FSA®
Financial Services Authority

Banks' management of high money-laundering risk situations

How banks deal with high-risk customers (including politically exposed persons), correspondent banking relationships and wire transfers

June 2011

Contents

1. Executive Summary

1.1. Introduction

1. This report describes how banks operating in the UK are managing money-laundering risk in higher risk situations. It focuses in particular on correspondent banking relationships, wire transfer payments and high-risk customers including politically exposed persons (PEPs). PEPs are individuals whose prominent position in public life may make them vulnerable to corruption. The definition extends to immediate family members and known close associates.

2. We expect firms to consider our findings and translate them into more effective policies and controls where necessary. This report also outlines proposed guidance, in the form of examples of good and poor practice which, following post-consultation implementation, we will expect firms to take into account. The finalised guidance will be included in Financial Crime: a guide for firms, on which we are currently consulting in CP11/12. If you have any comments on the proposed good and poor practice guidance in this report, please respond to the consultation on the guide.

3. As in any other area of their business, firms should adopt an appropriate, risk-based approach to anti-money laundering, taking into account relevant factors including their customer base, business and risk profile. Failure to do so may result in the FSA taking action.

4. As a result of this review and our concurrent casework, we have referred two banks to our enforcement division after identifying apparent serious weaknesses in their systems and controls for managing high-risk customers, including PEPs. We are considering whether further regulatory action is required in relation to other banks and further cases may be referred to enforcement.

5. Given the nature of our findings, the management of high-risk customers, including PEPs, will remain a significant focus of our anti-financial crime work for some time to come.

1.2. Findings

6. Although we identified some examples of good anti-money laundering (AML) risk management, we were concerned to find serious weaknesses common to many firms included in our review. The following are the main findings:

High-risk customers/PEPs

7. Some banks appeared unwilling to turn away, or exit, very profitable business relationships when there appeared to be an unacceptable risk of handling the proceeds of crime. Around a third of banks, including the private banking arms of some major banking groups, appeared willing to accept very high levels of money-laundering risk if the immediate reputational and regulatory risk was acceptable.

8. Over half the banks we visited failed to apply meaningful enhanced due diligence (EDD) measures in higher risk situations and therefore failed to identify or record adverse information about the customer or the customer's beneficial owner. Around a third of them dismissed serious allegations about their customers without adequate review.

9. More than a third of banks visited failed to put in place effective measures to identify customers as PEPs. Some banks exclusively relied on commercial PEPs databases, even when there were doubts about their effectiveness or coverage. Some small banks unrealistically claimed their relationship managers (RMs) or overseas offices knew all PEPs in the countries they dealt with. And, in some cases, banks failed to identify customers as PEPs even when it was obvious from the information they held that individuals were holding or had held senior public positions.

10. Three quarters of the banks in our sample failed to take adequate measures to establish the legitimacy of the source of wealth and source of funds to be used in the business relationship. This was of concern in particular where the bank was aware of significant adverse information about the customer's or beneficial owner's integrity.

11. Some banks' AML risk-assessment frameworks were not robust. For example, we found evidence of risk matrices allocating inappropriate low-risk scores to high-risk jurisdictions where the bank maintained significant business relationships. This could have led to them not having to apply EDD and monitoring measures.

12. Some banks had inadequate safeguards in place to mitigate RMs' conflicts of interest. At more than a quarter of banks visited, RMs appeared to be too close to the customer to take an objective view of the business relationship and many were primarily rewarded on the basis of profit and new business, regardless of their AML performance.

13. At a third of banks visited, the management of customer due diligence records was inadequate and some banks were unable to give us an overview of their high-risk or PEP relationships easily. This seriously impeded these banks' ability to assess money laundering risk on a continuing basis.

14. Nearly half the banks in our sample failed to review high-risk or PEP relationships regularly. Relevant review forms often contained recycled information year after year, indicating that these banks may not have been taking their obligation to conduct enhanced monitoring of PEP relationships seriously enough.

15. At a few banks, the general AML culture was a concern, with senior management and/or compliance challenging us about the whole point of the AML regime or the need to identify PEPs.

Correspondent banking

16. Some banks conducted good quality AML due diligence and monitoring of relationships, while others, particularly some smaller banks, conducted little and, in some cases, none. In several smaller banks, a tick-box approach to AML due diligence was noted. Many (especially smaller) banks' due diligence procedures resembled a 'paper gathering' exercise with no obvious assessment of the information collected; there was also over-reliance on the *Wolfsberg Group AML Questionnaire* which gives only simple yes or no answers to basic AML questions without making use of the Wolfsberg Principles on correspondent banking. And when reviews of correspondent relationships were conducted, they were often clearly copied and pasted year after year with no apparent challenge.

17. Some banks did not carry out due diligence on their parent banks or banks in the same group, even when they were located in a higher risk jurisdiction or there were other factors which increased the risk of money laundering.

18. A more risk-based approach is required where PEPs own, direct or control respondent banks. We found there was a risk that some banks' respondents could be influenced by allegedly corrupt PEPs, increasing the risk of these banks being used as vehicles for corruption and/or money laundering.

19. Transaction monitoring of correspondent relationships is a challenge for banks due to often erratic, yet legitimate, flows of funds. Banks ultimately need to rely on the explanations of unusual transactions given by respondents and this can be difficult to corroborate. However, there were some occasions where we felt banks did not take adequate steps to verify such explanations.

20. We found little evidence of assessment by internal audit of the money-laundering risk in correspondent banking relationships; this is unsatisfactory given the high money-laundering risk which is agreed internationally to be inherent in correspondent banking.

Wire transfers

21. We had no major concerns about banks' compliance with the Wire Transfer Regulations (WTRs). However, there seemed to be a lack of strategic response across the industry in terms of dealing with paying banks which repeatedly failed

to meet the WTRs' standards. There was clearly some concern among larger banks not to be the first to address this issue. So we encourage banks to work together to formulate a strategic response to dealing with non-compliant paying banks.

1.3. Conclusions

22. Our review found no major weaknesses in banks' compliance with the WTRs. On correspondent banking, there was a wide variance in standards, with some banks carrying out good quality AML work, while others, particularly smaller banks, carried out either inadequate due diligence or none at all.

23. Our main conclusion is that around three quarters of banks in our sample, including the majority of major banks, are not always managing high-risk customers and PEP relationships effectively and must do more to ensure they are not used for money laundering. Despite changes in the legal and regulatory framework a number of the weaknesses identified during this review are the same as, or similar to, those identified in the FSA report of March 2001 covering how banks in the UK handled accounts linked to the former Nigerian military leader, General Sani Abacha.[1] We are concerned there has been insufficient improvement in banks' AML systems and controls during this period.

24. Serious weaknesses identified in banks' systems and controls, as well as indications that some banks are willing to enter into very high-risk business relationships without adequate controls when there are potentially large profits to be made, means that it is likely that some banks are handling the proceeds of corruption or other financial crime. Section 6 of this report comprises anonymised case studies of some of the high-risk relationships we reviewed.

25. We will, where appropriate, use our enforcement powers to reinforce key messages in this report to encourage banks and other firms to strengthen AML systems and controls and deter them from making decisions which do not take adequate account of money laundering risk. We hope the case studies and examples of good and poor practice we set out here will help firms improve their practices.

1 See: www.fsa.gov.uk/Pages/Library/Communication/PR/2001/029.shtml

2. Introduction

2.1. Background and objectives

26. This report contains our findings from a major project to examine how banks manage situations where there is a high risk of money laundering. Our work focused on high-risk customers including PEPs, correspondent banking relationships and the money-laundering risk associated with wire transfer payments.

27. The risk of money laundering is relevant to two of our statutory objectives:

    - *Reducing the extent to which it is possible for a firm to be used for purposes connected with financial crime*, because weak AML controls leave firms vulnerable to becoming involved in money laundering, unwittingly or otherwise; and
    - *Maintaining market confidence* because the use of UK firms to launder money could adversely affect the reputation of the UK market.

28. The FSA is also the 'competent authority' under the Money Laundering Regulations and the Wire Transfer Regulations. This means we are responsible for ensuring that financial services firms comply with this legislation.

29. We decided to carry out this project because:

    - the areas covered have all been identified as high risk by the Financial Action Task Force (FATF);
    - the UK government views effective AML controls over PEPs as an integral part of its strategy to combat international corruption and its goal of 'making the UK a hostile environment for corrupt PEPs'; and
    - we had not previously conducted significant thematic work on correspondent banking or PEPs and none at all on wire transfers. One of the reasons for this is that we were awaiting the new SWIFT messaging standards introduced in November 2009.

30. Our main objective was to assess whether banks had robust and proportionate systems and controls in place to identify, detect and prevent the misuse of correspondent banking facilities, meet the requirements to identify the originators of international wire transfers, and reduce the risk of corrupt PEPs and other high-risk customers misusing the UK banking system. In addition, we aimed to identify good practice to share with the industry and highlight areas where improvement is required. This report contains many examples of good and poor practice observed during our fieldwork.

31. Firms should consider our findings, translate them into more effective assessment of this risk, and implement and maintain more effective controls where necessary. As in any other area of their business, firms should take an appropriate, risk-based approach to AML, taking into account relevant factors including their customer base, business and risk profile. Failure to do so may result in us taking action.

2.2. Methodology

32. The fieldwork for our review began in early 2010 and continued until February 2011. Before visiting banks, we met law enforcement agencies, forensic accountants, AML consultants, lawyers and commercial providers of intelligence tools (which some firms use in their AML work) to hear their views of banks' AML performance in the areas covered by our review.

33. From May 2010, we conducted 35 visits to 27 banking groups in the UK with significant international activity exposing them to money laundering risks arising from high-risk customers/PEPs, correspondent banking and wire transfers. Our sample comprised eight major banks and 19 medium-sized and smaller banks, including banks from higher risk countries and private banks. The banks were chosen because they dealt in products or with customers likely to give rise to high levels of inherent money laundering risk; none of the banks were selected because of pre-existing concerns about their AML systems and controls. We therefore consider our sample to be representative of banks dealing with higher risk customers and products.

34. In early 2011, we also visited several large banks' overseas centres to assess significant relevant outsourced functions such as payment processing and the initial assessment of transaction monitoring alerts. We obtained information from each of the banks before the visits, including relevant policies and procedures; risk assessments; details of staff involved in managing relationships with high-risk customers, including PEPs and respondent banks; recent minutes of any relevant committee meetings; and details of AML training received by key staff.

35. Our visits included interviews with key staff including the bank's Money Laundering Reporting Officer (MLRO); relationship managers for high-risk customers including PEPs and correspondent banks; and staff responsible for processing wire transfers so we could build a detailed understanding of the bank's relevant AML policies and procedures and their practical implementation. We also conducted reviews of a sample of files for high-risk customers in order to assess the quality of due diligence applied to these relationships both at customer take-on and on a continuing basis.

36. We would like to thank the banks which participated in the review for the information they supplied before and during our visits, and for meeting us. We would also like to thank the stakeholders for their advice and assistance.

2.3. Banks' AML legal and regulatory obligations

37. Banks' legal and regulatory AML obligations are primarily set out in the Money Laundering Regulations 2007, the Proceeds of Crime Act 2002, the Transfer of Funds (Information on the Payer) Regulations 2007 (the 'Wire Transfer Regulations') and the FSA's Handbook. This section summarises the obligations relevant to this review.

38. Banks are required to put in place and maintain policies and procedures to prevent and detect money-laundering. These policies and procedures have to be communicated to relevant staff and must cover matters including risk assessment and management, risk-sensitive customer due diligence and monitoring measures, staff training and record-keeping.

39. Banks are also under a regulatory obligation to establish, implement and maintain adequate policies and procedures for countering the risk that they might be used to further financial crime. These policies and procedures must be comprehensive and proportionate to the nature, scale and complexity of a bank's activities and include systems and controls to identify, assess, monitor and manage money laundering risk.

40. Banks must document their AML risk assessment, policies and procedures, and their application, in a way that allows the FSA to monitor banks' compliance with regulatory requirements, the Money Laundering Regulations and the Wire Transfer Regulations.

41. The FSA has regard to relevant provisions in the Joint Money Laundering Steering Group's guidance (the JMLSG Guidance) when considering whether a bank meets its legal and regulatory AML obligations.

Customer Due Diligence (CDD) and Monitoring

42. Banks are required to apply risk-sensitive CDD measures, conduct ongoing monitoring of the business relationship and keep records in line with Part 2 of the Money Laundering Regulations.

43. CDD obligations require banks to:

- identify and verify the customer's identity;
- identify, where applicable, the customer's beneficial owner and verify the beneficial owner's identity – this includes a requirement to take measures to understand the ownership and control structure of the customer; and
- obtain information on the purpose and intended nature of the business relationship.

44. Banks must apply CDD measures when they establish a business relationship; or doubt the veracity or adequacy of previously obtained documents, data or information; or suspect money laundering.

45. Banks are required to conduct ongoing monitoring of the business relationship, which includes an obligation to keep documents, data or information obtained for the purpose of customer due diligence measures up-to-date. Banks must be able to identify and scrutinise unusual transactions, or patterns of transactions which have no apparent economic or visible lawful purpose, complex or unusually large transactions and any other activity which is regarded as particularly likely to be related to money laundering. Where these give rise to knowledge, suspicion or reasonable grounds for knowing or suspecting that money laundering is taking place, banks must make a Suspicious Activity Report (SAR) to the Serious Organised Crime Agency (SOCA).

46. Banks must keep copies of, or references to, the evidence obtained during the CDD process, as well as supporting records for at least five years after the end of the business relationship or the completion of an occasional transaction. These records must be organised in an orderly way to enable banks to meet their legal obligations and to enable us to monitor their compliance.

47. Banks must determine the extent of CDD measures and ongoing monitoring on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction. They must be able to demonstrate to us that the extent of these measures is appropriate to the level of money-laundering risk.

Enhanced Customer Due Diligence (EDD) and monitoring

48. Where the money laundering or terrorist financing risk is increased, banks must apply EDD measures and conduct enhanced monitoring of the business relationship.

