate beneficial owners with political connections may have); products/operations; transaction volumes; market segments; the quality of the respondent's AML systems and controls and any adverse information known about the respondent.	• Failing to consider the money-laundering risks of correspondent relationships.
• More robust monitoring of respondents identified as presenting a higher risk.	• Inadequate or no documented policies and procedures setting out how to deal with respondents.
• Risk scores that drive the frequency of relationship reviews.	• Applying a 'one size fits all' approach to due diligence with no assessment of the risks of doing business with respondents located in higher risk countries.

• Taking into consideration publicly available information from national government bodies and non-governmental organisations and other credible sources.	• Failing to prioritise higher risk customers and transactions for review. • Failing to take into account high-risk business types such as money service businesses and offshore banks.

12.3.7 Correspondent banking – Customer take-on

Examples of good practice	Examples of poor practice
• Assigning clear responsibility for the CDD process and the gathering of relevant documentation.	• Inadequate CDD on parent banks and/or group affiliates, particularly if the respondent is based in a high-risk jurisdiction.
• EDD for respondents that present greater risks or where there is less publicly available information about the respondent.	• Collecting CDD information but failing to assess the risks.
• Gathering enough information to understand client details; ownership and management; products and offerings; transaction volumes and values; client market segments; client reputation; as well as the AML control environment.	• Applying a 'one size fits all' approach to due diligence with no assessment of the risks of doing business with respondents located in higher risk countries.
• Screening the names of senior managers, owners and controllers of respondent banks to identify PEPs and assessing the risk that identified PEPs pose.	• Failing to follow up on outstanding information that has been requested during the CDD process.
• Independent quality assurance work to ensure that CDD standards are up to required standards consistently across the bank.	• Failing to follow up on issues identified during the CDD process.
• Discussing with overseas regulators and other relevant bodies about the AML regime in a respondent's home country.	• Relying on parent banks to conduct CDD for a correspondent account and taking no steps to ensure this has been done.
• Gathering enough information to understand client details; ownership and management; products and offerings; transaction volumes and values; client	• Collecting AML policies etc but making no effort to assess them.

market segments; client reputation; as well as the AML control environment.	
• Visiting, or otherwise liaising with, respondent banks to discuss AML issues and gather CDD information.	• Having no information on file for expected activity volumes and values.
• Gathering information about procedures at respondent firms for sanctions screening and identifying/managing PEPs.	• Failing to consider adverse information about the respondent or individuals connected with it.
• Understanding respondents' processes for monitoring account activity and reporting suspicious activity.	• No senior management involvement in the approval process for new correspondent bank relationships or existing relationships being reviewed.
• Requesting details of how respondents manage their own correspondent banking relationships.	
• Senior management/senior committee sign-off for new correspondent banking relationships and reviews of existing ones.	

12.3.8 Correspondent banking –Ongoing monitoring of respondent accounts

Examples of good practice	Examples of poor practice
• Review periods driven by the risk rating of a particular relationship; with high risk relationships reviewed more frequently.	• Copying periodic review forms year after year without challenge from senior management.
• Obtaining an updated picture of the purpose of the account and expected activity.	• Failing to take account of any changes to key staff at respondent banks.
• Updating screening of respondents and connected individuals to identify individuals/entities with PEP connections or on relevant sanctions lists.	• Carrying out annual reviews of respondent relationships but failing to consider money-laundering risk adequately.
• Involving senior management and AML staff in reviews of respondent relationships and consideration of whether to maintain or exit high-risk relationships.	• Failing to assess new information gathered during ongoing monitoring of a relationship.
• Where appropriate, using intelligence reports to help decide whether to maintain or exit a relationship.	• Failing to consider money laundering alerts generated since the last review.

• Carrying out ad-hoc reviews in light of material changes to the risk profile of a customer.	• Relying on parent banks to carry out monitoring of respondents without understanding what monitoring has been done or what the monitoring found. • Failing to take action when respondents do not provide satisfactory answers to reasonable questions regarding activity on their account. • Focusing too much on reputational or business issues when deciding whether to exit relationships with respondents which give rise to high money-laundering risk.

12.3.9 Wire transfers – Paying banks

Examples of good practice	Examples of poor practice
• Banks' core banking systems ensure that all static data (name, address, account number) held on the ordering customer are automatically inserted in the correct lines of the outgoing MT103 payment instruction and any matching MT202COV.	• Paying banks take insufficient steps to ensure that all outgoing MT103s contain sufficient beneficiary information to mitigate the risk of customer funds being incorrectly blocked, delayed or rejected.

12.3.10 Wire transfers – Intermediary banks

Examples of good practice	Examples of poor practice
• Where practical, intermediary and beneficiary banks delay processing payments until they receive complete and meaningful information on the ordering customer. • Intermediary and beneficiary banks have systems that generate an automatic investigation every time a MT103 appears to contain	• Banks have no procedures in place to detect incoming payments containing meaningless or inadequate payer information, which could allow payments in breach of sanctions to slip through unnoticed.

	inadequate payer information. • Following processing, risk-based sampling for inward payments identifies inadequate payer information. • Search for phrases in payment messages such as 'one of our clients' or 'our valued customer' in all the main languages which may indicate a bank or customer trying to conceal their identity.

12.3.11 Wire transfers – Beneficiary banks

Examples of good practice	Examples of poor practice
• Establishing a specialist team to undertake risk-based sampling of incoming customer payments, with subsequent detailed analysis to identify banks initiating cross-border payments containing inadequate or meaningless payer information. • Actively engaging in dialogue with peers about the difficult issue of taking appropriate action against persistently offending banks.	• Insufficient processes to identify payments with incomplete or meaningless payer information.

12.3.12 Wire transfers – Implementation of SWIFT MT202COV

Examples of good practice	Examples of poor practice
• Reviewing all correspondent banks' use of the MT202 and MT202COV. • Introducing the MT202COV as an additional element of the CDD review process including whether the local regulator expects proper use of the new message type. • Always sending an MT103 and matching MT202COV wherever the sending bank has a correspondent relationship and is not in a position to 'self clear' (eg for Euro payments within	• Continuing to use the MT202 for all bank-to-bank payments, even if the payment is cover for an underlying customer transaction.

	a scheme of which the bank is a member).
•	Searching relevant fields in MT202 messages for the word 'cover' to detect when the MT202COV is not being used as it should be.