49. The Money Laundering Regulations set out three situations where specific EDD measures must always be applied:

- in relation to correspondent banking relationships with respondents from non-EEA countries;

- in situations where the customer is not physically present for identification purposes; and
- where the customer is a Politically Exposed Person (PEP).

50. PEPs are individuals whose prominent position in public life may make them vulnerable to corruption. The definition extends to immediate family members and known close associates. Banks must establish and maintain appropriate and risk-sensitive policies and procedures to determine whether a customer is a PEP.

51. When dealing with a PEP customer, the Money Laundering Regulations require banks, on a risk-sensitive basis, to:

- obtain appropriate senior management approval for establishing a business relationship with a PEP customer;
- take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction; and
- conduct enhanced ongoing monitoring of the business relationship.

Prohibited business relationships

52. Banks must not engage in, or continue, a business relationship in situations where:

- a bank is unable to apply CDD measures in line with the provisions of Part 2 of the Money Laundering Regulations;
- the Treasury uses its powers under the Money Laundering Regulations to prohibit firms from forming, or to require them to terminate, relationships with customers situated in a given country to which the FATF has applied countermeasures; or
- the UK's financial sanctions regime applies.

2.3.1. The Wire Transfer Regulations

53. FATF issued Special Recommendation VII in October 2001, with the objective of enhancing the transparency of all wire transfers, both domestic and cross-border, thereby making it easier for law enforcement investigators to track funds transferred electronically by terrorists and other criminals. It was implemented in EU member states through the Wire Transfer Regulations (WTRs) which came into effect on 1 January 2007. The JMLSG Guidance, Section 3[2] covers wire transfers in detail.

2 See: www.jmlsg.org/download/6130

Paying banks

54. The WTRs require paying banks to ensure all wire transfers carry specified information about the payer. The core requirement is that this information comprises the payer's name, address and account number although there are some important exceptions and derogations to this requirement, which are set out in the JMLSG Guidance. The WTRs apply even where payer and payee hold accounts with the same bank.

55. Paying banks must ensure that the payer information conveyed in payment messages is accurate and verified. The verification requirement is deemed to be met for account holders on whom adequate AML CDD has been conducted. For non-account holders, paying banks should verify the identity and address (or a permitted alternative) of the payer before making one-off payments, or a number of linked transactions, exceeding €1,000.

Intermediary banks

56. Intermediary banks must ensure that all information received on the payer which accompanies a wire transfer is retained with the transfer. However, where an intermediary bank within the EU is technically unable to pass on payer information originating outside the EU, it may use a system with technical limitations provided that:

    - if it is aware that the payer information is missing or incomplete, it must concurrently advise the payee's payment services provider (PSP); and
    - it retains records of information received for five years, whether or not it is complete. If requested by the payee's PSP, the intermediary bank must provide the payer information within three working days.

Checking incoming payments

57. PSPs should have effective procedures for checking that incoming wire transfers comply with the WTRs. However, to avoid disrupting straight-through processing, it is not expected that banks monitor them while processing a transfer. But banks should have procedures to detect whether required information is missing and take remedial action when they become aware that an incoming payment is not compliant.

In practical terms, SWIFT's validation procedures provide only a very limited initial defence against a beneficiary bank receiving payment messages with no, or incomplete, payer information. Where the payer information fields have been completed with incorrect or meaningless information, or where there is no account number, the payment cannot be stopped by SWIFT's validation procedures. Only SWIFT messages in which mandatory payer information fields have been left blank will fail validation.

58. It is acknowledged that many deficient payments will inevitably pass through the international payment system. Therefore, PSPs should deploy two types of control:

    - first, unless PSPs can detect incomplete or meaningless payer information at the time of processing a transfer, there should be risk-based sampling to detect non-compliant payments after they have been processed; and
    - second, PSPs are encouraged to apply filtering procedures to pick up obvious meaningless information, such as 'one of our customers' or similar forms of words that avoids providing specific information about the payer.

59. The JMLSG Guidance states that if a PSP becomes aware that a payment contains meaningless or incomplete information, it should either reject the transfer or ask for complete information on the payer. In addition, in such cases, the PSP must take any necessary action to comply with its money laundering and terrorist financing obligations; this could include making the payment or holding the funds and advising the MLRO.

Dealing with PSPs who regularly fail to comply with the WTRs

60. In the absence of a satisfactory response to a request for missing information, the sending PSP should be warned that it may in future be subject to high-risk monitoring and, if the payment is deemed suspicious, a SAR should be made.

A 'Common Understanding' published in October 2008 by the AML Task Force of three European regulatory bodies stated that a receiving PSP is expected to establish criteria for determining when a sending PSP is 'regularly failing' to provide information. The receiving PSP then:

- *is expected to notify the failing PSP that it has been identified as failing to comply with the WTRs; and*
- *must notify its regulator of the failing PSP.*

61. However, while the WTRs state that a receiving PSP should decide whether to restrict or terminate business relationships with failing PSPs, other factors and business considerations will usually need to be considered in practice. Despite this, the JMLSG Guidance states that PSPs are expected to have a clearly

articulated policy, approved by senior management, defining the approach to be taken to persistently failing sender PSPs.

2.3.2. The FSA Handbook

62. Firms' regulatory responsibilities in this area are defined in our Handbook. Principle 2 requires that 'a firm must conduct its business with due skill, care and diligence' and Principle 3 that 'a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems'. In addition, Principle 1, which requires firms to conduct business with integrity, may be relevant if banks were knowingly to enter into relationships with high money-laundering risk in order to make profit.

63. In line with these Principles, firms' senior management are responsible for making an appropriate assessment of financial crime risks, including those relating to AML. Our rule SYSC 6.1.1R requires banks and other firms to 'establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable, tied agents) with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime.' This is the minimum standard to meet the requirements of the regulatory system.

3. Findings – high risk customers and PEPs

3.1. AML policies and procedures

64. The Money Laundering Regulations 2007 and our senior management systems and control rules require banks to put in place risk-sensitive AML policies and processes. These should enable banks to identify and focus on those business relationships that pose the greatest risk of money laundering. These policies and processes should have the clear support of senior management, be communicated to relevant staff and implemented effectively.

65. Although all the banks we visited had an AML policy document, some banks' policies were clearly out of date and had not been reviewed for some time. Examples of outdated information noted in banks' policies included references to the requirements of Money Laundering Regulations 2003 rather than the requirements of the Money Laundering Regulations 2007. This meant that, in some cases, banks' AML policies and processes had not been updated to ensure compliance with current legal and regulatory obligations.

66. Other policy documents contained significant gaps. For example, some banks had no formal procedures in place to identify PEP customers and one small bank had no reference to PEPs anywhere in its policy.

67. Two banks in our sample had employed consultants to review the firm's policies, procedures, systems and controls for the first time after receiving notice of our visit. In those cases, we found good AML policies that had either not been implemented or were not understood by key members of staff.

68. It is essential for banks to update their AML policies and procedures regularly to take account of new operational, legal and regulatory developments and of emerging risks.

Two banks in our sample were using overseas group policy without (i) key UK staff understanding it or (ii) ensuring it took into account UK AML legal and regulatory obligations.

69. It is equally important that these policies and procedures are implemented effectively. We found that some banks failed to comply with their own, well-documented, AML policies and procedures.

3.1.1. PEP definition

70. The Money Laundering Regulations define PEPs as individuals who are or have, at any time in the preceding year, been entrusted with a prominent public function by a non-UK country, the European Community or an international body. The definition extends to such individuals' immediate family members and close associates.

71. We found that most banks in our sample based their PEP definition on the Money Laundering Regulations' definition. However, more than half the banks we visited also included UK customers holding public office within their PEP definition and often referred to these customers as 'domestic PEPs'. Some banks classified PEPs to a more granular level to adjust levels of enhanced due diligence and ongoing monitoring accordingly. For example, some banks distinguished between normal PEPs and 'sensitive' (ie very high risk) PEPs; current and former PEPs; and foreign and 'domestic PEPs'.

72. However, some banks' PEP definition did not fully reflect the risk of corruption posed by PEP customers, and some banks' definition of PEPs revealed significant gaps by excluding positions associated with significant corruption risks.

One bank's PEP definition appeared inconsistent because it included 'Russian oligarchs' but oligarch-type customers from other countries were not considered to be PEPs.

73. Staff at some banks failed to understand their own PEP definition. In addition, a third of banks visited failed to give due consideration to certain political connections (eg wider family) which meant that, although certain customers might not fall within the Money Laundering Regulations definition of a PEP, they might still have need to be treated as high risk and subject to enhanced due diligence.

At two banks, the MLROs could not explain their PEP definition.

74. A quarter of banks visited appeared more concerned that a PEP might be involved in a public corruption scandal than that they might be corrupt and/or laundering the proceeds of corruption. Reputational risk and money laundering risk are not the same and steps to mitigate reputational risk will not always reduce the risk of money laundering.

3.1.2. Training and awareness

75. It is important for firms engaged in activity with higher risk customers, including PEPs and correspondent banks, to train relevant staff on the money-laundering risks associated with them. (There are more specific findings from our review of correspondent banking relationships in Section 4.)

76. All firms required staff to take undertake training, and in some cases pass a test on, AML. This training was usually computer-based or a presentation from the compliance department. However, these general AML training programmes rarely contained specific, detailed material on higher risk activities.

> *One of the few firms which did provide relevant training material to us ahead of our visit had not, in fact, given this training to relevant staff. So when we followed up on this training with a number of RMs for high-risk correspondent banking customers, they were not aware of it.*

77. Although detailed training on the risk posed by high-risk customers may not be needed for some staff who are not involved in dealing with them, we were generally disappointed at the lack of bespoke training provided to staff directly involved in dealing with high-risk customers and we expect firms to improve in this area. This is especially important as we identified a number of issues during our review (covered in depth elsewhere in this report) which showed that staff dealing with high-risk customers were sometimes making poor judgements about the associated money-laundering risk.

3.1.3. AML policies and procedures – examples of good and poor practice

Good practice

- Senior management take money laundering risk seriously and understand what the Regulations are trying to achieve.
- Keeping AML policies and procedures up-to-date to ensure compliance with evolving legal and regulatory obligations.
- A clearly articulated definition of a PEP (and any relevant sub-categories) which is well understood by relevant staff.
- Considering the risk posed by former PEPs and 'domestic PEPs' on a case-by-case basis.
- 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.
- Providing good quality training to relevant staff on the risks posed by higher risk customers including PEPs and correspondent banks.
- Ensuring RMs 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.

- 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.

Poor practice

- A lack of commitment to AML risk management among senior management and key AML staff.
- Failing to conduct quality assurance work to ensure AML policies and procedures are fit for purpose and working in practice.
- Informal, undocumented processes for identifying, classifying and declassifying customers as PEPs.
- 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.
- Giving waivers from AML policies without good reason.
- Considering the reputational risk rather than the AML risk presented by customers.
- Using group policies which do not comply fully with UK AML legislation and regulatory requirements.
- Using consultants to draw up policies which are then not implemented.
- 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.

3.2. Risk assessment

3.2.1. Common risk assessment methodology

78. All the banks we visited had an AML policy and most banks' overall money-laundering risk assessment was reflected in that policy. This typically referred to high-risk jurisdictions, vulnerable business activities and, in some cases, prohibitions of relationships that were deemed too risky. Many banks had adjusted their risk assessment in line with different areas of operation.

79. When assessing the risk associated with individual business relationships, most banks used a risk-scoring system. The risk score was usually generated by staff completing a risk assessment form either on paper or on a computer

system. The overall risk score was usually generated by adding together scores (or taking an average) for different AML risk factors. AML risk factors banks considered included:

- the transparency of company structures and beneficial owners;
- political connections of the customer or associated individuals;
- connections (through nationality, residency, country of incorporation etc) to high risk countries or those subject to financial sanctions;
- the customer's reputation and/or known adverse information about the customer;
- the source, structure and adequacy of information about the customer's wealth;
- the source of the customer's funds;
- expected activity on the account (types of transaction, volumes, amounts, the use of cash);
- the customer's profession/industry sector; and
- involvement in public contracts.

80. Once a score was generated, the customer was usually categorised as high, medium or low risk and this usually determined the level of CDD required; the frequency at which the relationship was reviewed; and the level of seniority required to give approval for entering into the relationship and for signing off account reviews.

81. In some firms, the existence of certain high-risk factors (eg political connections, opaque company structures, high-risk countries or adverse information about the customer) led either to automatic referral of the proposed relationship to the bank's Compliance or AML team or an automatic high-risk classification, regardless of the overall customer score.

82. In general, this kind of structured risk assessment process appeared to help some banks make well-informed and consistent decisions about whether a potential or existing customer relationship was within risk appetite.

3.2.2. Common weaknesses in risk assessment

83. We found serious weaknesses in some banks' risk assessment policies and processes. A third of banks we visited failed to review their risk assessment regularly and to take account of significant new developments and insights, such as new evidence of country risk or displacement of criminal activity to other products or services. For example, some had not updated their risk assessment to take into account FATF's current list of countries with strategic deficiencies. Other weaknesses included:

- Some banks allocating inappropriately low risk weightings for certain high risk factors, apparently – and sometimes overtly – to avoid having to conduct enhanced due diligence on much of their business. Others failed to take into account well-known high-risk indicators, such as links to certain business activities commonly associated with higher levels of corruption, or failed to take into account adverse information from a variety of sources.

One bank considered several higher risk countries as 'low risk' because they had 'lots of dealings' with them. At another bank, relationships with customers in a higher risk country were exempt from country risk assessment simply because the bank's parent had a presence in the higher risk country.

At other banks, sectors normally associated with increased corruption risks such as extractive industries and pharmaceuticals were classified as low risk because these sectors were 'regulated'. However, they are not regulated for AML purposes.

- Some banks failing to carry out a risk assessment of their business relationships at all or only shortly before our visit.

One bank with many high-risk customer relationships changed the status of many relationships from low risk to high risk one month before our visit.

- Some banks' CDD files did not contain adequate documentary evidence on files to show why customers were rated a high, medium or low risk.

At one bank, we reviewed 13 retail accounts classified as high risk but there was no explanation or obvious reason to show why.

- At some banks, RMs were able to override the risk score generated by the risk-assessment process without sufficient evidence to support their decision.

At one bank, a customer who was the subject of allegations of corruption was classified as low risk simply because he came from a low risk country.

- Some banks scored risks in a way such that, in practice, it was almost impossible for a relationship to be classified as high risk.

A small bank had introduced a system to score its customers but the risk scoring methodology meant it would be very unlikely for a customer to be given a 'high risk' rating. In addition, the AML risk factors considered by the bank were weighted equally when some factors appeared to give rise to more risk. Moreover, customer-facing staff at this bank did not understand how the risk score was generated and were confused about what score would make a customer 'high risk'.

- In some banks, staff did not understand or were unaware of the risk assessment process and/or methodology.

One firm could not explain to us how customer risk ratings were decided. The MLRO said the bank simply followed its overseas parent's procedures which may not have been fully compatible with UK AML requirements.

- Some banks failed to update customer risk assessment during ongoing monitoring of the relationship.

3.2.3. Risk assessment– examples of good practice and poor practice

Good practice

- Using robust risk assessment systems and controls appropriate to the nature, scale and complexities of the bank's business.
- 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.
- Risk assessment policies which reflect the bank's risk assessment procedures and risk appetite.
- Clear understanding and awareness of risk assessment policies, procedures, systems and controls among relevant staff.
- Quality assurance work to ensure risk assessment policies, procedures, systems and controls are working effectively in practice.
- 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.

Poor practice

- Allocating higher risk countries with low risk scores to avoid having to conduct EDD.
- MLROs who are too stretched or under resourced to carry out their function appropriately.
- Failing to risk assess customers until shortly before an FSA visit.
- Allowing RMs to override customer risk scores without sufficient evidence to support their decision.
- Inappropriate customer classification systems which make it almost impossible for a customer to be classified as high risk.

3.3. Customer take-on

84. 'Customer take-on' describes the process during which a bank applies CDD measures and decides whether to establish a business relationship. The bank will determine this through a consideration of factual information and the its risk appetite.

3.3.1. CDD

85. Banks must carry out CDD measures to understand who their customer and, where applicable, the customer's beneficial owner are and to verify that they are who they claim to be. CDD also encompasses a requirement to understand the purpose and intended nature of the business relationship; this includes taking risk-sensitive measures to understand where the customer's funds and wealth come from. Banks have to obtain sufficient CDD information to develop a comprehensive profile of the customer and, where applicable, the beneficial owner, and to understand the risks associated with the business relationship.

86. Where the money-laundering risk associated with the business relationship is increased, including where the customer is a PEP, banks must carry out additional, enhanced due diligence or 'EDD'.

3.3.2. Identification and verification of identity

87. Identifying a customer and, where appropriate the customer's beneficial owner, means taking steps to understand who the customer or beneficial owner is. For AML purposes, a person's identity consists of their name, date of birth and residential address, but other aspects, such as their occupation, will also be relevant. The identity of legal persons or arrangements is primarily defined by their legal and ownership structure, their business and their constitution.

88. Banks must decide how much information about a customer's or beneficial owner's identity they need to obtain and which information they need to verify to be satisfied that they know who the customer and, where appropriate, the customer's beneficial owner are. This decision will be influenced by information such as the nature of the product or service sought. Banks must be flexible in their application of identification and verification measures to respond appropriately to higher risk indicators as they emerge.

89. In general, we found most banks took the steps necessary to meet their customer identification and verification obligations under the Money Laundering Regulations. Many banks also had good processes in place to identify whether a customer was a PEP. We were, however, concerned to find that some banks failed to give due consideration to the risks posed by customers who no longer met the Money Laundering Regulations' PEP definition. For example, some banks who had customers who had left public office more than a year before did not properly consider whether the high money-laundering risk associated with their previous position had adequately abated. Other banks relied exclusively on commercially available PEP databases to identify PEPs. And a fifth of banks visited failed to identify high-risk PEPs even where they were in possession of other information which clearly indicated the customer was a PEP and, in some cases, alleged criminal activity.

One large bank held an account for a wealthy customer from an oil-rich country associated with very high levels of corruption. This customer had accumulated considerable wealth in the oil industry and maintained close links to the country's political and military elite. The bank's PEP database checks did not identify the customer as a PEP and the bank did not conduct any further research on him.

When challenged about the customer's political exposure and the corruption allegations, the bank's MLRO called the FSA to say that his team had been unable to find any adverse information. We told the MLRO that the first result of a simple Google search of the customer's name linked the customer to serious and credible allegations of corruption.

90. Some banks were unable to prove that they had obtained meaningful evidence of identity. This was sometimes the result of the inappropriate application of CDD waivers in cases of high money-laundering risk, of banks' failure to obtain missing information when accounts were reviewed or, in some cases, inadequate record-keeping which made identifying missing information very difficult.

We reviewed over 100 high-risk or PEP customer files at the private banking arm of a major banking group. We found that around 25% of these accounts had seriously deficient identification and verification documentation or none at all. This was especially serious as the bank should have applied EDD measures for high-risk or PEP accounts.

91. Other examples of poor verification practice included banks' over-reliance on undocumented 'community knowledge' and personal acquaintances, for example where a bank's CEO had personally introduced a customer.

At one bank, it appeared that many new clients were introduced by the bank's CEO, and that relevant staff did not question his judgement of these clients' integrity.

Intra-group introductions and overseas banking secrecy laws

92. We found that some banks were relying on intra-group introductions, even where they could not be satisfied that verification had been carried out to UK-equivalent standards or where they knew that underlying CDD information was inaccessible due to legal constraints in the jurisdiction where this information was held. Banks must ensure that they have access to underlying CDD documentation at all times.

Keeping CDD up to date

93. We found that more than half the banks we visited failed to review regularly and, where necessary, update customer information. In some cases, banks had never obtained formal evidence of a long-standing customer's identity and also failed to assess whether they had collected sufficient information over the course of the business relationship to meet their legal obligations. Failure to keep CDD information up to date was of particular concern where the risk associated with the relationship had changed, for example, where transactions on the account were incompatible with the CDD information on file.

Three banks added relevant information to their CDD files for the first time shortly before our visit.

3.3.3. Beneficial owners

94. Under the Money Laundering Regulations, 'beneficial owners' of bodies corporate (for example companies, trusts and charities) include any individual who ultimately owns or controls more than 25% of the shares or voting rights in the body; or otherwise exercises control over the management of the body. We were not satisfied that all banks understood their legal CDD obligations in relation to their customers' beneficial owners.

95. A third of banks in our sample failed to take adequate measures to understand and verify their customers' ownership and control structure. And when the structure appeared complex, banks rarely questioned the rationale for the complexity and few were able to provide convincing reasons for them when challenged. At least a fifth of banks visited also failed to identify indirect beneficial owners who exercised considerable control over the customer. As a result, these banks often did not appear to know who their customer's ultimate beneficial owner really was.

One bank did not accept relationships where it was not satisfied that all beneficial owners and/or controllers had been identified, even when this meant going down from the 25% identification threshold set out in the Money Laundering Regulations.

96. In addition, at a fifth of banks visited, evidence of the beneficial owners' identity was very weak, even where the money-laundering risk associated with the business relationship was high.

One bank held an account for a corporate customer whose nominal beneficial owner changed frequently and without explanation. The bank did not carry out sufficient CDD to ensure there was no money-laundering risk associated with these changes.

97. Banks can be satisfied that they know who the beneficial owner is only if they know who ultimately owns or controls the customer – either directly, or indirectly through interests in the customer's beneficial owner(s). Identifying the beneficial owner may include measures to establish whether the beneficial owner is a PEP. Failure to identify who ultimately controls the business relationship is not only a breach of the bank's legal obligations, it also prevents banks from developing a clear understanding of the money-laundering risk associated with the business relationship.

3.3.4. Identifying PEPs

98. The obligation to have risk-sensitive policies and procedures to identify whether a customer is a PEP is not an obligation to screen every customer for PEP purposes. It does, however, require banks to take measures to identify PEPs and in particular those who pose a real money-laundering risk. So, in most cases, identifying PEPs should flow naturally from a bank's normal CDD process.

One small foreign bank which dealt mainly with its country of origin relied on its business manager to identify PEPs because he 'knew every PEP in the country'. However, when pressed, he could not tell us how many PEPs there were or satisfy us about the completeness of his knowledge of relevant PEPs. The bank also dispensed with CDD measures and instead relied on the Deputy MLRO 'knowing everyone' locally.

99. Commercially available PEP databases can be a useful tool to help banks identify PEPs and other high-risk customers and some of them also provide links to external sources of information which are likely to assist banks during the CDD process. But PEP databases are not comprehensive and can vary greatly in their coverage of different geographical regions and depth of content. Relying on commercial PEP databases as the only identification tool in cases of high money laundering risk is unlikely to be sufficient and simple internet research can often yield useful results in establishing an individual's political connections, as well as other information which should be investigated during the CDD process. Banks should take this into account when considering whether their systems and controls to identify PEPs are adequate.

100. Most large banks carried out daily screening against PEP databases in order to identify new PEPs among all existing customers. Although there is no requirement to do this, many large firms commented that screening their entire customer base daily was more efficient than trying to introduce a risk-based approach to screening. However, at more than a third of smaller banks visited, there was great reliance on the knowledge of RMs or other bank staff to identify existing customers who had become PEPs when this was not realistic.

One large UK retail bank did not conduct PEP screening of its existing customer base due to the small number of foreign PEPs it had previously identified at customer take-on. However, it was currently implementing a system which would enable regular screening against a PEP database.

3.3.5. Nature and intended purpose of the business relationship

101. Obtaining information on the nature and intended purpose of the business relationship means developing a more comprehensive picture of the customer, and includes, for example, measures to establish the customer's occupation and source of funds. This kind of information is key to providing banks with a solid basis for monitoring the business relationship. It also provides banks with an opportunity to assess whether the proposed business relationship is in line with what the bank would expect, based on the outcome of its identification and verification work.

102. We found that over 40% of banks in our sample failed to take meaningful steps to obtain information on the purpose and intended nature of the business relationship. Questions about the customer's reason to bank with the firm, or a customer's request for products or services that did not seem to make economic sense, were often left unanswered. In other cases, staff accepted meaningless replies and did not challenge them.

3.3.6. Source of wealth/funds

103. Taking adequate measures to establish the source of wealth and source of funds is a legal obligation where the customer is a PEP. It is also crucial to understanding the purpose and intended nature of the business relationship. Without establishing the legitimate origin of a customer's source of wealth and source of funds, banks cannot be satisfied that they are not being used to launder the proceeds of crime including corruption. So it is essential that banks obtain meaningful information, apply risk-sensitive measures to verify this information, and challenge information where appropriate, especially where the risk associated with the business relationship is increased.

104. We were therefore concerned to find that three quarters of banks visited failed to obtain adequate information about their customers' source of wealth and the source of funds to be used in the business relationship.

> *Questions on some banks' CDD forms about high risk and PEP customers' source of wealth and source of funds were either left blank or contained meaningless information, such as 'transfer from another account', 'from business', 'money left over from shopping trips to the UK' and, in some cases, 'not known'.*

105. Some banks appeared not to distinguish between the source of wealth (ie how a customer became wealthy) and the source of funds (ie where, specifically, the funds for the business relationship originated). And we found that at nearly half the banks visited, information provided by customers, however questionable, was accepted at face value. Furthermore, a quarter of banks in our sample stopped asking questions at the first obstacle, for example where the customer explained that their command of English was insufficient to explain where their wealth had come from, or where cultural sensitivities meant 'it was unacceptable' to ask questions about the source of their private wealth and funds.

106. In other cases, banks appeared to take the view that the proceeds of crime became legitimate after a certain, and in some cases a very short, period of time. Examples included where customers had acquired substantive wealth by allegedly corrupt means, but subsequently invested the proceeds in more legitimate ventures. For more detailed examples, see the case studies in Section 6.

107. More than a third of banks visited also placed undue reliance on assurances about the source of a customer's wealth from colleagues in other parts of the same banking group, rather than seeking independent verification.

One branch of a foreign bank relied almost exclusively on the insights of one RM in another jurisdiction to dispel any concerns about the legitimacy of their customers' wealth. In one email exchange, where a London-based compliance officer attempted to follow up allegations of corruption surrounding a customer's wealth, the RM wrote that 'I don't know where the funds are coming from as I didn't know her at the time, but they are definitely hers'. This was apparently deemed a sufficient reassurance by London staff, who made no further enquiries.

108. Even where relevant information about a customer's source of wealth or source of funds was obtained, nearly three quarters of banks in our sample did nothing to verify this and too much reliance was placed on the word of customers or relationship managers, even when there were serious allegations of criminal conduct about the customer.

3.3.7. EDD

109. Banks must apply EDD measures where the risk associated with the business relationship is increased. The Money Laundering Regulations do not define EDD measures, but provide examples, in Regulation 14, as to what these might be. The central objective of EDD measures is for banks to understand better the risk associated with the customer to be able to decide whether to proceed with the business relationship, and if so, how to mitigate the associated money laundering risks.

110. Several banks gathered additional due diligence information from a variety of internal and external sources where the risk associated with the business relationship appeared increased. Most major banks in our sample commissioned intelligence reports where existing CDD information gave rise to concern, and some of them always required this in respect of customers with connections to certain higher risk countries. Against this background, we were concerned that a third of banks visited failed to analyse this additional due diligence information properly and reflect the findings in their risk assessment.

A UK branch of a foreign bank charged RMs' business units for commissioning intelligence reports. We found evidence on files that, as a result, RMs often decided against commissioning these reports.

111. At nearly a quarter of banks in our sample, adverse information about customers was often easily dismissed as political slurs, or simply ignored without appropriate further investigation. More than a quarter of them treated the

absence of criminal convictions as sufficient reason not to act on corruption allegations, even where these came from reputable sources often repeatedly and over a sustained period of time. We also found that some front-line staff, particularly RMs, dismissed or even withheld negative information where banks stood to profit significantly from the business relationship. As a result, senior management and compliance staff at around a quarter of banks in our sample were sometimes presented with an incomplete or misleading picture of the risk associated with the customer.

One bank had completed extensive EDD including an intelligence report on a potential customer. Despite the information highlighting substantive allegations relating to the customer, the bank still decided to take on the customer because no charges had been brought or convictions returned.

112. Banks should take very seriously adverse allegations against their customers in order to meet their legal and regulatory obligation to identify, assess and mitigate money laundering risk effectively and to avoid being used as a vehicle for money laundering. The extent and quality of EDD measures must be commensurate to the risk identified. Where a bank is not satisfied that it has applied all CDD measures in accordance with its legal obligations, the bank must not proceed with the business relationship.

Some banks placed undue reliance on the fact that some customers held investment visas. Investment visas are allocated on the basis of funds held in regulated financial institutions anywhere in the world; they are not an indication of the customer's integrity or the quality of AML controls in the jurisdiction where the funds are held. Banks should not, therefore, conclude that adverse allegations against customers can be disregarded simply because they hold an investment visa.

3.3.8. Record-keeping

113. Banks must keep records of information obtained in the course of their CDD work to manage the business relationship and to provide an audit trail. Adequate records can also serve as evidence that the firm has met its legal and regulatory AML obligations.

114. We told the banks selected for our thematic work before our visits that we wanted to see all CDD information for certain high-risk customers. Despite this, over a third of them were unable to access relevant information or provide us with complete sets of CDD files. Information was sometimes inaccessible 'in storage', in countries with strict banking secrecy legislation or dispersed across multiple databases; some was 'lost' or 'temporarily misplaced'. When presenting our findings to a fifth of banks in our sample, we were told that we had not seen all relevant CDD documentation about the customer relationships we reviewed. In

a small number of banks, the MLRO was unable to retrieve relevant information about the bank's high-risk customers.

115. We did, however, also find some examples of good record-keeping practice. In those firms, CDD files were well structured, comprehensive and organised. Some of them had created customer profile documents which summarised relevant information such as the risk assessment, expected account activity, and beneficial ownership, and provided an overview of any information outstanding or requiring follow-up. Some firms had sophisticated secure online systems, where all CDD information was easily accessible. We were also pleased to note that several MLROs were easily able to produce a list of known PEP and other high-risk customers. Some had compiled all relevant information, including a summary of the reason for the high risk classification and key mitigants, in a single document.

116. The ability to retrieve relevant information about high-risk customers, including PEPs, easily is an important prerequisite for managing money-laundering risk effectively.

3.3.9. Approval of business relationships

117. Effective AML systems and controls should ensure that money-laundering risk is taken into account when taking on new customers. The MLRO and, ultimately, senior management are responsible for ensuring that the bank complies with its legal and regulatory AML obligations.

Escalation

118. Under FSA rules, a director or senior manager must be allocated personal responsibility for ensuring that a bank has effective AML systems and controls. In addition, certain senior managers can be held criminally liable where the bank commits an offence under the Money Laundering Regulations, including where an offence is attributable to any neglect on their part. This means that, in order to discharge their functions effectively, relevant senior managers must be involved in decisions on entering or maintaining high-risk business relationships, including with PEPs, on a risk-sensitive basis. Under the Money Laundering Regulations, all decisions to establish a business relationship with a PEP must have approval from senior management. These decisions should be well documented.

> *At some banks, decisions about the take-on of very high risk PEP customers were automatically escalated to very senior management, including the CEO.*

119. Over half the banks visited had a clear policy whereby decisions about higher risk business relationships were escalated as appropriate. And where the risk associated with the relationship was very high, just under half the banks we reviewed referred the case to a dedicated board or compliance committee for consideration.

At more than a third of banks in our sample, committee minutes and other records of senior management approval for high risk customers were vague and did not contain sufficient detail about discussions on AML risk. In some cases, it was unclear whether serious allegations about customers had been considered at all.

120. We were not satisfied that all banks effectively implemented their own escalation policies. We found cases where Relationship Managers (RMs) had apparently allocated a low risk-rating to circumvent escalation, or where compliance sign-off had been delegated to junior members of staff even where the risk associated with the business relationship was very high. We also found examples of banks where the escalation process was ill defined, or non-existent.

At one major bank's private wealth arm, we reviewed a large selection of PEP customer files. The application forms had a money laundering section where the risk was rated as low, medium or high. Almost all the files we reviewed were ticked low – even when the files contained references to serious corruption allegations.

121. Banks should escalate decisions to establish and maintain business relationships with high risk customers to appropriate levels of senior management. Where the money laundering risk associated with the customer is very high, involvement of the most senior levels of management is appropriate. Senior management must be aware of the level of money-laundering risk the bank is exposed to and take a view whether the bank is equipped to mitigate that risk effectively.

Quality of information

122. Where decisions about customer take-on are escalated to compliance or senior management, it is essential that the documentation used as the basis for decision making provides an accurate picture of the risk to which the bank would be exposed.

123. At a quarter of banks visited, we found that information provided by RMs to senior management was often inadequate, and sometimes unbalanced or misleading. This was usually due to poor risk assessments, a lack of analysis or a lack of oversight of RMs' work. Due to the nature of an RM's role, the risk of capture or conflict of interest is high, in particular where they are rewarded for bringing in business or penalised for lost business opportunities. However, we found some banks failed to give due regard to the potential conflicts of interest arising from RMs' reward structures.

A major bank had a relationship with a former government minister from a high-risk country who had acquired significant wealth through business assets awarded to him by a former senior military officer who has been subject to very serious and credible allegations of corruption. Although the bank had generally conducted thorough enhanced due diligence, we were concerned that a four-page paper presented to a key customer approval committee failed to mention the individual's connection to the former military officer.

124. At a fifth of banks reviewed, we found that RMs omitted or downplayed negative allegations against customers in their briefings to compliance or senior management. For example, we saw some files where RMs had dismissed negative allegations about customers on the basis of the customer being 'very nice', 'trustworthy' or 'from a respectable family'. We also found information provided by RMs that focused too much on the potential profitability of the business relationship. To compound this, we found in some banks little evidence of senior management or MLROs effectively challenging the information provided by RMs.

In one bank, a member of the AML team had signed off very high-risk relationships despite knowledge of considerable negative information about the customer. In one email, he wrote 'In my view, provided there is sufficient business to justify the risk then I am happy to recommend we proceed.'

125. Other MLROs lacked the authority to challenge RMs' standard business practices effectively, even where they undermined the effectiveness of the bank's AML policies and procedures. MLROs are responsible for overseeing the bank's compliance with its anti-money laundering obligations. To this end, the MLRO must have a level of authority and independence within the bank and access to resources and information sufficient to enable him to carry out this responsibility.

3.3.10. Risk appetite, culture and resources

126. We were not confident that all banks had adequate risk-management systems in place effectively to mitigate the money-laundering risk they were prepared to take on. At more than a quarter of banks visited, the risks they sought to mitigate were of limited relevance to AML.

AML risk culture

127. In some banks, we found that the dominant culture appeared to undermine the effective implementation of AML policies. At nearly half the banks in our sample, a poor AML compliance culture and an apparent lack of leadership on AML issues from senior management were accompanied by a lack of senior management involvement in PEP and high risk customer sign-off processes. Sometimes in these circumstances, MLROs and other AML staff were operating with stretched resources, particularly in smaller banks.

At a small bank, the MLRO had several other functions to carry out. This over-stretch of his resource meant that he had never visited some branches of the bank and he told us he would need a significantly expanded team to do the required AML work effectively.

128. Generally, MLROs at larger banks had developed more specialist knowledge on AML requirements as they spent all their time on AML issues. However, we found that, at around a fifth of banks visited, Group MLROs were too remote from their business units and sometimes had a poor awareness of the group's highest risk relationships.

One MLRO told us he could not see the value in collecting CDD information because customers would be taken on even if they were subject to serious allegations of criminal activity.

The relationship between criminality risk and reputational risk

129. We were concerned that senior management at a quarter of banks visited (mostly private banks or the private banking arms of major banks) appeared to treat money-laundering risk as a reputational risk issue only. In these banks, senior management attached greater importance to the risk that a customer might be involved in a public scandal, than to the risk that the customer might be corrupt or otherwise engaged in financial crime, and using the bank to launder criminal proceeds. At around a third of banks in our sample, serious allegations against customers were often discounted where criminal charges were unlikely to be brought, for example because the customer maintained good relations with allegedly corrupt regimes. As a result, senior management were willing to take on extremely high-risk customers, including where evidence appeared to point towards the customer being engaged in financial crime, as long as they judged the immediate reputational risk to be low.

One firm told us they might have PEP customers who would be above their risk appetite, but they did not have formal criteria in place to decide how much risk they were prepared to take on.

130. In some banks, money-laundering risk appeared to be treated as a regulatory risk issue, with senior management apparently willing to take on extremely high-risk customers. In others, money laundering risks were given less weight as long as the credit risk was within risk tolerance and the business relationship was likely to be profitable. An exclusive focus on reputational, regulatory or credit risks rather than money-laundering risk is unlikely to be conducive to banks understanding and effectively managing their money-laundering risk.

At more than a fifth of banks in our sample, high money-laundering risk relationships were considered by a regulatory and/or reputational risk committee rather than an AML committee.

3.3.11. Customer take-on – examples of good and poor practice

Good 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.
- Having all new PEP or other high-risk relationships checked by the MLRO or the AML team.
- 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.
- Using, where available, local knowledge and open source internet checks to supplement commercially available databases when researching potential high risk customers including PEPs.
- Having clear risk-based policies and procedures setting out the EDD required for higher risk and PEP customers, particularly in relation to source of wealth.
- Effective challenge of RMs and business units by banks' AML and compliance teams, and senior management.
- Reward structures for RMs which take into account good AML/compliance practice rather than simply the amount of profit generated.
- Clearly establishing and documenting PEP and other high-risk customers' source of wealth.
- 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.
- Understanding and documenting ownership structures complex or opaque corporate structures and the reasons for them. Face-to-face meetings and discussions with high-risk and PEP prospects before accepting them as a customer.
- Making clear judgements on money-laundering risk which are not compromised by the potential profitability of new or existing relationships.

- Recognising and mitigating the risk arising from RMs becoming too close to customers and conflicts of interest arising from RMs' remuneration structures.

Poor practice

- Failing to give due consideration to certain political connections which fall outside the Money Laundering Regulations 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.
- Poor quality, incomplete or inconsistent CDD.
- Relying on Group introductions where overseas standards are not UK-equivalent or where CDD is inaccessible due to legal constraints.
- Inadequate analysis and challenge of information found in documents gathered for CDD purposes.
- Lacking evidence of formal sign-off and approval by senior management of high-risk and PEP customers and failure to document appropriately why the customer was within AML risk appetite.
- Failing to record adequately face-to-face meetings that form part of CDD.
- Failing to carry out EDD for high risk/PEP customers.
- Failing to conduct adequate CDD before customer relationships are approved.
- Over-reliance on undocumented 'staff knowledge' during the CDD process.
- Granting waivers from establishing a customer's source of funds, source of wealth and other CDD without good reason.
- Discouraging business units from carrying out adequate CDD, for example by charging them for intelligence reports.
- Failing to carry out CDD on customers because they were referred by senior managers.
- 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.
- Allowing accounts to be used for purposes inconsistent with the expected activity on the account (eg 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.

3.4. Enhanced monitoring of high-risk relationships

131. The Money Laundering Regulations require that banks conduct ongoing monitoring of the business relationship with their customers and that they conduct enhanced monitoring for PEP customers. Banks should scrutinise transactions using a risk-based approach to ensure that they are consistent with their recorded knowledge of the customer, including their personal and business activities, risk profile and source of wealth and funds. Good transaction monitoring depends on having completed good initial CDD work. Where CDD has not been properly completed, documented or kept up to date, effective monitoring becomes harder. We found that a third of banks visited had serious weaknesses in CDD on expected account activity.

132. Ongoing monitoring is necessary to identify unusual activity and transactions and to seek a legitimate explanation for it. If no such explanation can be found or if the customer is not willing to provide such an explanation, banks should consider whether to continue the relationship and whether the facts amount to a suspicion of, or reasonable ground to suspect, money laundering which must be reported to SOCA. Banks' systems and controls should identify unusual transactions or trends for further examination. A person or persons with adequate knowledge, ability and experience to assess whether further action should be taken should

then review these transactions. Ultimately the firm's MLRO must assess whether it should make a SAR to SOCA.

A personal savings account opened at a small foreign bank showed an expected income of £20k to £30k from the business of the account holder as a restaurateur. Less than three months later, a significant deposit of £150k was made with over £3m deposited over the next three years. During this time, these transactions were not identified as unusual and no explanation was sought from the customer.

133. Banks which have high-risk customers, including PEPs, must carry out enhanced monitoring throughout the relationship which will be beyond that needed for normal retail banking purposes.

134. There was a wide variation on the quality of monitoring carried out at the smaller banks covered by our review. For example, one small bank had not taken account of any developments in the AML framework over the past few years, including the introduction of the Money Laundering Regulations 2007. The bank had not applied a risk-based approach and did not carry out any effective monitoring, even for higher risk customers. As a result, there was no evidence of discussion of unusual transactions or evidence of management challenge and no regular reviews of high-risk relationships. In contrast, other small banks had a good risk assessment and risk-based monitoring with clear documentary evidence of daily transaction monitoring, management challenge and regular reviews.

The importance of good challenge is key. At one regional bank the Deputy MLRO reviewed all PEP transactions on a daily basis. But a review of files dating back to 2002 showed that there had been no challenge of activity which was out of line with anticipated volumes.

3.4.1. Transaction monitoring

135. We found the most effective ongoing monitoring regimes combined a rules-based system to generate alerts when activity on the account was unexpected or indicated potential money laundering with regular independent reviews of the customer relationship.

136. Transaction monitoring does not necessarily require sophisticated electronic systems. The type of transaction monitoring systems and processes required by banks depends on the nature, scale and complexity of their activities. However, a well-designed transaction monitoring system should take into account a bank's particular business model and assess the frequency, value and patterns of transactions in line with the associated customer and product risk. We recognise, though, that for some business activities such as investment banking, it is more difficult to assess a 'normal' pattern of transactions.

A small European bank set clear parameters on its accounting system of expected income and outflows on customer accounts. If these limits were exceeded, the account operator needed to fill in a pop-up box to explain the transaction. This audit trail was available for the internal auditor and MLRO to use for the purposes of quality assurance and suspicious activity reporting.

137. The types of transaction monitoring systems seen during our review varied from fully manual analysis of all transactions by staff to complex, risk-based analysis of system-generated alerts coupled with staff awareness of potentially suspicious activities. The small banks which relied on manual monitoring varied considerably: at least one small bank conducted no transaction monitoring at all while others required RMs to explain in writing the reason for all transactions.

At a small regional bank the transaction monitoring system had been configured to identify certain generic 'scenarios' but it did not compare expected activity with actual activity on individual accounts, even though this information was readily available.

138. We found larger banks in our sample tended to use rules-based automatic monitoring systems. These banks usually had clear processes to fine-tune the system rules and keep the number of false positives to a manageable level. It is important in these circumstances that the money-laundering risk, not the available resource, is the key driver in how rules are calibrated.

139. Automated systems add value by being able to deal with large volumes of transactions but the parameters need to be carefully set. Banks should broadly understand how their systems work, the rationale and appropriateness of rules, and not rely unquestioningly on default system outputs.

The role of RMs in the transaction monitoring process

140. RMs should be a bank's first line of defence in managing and controlling money laundering or terrorist financing risk because they develop strong personal relationships with their clients, which can facilitate the collection of CDD information both at customer take-on and during the course of the relationship. Banks, however, should ensure that RMs do not become too close to the customer or motivated by financial incentives which may compromise a bank's ability to meet its AML obligations.

At a small private bank, RMs were well-trained and aware of the need to identify unusual transactions. They had notified their customers of this requirement so that customers were pre-notifying the RMs of certain transactions they wished to make. There were also notes on file from RMs setting out the gaps in their knowledge of customers and clear evidence that these were followed up with customers at the next meeting with corroborating evidence gathered as necessary.

141. We found there was considerable variation in how alerts were dealt with and there were some banks where complete reliance was placed on an RM's explanation of why an unusual, potentially high-risk transaction was not suspicious. In these circumstances, there is a risk that RMs are able to pass off transactions as 'normal' when, in fact, the activity may be suspicious.

142. We found, at nearly a quarter of banks in our sample, that when there was an unusual transaction, the RM or customer was asked for a response but no independent corroboration was requested or received, even when the customer was the subject of serious allegations of criminal activity. In addition, at more than a third of banks visited, we found that compliance staff did not sufficiently challenge RMs or customers and often accepted poor explanations of potentially suspicious activities.

3.4.2. Regular reviews

143. In addition to transaction monitoring, it is good practice for staff independent of the business to review the conduct and development of higher risk and PEP relationships from an AML perspective, at least annually. And when there has been a significant change to the relationship, it is good practice for annual reviews to be subject to the same approval processes as new customers.

At a major international bank, senior management require all business areas to gather information on PEP clients for a regular annual review. The process forces business areas to justify the retention of that PEP client with reference to the legitimacy of the clients' source of wealth and source of funds. The senior management team that includes the senior business and compliance representatives and the CEO then review all cases in detail to determine the true risk appetite of the firm.

144. Generally, we found that the risk-based approach to customers drove the frequency of reviews. The most frequently seen model was to score customers as high, medium or low risk, with reviews expected every one, two or three years respectively. Under these models, PEP customers were usually considered to be high risk.

One large bank planned to introduce additional high-risk customer reviews when there was a 'trigger event'. Examples of trigger events included Suspicious Activity Reports, a change of address, the addition of a new party to the account or the customer taking out a new product. The RM would be responsible for undertaking a review and this was then signed off by Compliance.

145. At nearly a third of banks in our sample, we found that RMs carried out annual reviews for customers but there was often inadequate management oversight and inadequate challenge of the findings. In some cases, the reviews were being treated as a 'tick-box' exercise and not completed properly. It was clear from many of our file reviews that some annual reviews were exact copies of the previous year's with no new information added, but had nevertheless been signed off by compliance staff or AML teams.

At the private banking arm of a major bank, we noted that regular reviews for very high-risk customer relationships were not usually approved by senior management and in some cases no-one apart from the RM appeared to have been involved in the review.

146. At nearly half the banks we visited, there was no evidence of any PEP or high risk customer files being reviewed, as required in many cases by the banks' own policies.

At one bank, an annual review form for a high-risk customer relationship simply stated 'unable to get new info'.

3.4.3. Enhanced monitoring of high risk relationships – examples of good and poor practice

Good practice

- Transaction monitoring which takes account of up-to-date CDD information including expected activity, source of wealth and source of funds.
- Regularly reviewing PEP relationships at a senior level based on a full and balanced assessment of the source of wealth of the PEP.
- Monitoring new clients more closely to confirm or amend the expected account activity.
- A risk-based framework for assessing the necessary frequency of relationship reviews and the degree of scrutiny required for transaction monitoring.
- Proactively following up gaps in, and updating, CDD during the course of a relationship.

- Ensuring transaction monitoring systems are properly calibrated to identify higher risk transactions and reduce false positives.
- 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.
- A good knowledge among key AML staff of a bank's highest risk/PEP customers.
- 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.
- Global consistency when deciding whether to keep or exit relationships with high-risk customers and PEPs.
- Assessing RMs' performance on ongoing monitoring and feed this into their annual performance assessment and pay review.
- Lower transaction monitoring alert thresholds for higher risk customers.

Poor practice

- Failing to carry out regular reviews of high-risk and PEP customers in order to update CDD.
- Reviews carried out by RMs with no independent assessment by money laundering or compliance professionals of the quality or validity of the review.
- Failing to disclose suspicious transactions to SOCA.
- Failing to seek consent from SOCA on suspicious transactions before processing them.
- Unwarranted delay between identifying suspicious transactions and disclosure to SOCA.
- Treating annual reviews as a tick-box exercise and copying information from the previous review.
- Annual reviews which fail to assess AML risk and instead focus on business issues such as sales or debt repayment.
- Failing to apply enhanced ongoing monitoring techniques to high-risk clients and PEPs.
- Failing to update CDD based on actual transactional experience.
- Allowing junior or inexperienced staff to play a key role in ongoing monitoring of high-risk and PEP 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.

4. Findings – correspondent banking

4.1. What is correspondent banking?

147. Correspondent banking is defined in the JMLSG Guidance as the provision of banking services by one bank (the 'correspondent') to an overseas bank (the 'respondent') to enable the respondent to provide its own customers with cross-border products and services that it cannot provide itself, typically because it lacks an international network.

148. Correspondent banking activity can include establishing accounts, exchanging methods of authenticating instructions (eg by exchanging SWIFT keys) and providing payment or other clearing-related services. A correspondent relationship can be based solely on the exchange of test keys, with cover for direct payment instructions being arranged through a third bank for credit to the correspondent's/respondent's own account in another jurisdiction. Activity can also encompass trade related business and treasury money market activities, for which the transactions can be settled through the correspondent relationship.

149. A correspondent is effectively an agent for the respondent and executes/processes payments or other transactions for customers of the respondent. The underlying customers may be individuals, corporates or even other financial services firms. Beneficiaries of transactions can be customers of the correspondent, the respondent itself or, in many cases, customers of other banks.

4.2. Money-laundering risks in correspondent banking

150. The facility for banks to process transactions with speed, accuracy and efficiency via correspondent banking relationships does, however, lead to money laundering risk. The vast numbers of payments being processed through the system, and the speed at which such payments must be made, makes it extremely difficult to identify and intercept suspicious payments.

151. The JMLSG Guidance sets out very clearly the money-laundering risks inherent in correspondent banking. In particular, correspondents often have no direct relationship with the underlying parties to a transaction and are therefore not in a position to verify their identities. In addition, they often have limited information regarding the nature or purpose of the underlying transactions, particularly when processing electronic payments or clearing cheques. It is therefore primarily non-face-to-face business and must be regarded as high risk from a money laundering and terrorist financing perspective. So we expect firms

undertaking such business to apply enhanced customer due diligence measures on a risk-sensitive basis.

152. If banks fail to implement appropriate controls for accepting correspondent banking relationships, this can give banks with inadequate AML systems and controls access to the international banking system.

4.3. New business origination and strategy

153. We expect banks to make proper assessments of the money-laundering risks associated with individual correspondent banking relationships and have documented procedures in place to manage such relationships.

154. We found many different reasons why banks provide correspondent banking services to their customers. In many of the small foreign banks we visited, the main reason was to provide banking services to customers of their parent bank's group who want to make payments in the UK. Others had relationships with banks in countries with which their home country traditionally conducted trade finance business.

155. We noted that few larger banks were looking to expand their correspondent customer base and were instead focusing attention on developing the services offered to existing customers. One major bank that had recently been through a merger was cross-selling its product range to acquired customers. At many larger firms the focus was on countries' top-tier banks as it was considered that the control frameworks were better developed and the risks of money laundering reduced. This kind of approach had led to a reduction in the number of correspondent accounts in the past few years.

One major bank had undertaken a major review of correspondent relationships and SWIFT keys post 9/11. Approximately 500 of 2,500 were closed down; 400 on economic grounds and the remaining 100 for AML reasons.

156. One of the key considerations, particularly for larger banks, in establishing and maintaining correspondent accounts is the profitability of an account once the necessary operating and compliance costs have been factored in.

One firm applied two key filters to determine the viability of its correspondent relationships. The first was a country revenue filter, which took account of the total revenue the firm could obtain from a country where it has no presence. An example of this we were given was a country with total revenue potential of $50k. The second was a filter applied in response to the increasing cost of compliance, which dictated that a relationship must generate at least $50k of revenue. On this basis the two relationships that this bank had in this country were closed down.

157. However, some banks also considered reputational/franchise issues and were wary of withdrawing from certain countries when they wanted to be seen as a solid bank partner and provider. In these circumstances, long standing correspondent relationships were sometimes allowed to continue even if they generated little revenue.

The same bank that exited its correspondent relationships in one country (see above) decided its two correspondent relationships in a neighbouring country, while having low business potential, were worth continuing because those two banks accounted for nearly all the available business there.

4.4. Risk assessment of respondent banks

158. A number of risk indicators should be considered both at the start of a relationship, and on a continuing basis after that, to determine the levels of risk-based due diligence that should be undertaken.

159. The banks we visited had relationships with respondents across the globe covering many different types of banking activity which gave rise to varying money laundering risk. We expect firms to use a risk-based approach to target banks and activities that present the greatest risks; this will enable them to make the best use of resources and achieve optimum risk mitigation.

160. One key area for firms to consider is the location of the respondent and/or where its parent is based. Some jurisdictions, such as many members of the Financial Action Task Force (FATF), have more robust regulatory environments and should be lower risk. Conversely, other jurisdictions are recognised internationally as having inadequate anti-money laundering standards, insufficient regulatory supervision and/or presenting greater risk of financial crime.

Publicly available information from relevant national government bodies and non-governmental organisations, including the Transparency International CPI and FATF mutual evaluations may be useful in assessing the risk posed by a respondent. Such information should ideally be objective; verifiable; recently published; and where possible, international in scope.

4.4.1. Examples of risk-assessment methodology

161. We found various methods of assessing risk at the banks we visited. The objectives were generally to:

- identify as early as possible suspicious activity and/or high risk customers;
- prioritise high-risk customers and transactions for review and investigation;

- ensure that resources were focused on higher risk relationships and transactions; and
- ensure AML work on correspondent banking was consistent and high quality on a global basis.

162. One major bank had put in place a risk matrix that rated countries according to their perceived risk of money laundering and terrorist financing. Examples of country risk factors that usually led to respondents being designated high country risk included: countries with inadequate or no AML laws or regulations; countries designated as being of 'primary money laundering concern' by the US or UK governments; countries subject to financial sanctions; offshore financial centres and countries designated as tax havens by the OECD or G20; and drug source or drug transit countries. This assessment, in conjunction with customer and product risk factors, generated a low, medium or high risk rating for clients that drove the frequency of the customer review process.

163. Another major bank assessed all correspondent banking relationships as high risk and required EDD to be performed for all entities. Here, a simplified approach to risk assessment was confined to ownership structure (listed on a stock exchange versus non-listed) and country of domicile.

It is good practice for firms to find out whether publicly-owned respondents are traded on a recognised market or exchange in a country with a satisfactory regulatory regime or, for privately owned respondents, to establish the identity of their beneficial owners and controllers.

164. At a third major bank, each respondent was allocated a risk score, determined by an overall assessment of six risk factors: country; ownership/management structure; products/operations; transaction volume; market segment; and the quality of its AML programme. The assessor then took into account, for example, whether there was material adverse information known about the respondent and could make adjustments to ensure that the overall risk score took account of whether the respondent's customers included certain higher risk business types like money service businesses, offshore banks or internet service providers. The client's risk score drove the frequency of reviews, with annual review for high risk, reviews every two years for medium risk and every three years for low risk.

At one small bank, there was no evidence from our file reviews that respondents had been risk rated. It is essential that firms have procedures in place for accepting new respondents and that CDD and ongoing monitoring are commensurate with the risk profile.

A small foreign bank had no written policies or procedures for dealing with and managing the risks arising from correspondent banking. We were told that the bank's parent was working on a group-wide AML process for correspondent banking, but the UK business knew no details of its content or its expected implementation date.

4.4.2. Risk assessment of respondent banks – examples of good and poor practice

Good practice

- Regularly 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.
- More robust monitoring respondents identified as presenting a higher risk.
- Risk scores that drive the frequency of relationship reviews.
- Taking into consideration publicly available information from national government bodies and non-governmental organisations and other credible sources.

Poor practice

- Failing to consider the money-laundering risks of correspondent relationships.
- Inadequate or no documented policies and procedures setting out how to deal with respondents.
- 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.
- 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.

4.5. Customer take-on

4.5.1. Responsibility for carrying out CDD

165. All correspondent banking relationships with respondents must be subject to an appropriate level of CDD. Firms should assign clear responsibility for this task and there should be some form of independent review to ensure that those responsible are following agreed standards.

166. At most of the firms that we visited, ultimate responsibility for CDD rested with the business, specifically RMs. Some banks managed respondent relationships from the UK; whereas others felt it was necessary for its RMs to be located closer to respondents in order to better understand the regulatory environment and the risks involved.

167. Some banks operated 'hubs' to achieve an even broader correspondent banking footprint. For example one firm had a hub in South Africa which serviced respondent accounts from the Sub-Sahara region. However, not all banks adopted this approach to gathering CDD information.

> *One major bank had decided to remove CDD gathering responsibilities entirely from RMs and let them concentrate on 'what they were good at; namely getting new business'. At this bank, the AML team was responsible for carrying out a desktop review of the respondent and having an extensive discussion on AML with the respondent's Head of Compliance or MLRO. The AML team then documented this conversation and ensured that all necessary information had been received.*

168. Many of the smaller foreign banks which tended to conduct most of their correspondent banking business with banks in their home country used RMs at their parent bank to service respondents. As a result, they often relied on their parent banks to gather CDD information. However, where banks use this approach, we expect them to understand and have access to the CDD collected on their behalf.

> *One bank whose parent was located in the Middle East had no knowledge of the CDD on respondent accounts that had been carried out on its behalf by its parent.*

4.5.2. The quality of CDD

169. The quality of CDD carried out on respondents was variable but, generally, we found the CDD carried out by larger banks was stronger. This was usually because these banks regarded visits by relationship managers to respondents as

an essential part of CDD and were able to gather more information and be better informed about a respondent as a result.

At one major bank, comprehensive CDD forms covered, in great detail: client details; ownership and management; products and offerings; transaction volumes and values; client market segments; client reputation; additional information for higher risk respondents; AML discussions with higher risk clients; and the respondent's AML policies and procedures. We were advised by this bank that it could take up to six months to obtain all the necessary CDD and, in the meantime, the relationship was 'on ice'.

170. However at several banks, the RM's evaluation of a respondent was often far more business-oriented than AML-focused. We expect those responsible for carrying out CDD to be making proper assessments of the AML risks of respondent banks and not treating the CDD process as a 'paper gathering exercise'. There were indications that some banks may need to enhance training for RMs in this area.

171. At some of the smaller banks, the level of due diligence on respondents was inadequate and, in some cases, absent. These banks failed to obtain information about, and assess, the respondent's regulatory status, the effectiveness of the respondent's AML systems and controls, the effectiveness of the AML regime in the respondent's home country or the expected turnover of the account.

In several smaller banks, a tick-box approach to CDD was noted, and there was no obvious assessment of the information collected; there was also over-reliance on the Wolfsberg Group AML Questionnaire, which gives only simple 'yes' or 'no' answers to basic AML questions, without making use of the Wolfsberg Principles on correspondent banking.

172. At these firms we felt that a thorough overhaul of client due diligence was required as most of the respondents were from high-risk countries and the current standard of due diligence was very poor. Where firms fall substantially below our expectations on gathering appropriate levels of client due diligence, we will consider appropriate further regulatory action.

One bank told us that CDD files for all its respondents had been misplaced before our visit and the Head of Correspondent Banking could not explain how the bank managed its higher risk respondents.

Assessing overseas AML regimes

173. When assessing the level of CDD to be carried out on particular respondents, banks should consider the primary regulatory body responsible for overseeing or supervising the respondent and the quality of its supervision. This is an important part of the due diligence process and may alert firms to previous

criminal or regulatory action against respondents. However, we found that the extent to which judgements about the quality of AML oversight by authorities in different jurisdictions had been considered varied considerably between the firms that we visited.

174. At many smaller banks, there was no evidence that any assessment had been made of the quality of AML supervision to which its respondents were subject. However, some of the larger firms took more effective steps to assess this. The best files we reviewed demonstrated detailed discussions with the local regulator about the AML framework. However, this was sometimes inconsistent. For example, at one major bank, a number of CDD files for respondents from the Asia-Pacific region contained no information about AML oversight by the regulator and instead contained printed internet extracts which were all dated after we had selected our files for review.

We were impressed that one major bank always met the local regulator and, in some countries, also called on the Financial Intelligence Unit and relevant government departments in order to make a better assessment of a country's AML regime. We saw evidence that they had entered into detailed discussion of the AML regime; fines; censures of particular banks; level of AML compliance of banks; the main money laundering risks (tax evasion, corruption, drug trafficking etc) that are faced and how banks are controlling those risks; audit; and training on AML compliance.

175. There are significant benefits to be gained from banks engaging with overseas regulators and we would recommend that firms consider this. Where banks do conduct meetings with overseas regulators, we expect, of course, that they make a proper assessment of information obtained and follow up where issues have been identified.

Assessing respondents' AML systems and controls

176. Other areas that banks should consider when entering into correspondent banking relationships include the nature of that respondent's AML controls and the extent to which they are globally applied. This is because, if the respondent is not adequately regulated for AML purposes or required to verify the identity of its customers, the JMLSG Guidance states that the correspondent is required to undertake EDD to obtain, and most importantly assess the effectiveness of, the respondent's AML policy. It is also good practice for firms to make an assessment of a respondent's approach to CDD and ongoing monitoring systems and controls.

One large bank told us they may read prospective respondents' AML policies and procedures but told us 'we are struggling with this right now'.

177. Once again, we saw a marked variation in the extent to which respondents' AML controls were considered. In many cases, the banks we visited had collected AML policies from their respondents but it was not always clear whether or how they were formally assessed.

One major bank was undertaking a four-year rolling programme of compliance visits to all their respondent firms. At the time of our visit, this bank had visited 670 banks in 78 countries and it was clear that these visits had given them a good understanding of the AML controls at respondent banks, as well as a good understanding of their business. Discussions covered the respondent's background, size, numbers of customers, history, main income generators, domestic and international business, ownership, connections with PEPs, AML policies, procedures and associated legislation, suspicious transactions and suspicious activity reporting in the past 12 months, relations with the regulator (including regulatory action) and membership of any relevant trade associations. We were impressed with the detailed level of AML discussion reflected in some of the CDD files we reviewed.

178. Many banks aimed to capture views and opinions on respondents' AML control frameworks via local expert knowledge derived from personal or telephone contacts, often from another part of the banking group, in the respondent's home country. However, some banks acknowledged they were still not consistent enough globally.

One major bank exchanged letters with respondents setting out sanctions policy (including sanctions lists screened) and details of systems used for sanctions screening. This enabled them to gauge respondents' levels of sanctions compliance and establish what business, if any, they did with sanctioned countries. The same bank also established how the respondent managed its own correspondent banking relationships and what audit processes and training were in place.

179. Consistent with correspondent banking CDD standards more generally, smaller banks often had an inadequate, 'tick-box' approach to assessing respondents' systems and controls. Although several smaller banks had received copies of the Wolfsberg Group AML questionnaire from respondents, most had not sought more substantive, narrative information about respondents' AML controls. This made it difficult for these banks to make any qualitative assessment of their respondents' AML frameworks.

At one small bank, we noted that there was very little other information on file. For example, apart from a Wolfsberg questionnaire dated June 2010 (ie after the bank knew of our impending visit), the most recent paper on the file for one respondent bank was dated 1995.

Another small bank had made no assessment of its respondents' AML policies and procedures because the London-based branch manager who was responsible for opening such accounts 'knew the banks personally'.

180. However, one small foreign bank showed it was possible for a smaller bank to assess respondents' AML systems and controls in a well-structured, thorough manner. This bank had visited all the respondents in its home country as part of a week long AML-specific visit. A comprehensive report of each respondent's AML systems and controls was produced and contained good quality, well-informed narrative covering customer identification; transaction monitoring; suspicious activity reporting; staff training; bureau de change business; FATF Special Recommendation VII; PEPs; and independent internal and external audit reviews.

181. Other small banks should consider a similar approach to CDD for respondent banks on a risk-sensitive basis. In many cases, this should not be particularly onerous because, as mentioned before, most small banks tended to have the vast majority of their correspondent relationships with banks from a small number of countries, generally in the same region.

Understanding ownership and connections with PEPs

182. Banks should understand the ownership structures of respondents and, where appropriate, identify beneficial owners and/or controllers, their sources of wealth and background, including any political connections. Most banks we visited used commercially available databases to screen respondents and their key staff for sanctions and PEP purposes. However, at some of the smaller banks there was no PEP screening carried out on shareholders and directors of respondents.

Our file review at one bank with a respondent based in a very high-risk country revealed that one of the shareholders was an adviser to a government ministry but this had not been identified by the bank or factored into the respondent's risk score. At another bank we found that screening of signatories had taken place just one week before our visit; and for two relationships potential PEPs had been identified but this had not been followed up.

183. In general, we found that a more risk-based approach is required where PEPs direct, own or control respondent banks. We found that some banks were not managing the risk that some respondents could be influenced by allegedly corrupt PEPs, increasing the risks of these banks being used as vehicles of corruption and/or money laundering. However, we also recognise that there may be

circumstances where a PEP is involved with a bank but his/her level of influence is diluted and/or otherwise lower risk; for example, if a PEP is a non-executive director on a large Board of Directors or if the bank is in a country which is lower risk from a corruption perspective.

One major bank had a relationship with a respondent connected with several PEPs from a high risk country through management and ownership. The bank's CDD file identified that a PEP who co-owned the majority stake in the respondent bank had previously been implicated in a serious bribery scandal. However, an RM's assessment of this information in 2010 simply concluded 'I suggest to keep the relationship' with no reasons given for this decision.

CDD on respondents from the same group

184. We expect firms to carry out adequate, risk-based CDD on parent banks and/or group affiliates with whom correspondent relationships are established. This is particularly important when the bank is in a higher risk country or there are other factors which increase the risk of money laundering.

185. However, the level and scope of CDD conducted on group relationships, particularly by smaller foreign banks, varied considerably. For example, one bank's CDD on respondents from its own banking group (which were all based in high risk countries) was patchy, with some CDD documentation missing and no indication of expected account activity. Conversely, the bank's one non-group relationship had been subject to a reasonable level of client due diligence, despite the fact that it had a similar risk profile to, and was based in the same high risk country as, its other respondents.

Consistency issues

186. Interestingly, there was sometimes a marked regional variation in the quality and scope of CDD undertaken by banks on respondents from different parts of the world.

A major bank told us about logistical and language challenges when carrying out CDD on respondents in one country. When conducting CDD on one respondent, the bank had used a telephone conference with support from its local office but was still awaiting much CDD information from the respondent. It was therefore difficult for them assess the risk associated with the respondent.

187. Banks should ensure through training, compliance monitoring and quality assurance that CDD standards are consistent with risk-based policies and procedures.

4.5.3. Approval of respondent relationships

188. At many smaller banks where CDD information was collected by RMs, we found that there was often a lack of EDD on higher risk files. This may have been because the RMs were inclined to take a less rigorous approach in order to speed up the client acceptance process.

189. To manage the risk of taking on respondent relationships that present an unacceptable level of risk, firms should encourage formal approval of new relationships (and reviews of existing relationships) by appropriately senior management, independent of the business area.

190. Most banks did require approval of respondent relationships from outside the RM's business unit, usually by compliance, risk, the CEO, or a committee including representatives from these business areas.

> *At one small foreign bank, CDD carried out by RMs was sent to compliance for sign-off. The compliance team supplemented the RM's CDD work by carrying out searches on principal owners and controllers (for PEP and sanctions identification purposes). Finally, the checklist was signed off by the Head of Correspondent Banking and the MD.*

191. However, despite the fact that many firms had identified some correspondent relationships as high risk, there was a lack of evidence of formal senior management sign-off at some banks.

> *There was no senior management sign-off of high risk correspondent banking relationships at several banks despite their AML policies stating that new correspondent bank relationships should be signed off by the CEO.*

192. It is good practice for banks to demonstrate through commentary on CDD files that senior management have considered money-laundering risks, as well as the rationale for opening such accounts.

> *At one major banking group, when all CDD documentation was collected for prospective correspondent banking relationships, they were referred to a senior management committee chaired by the CEO of the EMEA region which included the Head of Legal and Head of Risk. The EMEA Head of Banking and AML Compliance presented to this committee.*

4.5.4. Customer take-on – examples of good and poor practice

Good practice

- Assigning clear responsibility for the CDD process and the gathering of relevant documentation.

- EDD for respondents that present greater risks or where there is less publicly available information about the respondent.
- 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.
- Screening the names of senior managers, owners and controllers of respondent banks to identify PEPs and assessing the risk that identified PEPs pose.
- Independent quality assurance work to ensure that CDD standards are up to required standards consistently across the bank.
- Discussing with overseas regulators and other relevant bodies about the AML regime in a respondent's home country.
- Identifying risk in particular business areas (eg informal value transfer such as 'hawala', tax evasion, corruption) through discussions with overseas regulators.
- Visiting, or discuss with, respondent banks to discuss AML issues and gather CDD information.
- Gathering information about procedures at respondent firms for sanctions screening and identifying/managing PEPs.
- Understanding respondents' processes for monitoring account activity and reporting suspicious activity.
- 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.

Poor practice

- Inadequate CDD on parent banks and/or group affiliates, particularly if the respondent is based in a high-risk jurisdiction.
- Collecting CDD information but failing to assess the risks.
- Over-relying on the Wolfsberg Group AML questionnaire.
- Failing to follow up on outstanding information that has been requested during the CDD process.
- Fail to follow up on issues identified during the CDD process.
- Relying on parent banks to conduct CDD for a correspondent account and taking no steps to ensure this has been done.
- Collecting AML policies etc but making no effort to assess them.

- Having no information on file for expected activity volumes and values.
- Failing to consider adverse information about the respondent or individuals connected with it.
- No senior management involvement in the approval process for new correspondent bank relationships or existing relationships being reviewed.

4.6. Ongoing monitoring of respondent accounts

4.6.1. Transaction monitoring

193. Transaction monitoring of respondent accounts can help mitigate the money-laundering risks arising from correspondent banking activities. Depending on the nature and scale of a bank's correspondent banking activity, automated AML transaction monitoring systems may be appropriate. The JMLSG Guidance suggests the following good practice when carrying out automated transaction monitoring of correspondent banking relationships:

    - **Anomalies in behaviour** – monitoring for sudden and/or significant changes in transaction activity by value or volume.
    - **Hidden relationships** – monitoring activity between accounts and customers (including respondents and their underlying customers), and identifying common beneficiaries and remitters amongst apparently unconnected accounts/respondents. This is sometimes known as 'link analysis'.
    - **High-risk geographies and entities** – monitoring for significant increases of activity or consistently high levels of activity with (to or from) higher risk countries and/or entities.
    - **Other money-laundering behaviours** – monitoring for activity that may, in the absence of other explanation, indicate possible money laundering, such as the structuring of transactions under reporting thresholds, or transactions in round amounts.
    - **Other considerations** – to facilitate the monitoring techniques above, transaction monitoring systems should allow banks to apply different thresholds against customers that are appropriate to their particular risk category.

194. Transaction monitoring was one of the areas that banks struggled with most in dealing with respondents. We accept this can be a challenge for banks due to often erratic, yet legitimate, flows of funds. In addition, banks often needed to rely ultimately on the explanations of unusual transactions given by respondents and these can be difficult to corroborate.

195. Nevertheless, we found many banks did not have any systems in place to monitor the activity of their respondents. For example, one foreign bank admitted to us that transactions over respondent accounts are monitored for sanctions purposes but not for AML purposes. At another small bank, transaction monitoring was mainly done from a credit, rather than an AML, perspective.

196. One of the major difficulties for banks arose from a lack of CDD on expected levels of activity on respondent accounts.

> *Many banks' files contained only vague explanations of expected activity which made it difficult for the firm to identify unusual transactions.*

197. In addition, we found that, when larger banks used transaction monitoring systems, there were often few detection scenarios specific to correspondent banking.

> *One major bank ran six automated detection scenarios for all of its transaction services business. However, the only scenario directly relevant to correspondent banking was 'recurring originator/beneficiary'.*

198. Examples of good and poor practice in relation to transaction monitoring for high risk customers, including respondent banks, can be found in Section 3.4.3.

4.6.2. Regular reviews of respondent accounts

199. CDD information should be reviewed on a periodic basis to identify changes in business ownership and the status of respondent banks. This is to ensure that accounts continue to be used in line with agreements made and that risk categorisations remain valid.

200. Many banks had designated specific review periods depending on the risk rating of a particular relationship. We found that most relationships considered to be high risk were reviewed at least annually; medium risk usually every one-two years and low risk every two-three years.

201. A number of banks had systems in place to generate alerts to relevant RMs to commence the periodic review process, which was usually done via telephone discussions between RMs and key AML staff at the respondent.

> *One major bank kept a diary which, every month, brought up a list of correspondent banking relationships for review within the next two months. The risk management team monitored this diary centrally to ensure reviews happened.*

202. We were impressed with the level of detail that went into regular reviews of correspondent relationships at some of the major banks visited. The type of information routinely assessed at these banks included:

- whether there was sufficient economic justification for maintaining the relationship;
- a review of account activity since the last review and numbers of SWIFT messages;
- refreshed database and searches to identify changes at the respondent (including to the Board) and individuals/entities connected with the respondent who had PEP connections or were on relevant sanctions lists;
- proof of listing, confirmation of authorisation and any changes to legal status;
- whether Group AML statements and questionnaires had been obtained from the respondent and qualitative assessment of these documents; and
- money-laundering alerts for the relationship in the preceding period.

203. However, there were also weaknesses at other banks. For example, at one small foreign bank which had conducted good CDD and reviews of correspondent banking relationships in its home country, we found evidence during our file review that two higher risk respondent relationships for banks in other countries had not been 'refreshed' for several years, though belated attempts had been made to fill gaps and bring CDD up to date.

204. At several small banks, the quality of CDD files we reviewed was very weak. The focus of most file content was on ensuring that the respondent's list of signatories was up to date and there was often very little CDD evident on file. In particular, ultimate beneficial owners were often not identified, there were often no customer risk assessments and the purpose of the account and expected activity were not noted. In addition, there had often been no annual reviews so information held on long-standing relationships was often many years old.

At several banks, weaknesses in initial CDD were allowed to linger for many years due to a failure to conduct regular reviews of correspondent banking relationships.

205. Consistent with our findings on high risk customers and PEPs, we found that some banks' periodic reviews were clearly copied and pasted year after year with no challenge. This was particularly concerning as many of these annual reviews had been signed off by senior management, calling into question the rigour with which reviews are looked at by some firms. A respondent's risk profile can change significantly from one year to the next for a range of reasons. So we expect firms to assess new and emerging risks during reviews and make appropriate decisions on whether to maintain these higher risk relationships.

At one bank, we identified some review sheets for different respondent banks which had exactly the same answers to questions suggesting a lack of thorough review and a mechanistic approach to risk assessment.

206. In addition to regular periodic reviews, firms should also consider conducting ad-hoc reviews in light of changes identified in the interim which could result in a material change in the respondent's risk profile.

207. The JMLSG Guidance states that banks should consider terminating correspondent banking relationships and consider their obligation to report suspicious activity if respondents fail to provide satisfactory answers to reasonable questions regarding their transactions or activities. This should include, where appropriate, sharing the identity of customers featuring in unusual or suspicious transactions or activities.

208. However, we found that the termination of respondent accounts for AML reasons was relatively rare and it was clear to us that banks were often more concerned about reputational risk than AML risk when deciding whether to maintain or exit relationships. We expect banks to consider serious AML concerns in relation to correspondent banking relationships thoroughly and exit relationships which give rise to unacceptable AML risk.

At one major bank, when more than five SARS were submitted on a correspondent account in one year, it was the bank's policy to refer the case to the Global Head of AML to decide whether or not to exit the account.

However, there was one higher risk respondent which had been the subject of 300 SARS in two years. This account was maintained because the respondent's parent was government-owned and the major bank felt that exiting the relationship could affect its operations in the respondent's country.

209. Many large banks had set up committees to discuss respondent accounts and the continuation of relationships with higher risk respondents from an AML perspective. For example, one bank had a business risk committee which considered higher risk respondents and could refer AML-related concerns to an AML committee for specialist advice. One such scenario that had recently been discussed was whether to re-enter one country with a high risk of corruption.

210. At several smaller banks the oversight of respondents was often quite remote as they relied heavily on representatives of their parent banks who were more familiar with local banking requirements and regulations. However, our file reviews showed that banks like this usually did not check that its parent's representatives were conducting adequate monitoring of its respondent and there was often no evidence that the parent had done any monitoring at all.

4.6.3. Ongoing monitoring of respondent accounts – examples of good practice and poor practice

Good practice

- Review periods driven by the risk rating of a particular relationship; with high risk relationships reviewed more frequently.
- Obtaining an updated picture for the purpose of the account and expected activity.
- Updating screening of respondents and connected individuals to identify individuals/entities with PEP connections or on relevant sanctions lists.
- Involving senior management and AML staff in reviews of respondent relationships and consideration of whether to maintain or exit high risk relationships.
- Where appropriate, using intelligence reports to help decide whether to maintain or exit a relationship.
- Carrying out ad-hoc reviews in light of material changes to the risk profile of a customer.

Poor practice

- Copying periodic review forms year after year without challenge from senior management.
- Failing to take account of any changes to key staff at respondent banks.
- Carrying out annual reviews of respondent relationships but fail to consider money-laundering risk adequately.
- Failing to assess new information gathered during ongoing monitoring of a relationship.
- Failing to consider money laundering alerts generated since the last review.
- 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.

5. Findings – wire transfers

5.1. Background

211. The smooth functioning of the international payments system is vital to global financial stability. But the payments infrastructure is large and complex, having evolved as a complex patchwork of national and cross-border systems which are far from uniform but nevertheless closely connected.

212. At the heart of the international payments system is the global correspondent banking network, which allows banks around the world to make payments to and through each other. Within this network, banks communicate and transfer funds to each other, via both domestic payment systems and supra-national systems (eg TARGET). Banks' management of the money-laundering risks associated with correspondent banking are covered in more detail in Section 4.

213. A vital part of the infrastructure supporting both global correspondent banking and most domestic payment systems is the SWIFT network. SWIFT is the Society for Worldwide Interbank Financial Telecommunication, a member-owned co-operative of more than 9,000 financial institutions (banks, securities institutions and investment managers) and corporate customers in 209 jurisdictions world-wide. SWIFT provides the proprietary communications platform, products and services that allow its members to communicate with each other by means of standardised, encrypted messages. The SWIFT network handled a daily average 17.2m messages in March 2011.

214. The global payments system has evolved in a way that primarily promotes speed and efficiency. Accordingly, the system concentrates on information essential for processing a payment transaction with a minimum of human intervention (so-called 'straight through processing', or 'STP') and on including all countries and financial institutions within the system to allow payments to pass unimpeded across international borders.

215. A wire transfer usually involves the ordering customer (originator) instructing his bank (the originator's bank) to make a payment to the account of a payee (the beneficiary) with the beneficiary's bank. Where wire transfers in third party currencies are concerned, the originator's bank typically does not maintain an account with the beneficiary bank in the currency of the payment, which would allow the payment to be settled directly. Therefore, intermediary (or covering) banks are used for this purpose, usually located in the country where the currency of payment is the national currency.

216. Cover payments are usually effected via SWIFT and involve two distinct message streams:

- A customer payment order – usually a SWIFT Message Type ('MT') 103 – which is sent by the originator's bank direct to the beneficiary's bank and carries payment details, including originator and beneficiary information; and
- A covering bank-to-bank transfer (or cover payment), sent by the originator's bank to an intermediary bank (usually its own correspondent), asking the intermediary bank to cover the originator bank's obligation to pay the beneficiary bank. The intermediary bank debits the originator bank's account and either credits the beneficiary bank's account under advice or, if no account is held, sends the funds to the beneficiary bank's correspondent for settlement through the local payment system. The beneficiary bank is then able to match up the credit to its correspondent account with the MT103 received direct from the originator's bank.

217. Payments are sent using the 'cover method' mainly to avoid delays associated with different time zones and to reduce the costs associated with commercial transactions. The alternative, but less efficient, method of making such payments is by serial MT103 messages.

218. The role of the bank that maintains the customer relationship is key to effective AML and sanctions compliance. The bank at which an account is opened has the greatest opportunity to assess its potential customer, whether acting as the originator's bank or the beneficiary's bank. So, the primary CDD responsibility must remain with each bank involved at the beginning and end of a chain of payments to know its own customer and to fulfil its AML and sanctions obligations. And, of course, it must be borne in mind that it is the originator's bank that controls the initiation of the payment messaging process.

219. Banks' legal and regulatory responsibilities in relation to wire transfers are covered in detail in Section 2.3.1.

5.2. Paying Banks

220. The core obligation in the WTRs is that paying banks ensure that cross-border payments made on behalf of their customers (whether account holding or walk-in customers) contain complete payer information, comprising name, address and account number.

221. The banks we visited clearly understood this legal requirement and implemented it adequately, albeit with some variations in the manner of compliance, largely attributable to the sophistication, or otherwise, of their payments processes and interfaces with their customers and with the SWIFT network.

5.2.1. Large banks

222. The larger banks typically provided their major corporate customers, who make frequent payments world-wide, with a proprietary online banking tool or a direct connection with the bank's own technology platforms. (Alternatively, the corporate might be able to use SWIFT Corporate to initiate a MT103 payment instruction itself.) In this way, the major corporate generates its own electronic payment instruction which is routed to the bank's interface with the SWIFT network, usually via a sanctions screening tool that filters all outgoing payments before they are passed to the bank's processing application. Provided there is no sanctions 'hit', the payment is passed for processing and validation, after which a SWIFT MT103 and matching SWIFT MT202COV are created. (For more information on the MT202COV, see Section 5.5.

223. Whatever payment channel (SWIFT or electronic banking) is used by the payer, front end customer systems validation ensures that mandatory fields, which must be completed for STP purposes, have met the bank's minimum criteria for processing. Compliance with regulatory or other (eg FATF) requirements is enforced through coding in the payments systems. This coding ensures that static data on the customer, held in the bank's core accounting system, is entered in the correct fields in the payment instruction.

224. The core payments engine for cross-border payments validates key fields – ordering party, debit account, credit party, correspondent bank, amount, currency, etc – that are essential for routing the payment. The bank's SWIFT interface validates the outbound instruction ahead of sending to ensure compliance with scheme (eg CHAPS, SEPA, Target) and SWIFT formatting rules to ensure, among other things, that information is put in the correct lines and there are no invalid characters in the message.

Repairs

225. When incomplete or invalid data in outward or inward payments is detected, the payment instruction is routed to a repair queue in the relevant system.

> *Examples of instructions needing repair would be:*
>
> - *a payment to a third country in US dollars not stating who the US dollar correspondent bank is;*
> - *simple errors such as a bank branch address given but not a sort code; and*
> - *outgoing customer data getting "crushed up" occasionally so that it is not formatted correctly.*

226. Staff, who have generally received one-to-one training and coaching, do the repair. Any item that passes through the repair stage in any system requires

verification by a second operator with sufficient system privileges (eg a £50mn release limit) to allow them to verify and release the payment. All repaired items are then subject to the same controls as STP payments, including sanctions screening and ensuring that a particular account has a sufficient balance or credit for the payment to be made.

227. Within the repair queue, the message will show what caused the problem. This could be an invalid SWIFT Bank Identification Code (BIC) or a missing SWIFT BIC (with the name of the bank only) or no credit party identified. The repair agent has tools available to find the appropriate BIC and, having inserted it, can release the payment for checking by a second repair agent. If, say, the payment instruction simply named a bank, it would have to be placed in another queue for checking with the customer who the recipient was intended to be.

All SWIFT BICs are often incorporated in a major bank's system so that staff can validate whether a given BIC is correct. What staff cannot do, however, is authenticate whether the payer intended to credit that particular beneficiary.

228. It follows from the above that there should be no queries to major banks from beneficiary banks seeking full payer information. However, beneficiary information in the MT103 may well be incomplete.

229. Beneficiary field 59 in the MT103 needs to be filled with sufficient information about the beneficiary for the transaction to be processed electronically. Ideally, this should comprise the International Bank Account Number (IBAN) and SWIFT BIC. However, if the BIC has been omitted or is incomplete, beneficiary name and account number should normally be sufficient. But the paying bank is unable to validate the accuracy of the beneficiary data given by the ordering customer.

230. The bank's systems may be able to check that the given IBAN is the correct length and, furthermore, may check that the bank part of the IBAN matches the 'account with' institution given by the ordering customer. If not, the payment instruction goes through the repair process, which may be done manually or by referring back to the client.

If there were a simple branch/head office mismatch, for example, paying bank staff could repair it. But if the given beneficiary bank were plainly wrong – say, Bank A's IBAN and Bank B's BIC –the ordering customer would need to be contacted.

231. There is thus a limit to what any paying bank can do to validate the accuracy of beneficiary information given by the customer. Given the highly automated, high volume, straight-through-processing (STP) environment, major banks can do little to enrich or improve SWIFT message information. That said, because it is very important to large multinational companies to get their payments

processed rapidly, many have MT103 field 59 beneficiary information stored on their systems.

Unapplied funds cause all sorts of problems, which means that there is a considerable incentive to fix any identified one-off payment failure so that it does not recur.

5.2.2. Small banks

232. Smaller banks most commonly received customer payment instructions by telephone, fax or email. The paying bank's first steps were then to undertake checks on signatures and authenticity and to ensure that the customer had sufficient funds, or credit, to make the payment.

233. Once these checks had been completed, it was frequently the case that, as soon as the customer's account number was entered in the core banking system, the name, address and account number of the payer automatically entered in the correct field 50 lines in the SWIFT MT103 and any matching SWIFT MT202COV. Furthermore, the system would not allow those details to be changed. However, one bank told us that, where 'hold mail' accounts were involved, the input clerk must override that status and input the payer's proper address.

At two small foreign banks, appropriate software was incorporated in their SWIFT gateways, such that all incoming and outgoing SWIFT messages were automatically checked against more than 20 sanctions lists, including the HM Treasury and OFAC lists. Other banks relied on staff carrying out manual checks on beneficiary and purpose of payment against commercially available databases.

234. These smaller banks gave us some examples of queries received from beneficiary banks in response to MT103s received. These examples included:

- incorrect account numbers (eg two digits transposed) or references for the payee;
- spelling of names;
- a payer's address having become truncated in transmission; and
- a payment sent c/o the payer's business address.

One smaller bank gave us an insight into the reason for sending both serial MT103s and MT103s with accompanying MT202COVs, with all originator information automatically being copied from the MT103 to the MT202COV. In most cases, the serial MT103 is a cheaper option for customers. The other option can be self-defeating, because beneficiary banks wait to credit their customer's account until they know that cover for it has been received. And that cover can be delayed by false positive sanctions hits being found in the MT202COV.

5.2.3. Paying banks – examples of good and poor practice

Good 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.

Poor practice

- 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.

5.3. Intermediary banks

235. The key legal obligation for intermediary banks involved in cross-border payments is to ensure that all information received on the payer, which accompanies a transfer, is retained with the transfer. However, there are certain provisions (see paragraph 56) allowing an intermediary bank to use a payment system with technical limitations that prevent full payer information being passed on to another bank in a payment chain.

236. Payee banks are required to have effective procedures for checking that incoming wire transfers contain full payer information. But that monitoring may be undertaken after the transfers have been processed, in order not to disrupt the high daily volumes of straight-through processed international payments.

5.3.1. Large banks

237. We found that practice varied between the major banks we visited regarding their role as an intermediary bank, eg in circumstances where a non-UK bank wishes to make a customer payment in sterling, via one UK bank, for ultimate credit to the account of the customer of a second UK bank.

Two banks argued that, where they acted as intermediary and there was meaningless or incomplete payer information in a received MT103 or MT202COV, they had no responsibility to revert to the paying bank to obtain the relevant information. There was no SRVII or EU Regulation requirement in this respect and it was up to the beneficiary bank to resolve the problem with the paying bank. The intermediary bank's sole responsibility in this situation was to pass on whatever payer information had been received from the paying bank.

We asked one of these banks what would happen if the remitter was a well-known terrorist, or a sanctioned individual or entity. The bank conceded they would not want to find themselves in this position but appeared not to have adequately mitigated this risk.

238. It is worth adding that at least one major bank would not on-route payments via a system that truncated payer information in any way, despite the flexibility in the WTRs to cover such a situation. For example, a SWIFT payment instruction could be on-routed via CHAPS or Faster Payments without loss of payer data, but not via BACS. The proviso in the WTRs about the payee bank having to be informed that payer information was incomplete was seen as too onerous to be complied with in a largely STP environment.

In contrast, two other major banks screened all incoming payments for inadequate or incomplete payer information in MT103 field 50 and had procedures in place for contacting the remitting bank to obtain the required information. This usually entailed sending a SWIFT MT195 or MT199 enquiry to the remitting bank.

239. One of these major banks said that it sometimes happened that a piece of field 50 information was not actually missing but had been entered in a different line of that field. Nevertheless, if the software used to detect incomplete information failed to find the requisite information in the correct place, an enquiry was automatically generated anyway. In the early days of this software, it had thrown up thousands of cases every day. Consequently, the bank had needed to contact many remitting banks to ask them to format their messages differently, as a lot of unnecessary work was being created for both sides. The result was that, nowadays, paying banks typically responded to enquiries by re-formatting their messages to put the payer data where the payee bank's software expected to find it rather than providing missing or meaningful payer information so as to comply with FATF SRVII and the EU Regulation.

5.3.2. Small banks

240. Where smaller banks were concerned, the most common scenario was the UK bank receiving SWIFT MT103 instructions from its non-UK parent or correspondent bank to pay sterling to a customer of another UK bank.

We found that several small banks not only initiated proper enquiries of the remitting bank about inadequate payer information but actually did so in real time, delaying payment to the ultimate beneficiary until the requisite information had been received.

241. Because these banks received relatively small numbers of inward payments, which were all manually processed, it was a practical proposition to delay payment, pending receipt of complete payer information. Furthermore, this did not appear to cause any problems with payee banks and customers.

One of these banks argued it was in everyone's interests to obtain full payer information in these circumstances. If the intermediary bank did not take on the responsibility itself, then a bank further down the payment chain would have to do so. The result would be delays and inconvenience not only for the customers concerned but also for the banks in the payment chain who would be unable to apply funds to the beneficiary's account until full payer information was provided.

242. Smaller banks also routinely bounced back some inward payments for other reasons. These reasons included wrong formatting of the MT103 or other technical reasons, as well as missing IBAN or beneficiary information.

5.3.3. Intermediary banks – examples of good and poor practice

Good 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 inadequate payer information.
- Following processing, risk-based sampling for inward payments identify 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.

Poor practice

- 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.

5.4. Beneficiary banks

243. The key legal obligation for beneficiary banks is to have effective procedures for checking that incoming wire transfers are accompanied by full payer information. However, monitoring may be undertaken after the payments have been processed, in order not to disrupt the high daily volumes of straight-through processed international payments.

5.4.1. Large banks

244. The major banks we visited all had quite sophisticated processes, not only to detect inadequate payer information but also to undertake risk-based sampling to identify offending remitting banks and monitor their performance over time. These banks had also devoted considerable staff resources to what were commonly termed "FATF investigations".

> *One bank's FATF investigation team comprised 20 dedicated full-time employees in two different centres.*

Typical processes at major banks

245. At major banks, we generally found that receipt of customer payments was a heavily automated process, with very high STP rates for SWIFT MT103s. Consequently, payments were usually automatically credited to a beneficiary's account when certain information has been received. As with outward payments, processing was often done via a proprietary payments engine and separate software usually conducted sanctions checking at the same time.

Payments engines usually had robust artificial intelligence built into them which:

- *looked for the name and account number of the beneficiary in the correct fields;*
- *checked that the beneficiary had an adequate credit line or cover in place; and*
- *decided whether to credit the beneficiary's account on the strength of the MT103 only or, depending on the customer's risk rating, whether to wait for advice that cover had been credited to the bank's nostro account at the relevant correspondent bank.*

246. Provided that the sanctions and credit line checks were clear, the beneficiary's account would be credited. The credit would not be delayed by reason of inadequate payer information, because the WTRs allow three business days for enquiries about the payer to be made.

247. A report was usually built into the payments engine that checks for two things:

- payment orders where no, or only partial, information had been supplied; and
- any paying bank which might be trying to conceal remitter information by inputting meaningless information, for example '?*&!$@'.

248. The payments engine usually generated daily reports for a dedicated team to review.

One bank scrutinised around 100 alerts in total from both categories and sought further information. This total comprised:

- *20 banks based in high-risk countries and a further 80 banks from medium and low risk countries which had been identified as sending payment orders where no, or only partial, payer information had been supplied; and*
- *Five banks from high-risk countries and another five banks from medium and low risk countries which might be trying to conceal remitter information by inputting meaningless information.*

At the time the WTRs came into force, the numbers of alerts were 'huge'. By July 2009, there were about 10k alerts for all countries and at the time of our visit, the number had reduced to about 3k per month.

249. Where missing information was identified, banks usually used enquiry management systems allowing them to communicate with the whole SWIFT network with a full audit trail. MT199 enquiries were usually sent out, based on templates specifying the missing information and also the legal basis for the enquiry. There were then two possible scenarios:

- Either a reply was received apologising for the omission and supplying the missing originator data, which was then screened by the bank for sanctions purposes; or
- There was no response to the enquiry. In such cases, a reminder was usually sent around four business days later, repeating the request. If a response was still not received, the enquiry was usually closed on business day five without proper resolution.

We were told that, since the WTRs came into force, no potential sanctions hits had been identified as a result of obtaining missing payer information.

250. A consolidated monthly report for Compliance was usually compiled, containing trend analysis and more detailed data on banks who failed to respond. Compliance then decided how best to deal with their counterparts in the banks concerned.

One bank saw a significant reduction in the number of banks failing to respond adequately to requests for missing information. In March 2008, out of a total of nearly 350k relevant cases, just over 10% failed to give an adequate response. In contrast, by December 2010, banks failed to provide an adequate response in just 0.34% of 560k cases.

However, despite the generally significant reduction in the number of banks failing to provide adequate information, it was apparent that some banks continued to breach the WTRs and FATF standards.

Some interesting variations to the typical process

251. One major bank took a somewhat different approach to determining whether incoming MT103s contained sufficient payer information. It first decided how many characters in field 50 would make a complete name and address. An analyst undertook a major review of incoming payments from which he judged that, provided three lines of data were complete, the message should contain a complete name and address. A daily report was then produced on all incoming payments containing insufficient lines which was then reviewed on a risk based approach, starting with payments originating from non-FATF countries.

252. Another major bank's FATF investigation team received a daily email report identifying all inward payments from the previous day from high and medium risk countries. The team then reviewed all high-risk country payments plus 10% of Medium Risk country payments, to check for adequate payer information.

Good compliance rates

253. The overall message from the major banks was that compliance with the WTRs had steadily improved over time, to a point where a relatively small number of

payments and paying banks were non-compliant. There did not seem to be any obvious reasons for continuing non-compliance.

One bank noted an ongoing issue with some banks in the Middle East, who frequently gave the payer's PO Box instead of a full address. The bank's response had been to liaise with its correspondent bank RMs and to ask the offending banks to upgrade their systems to comply with FATF SRVII standards.

254. Some banks appeared nervous being ahead of their competitors in dealing with offending banks and were awaiting a formal 'industry' position on this. In addition, none of the major banks had thought it necessary or useful to write to the regulatory bodies responsible for the offending banks.

Ultimately, banks viewed terminating relationships with other banks on payer transparency issues as a 'nuclear option' only to be considered when all other remedial action had failed.

5.4.2. Small banks

255. Where smaller banks were concerned, as noted above, it was much more likely that any MT103s received with inadequate or meaningless payer information would be queried with the remitting bank before the funds were accepted. But this seemed to happen in only a small number of cases (generally about 1%-2%) and the banks all had procedures for sending out MT199 enquiries to offending banks, followed by a chasing enquiry if no response was received.

5.4.3. Beneficiary banks – examples of good and poor practice

Good 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.

Poor practice

- Insufficient processes to identify payments with incomplete or meaningless payer information.

5.5. Implementation of the SWIFT MT202COV

5.5.1. What is the MT202COV and why was it introduced?

256. Historically, the SWIFT MT202 was used both to effect cover for an underlying customer transfer (MT103) and for inter-bank payments that were unconnected to customer transfers, such as wholesale money market or foreign exchange transactions.

257. Consequently, an intermediary bank would not necessarily know that it was dealing with a cover payment when processing an MT202 message. Additionally, there was (and remains) no provision within the MT202 message format for it to carry the originator and beneficiary information that is contained in an underlying MT103 customer transfer, an intermediary bank. Therefore, prior to the practical introduction of the MT202COV in November 2009, banks could not screen or monitor underlying customer information in relation to cover payments, from a sanctions or AML perspective.

258. The MT202COV was introduced to help banks meet their legal obligations by ensuring that all necessary payer and beneficiary information could be monitored by intermediary banks and other financial institutions involved in cross-border payments.

> *The JMLSG Guidance states that the MT202COV should be used for all outgoing cover payment transactions for which there is an associated MT103 and must replicate the originator/beneficiary information contained in the MT103. MT202s should be used only for bank-to-bank transactions. In addition, banks should have the capability to receive MT202COV messages from other banks and, as a minimum, screen them against relevant sanctions lists.*
>
> *However, as an alternative to sending customer payments using the 'cover method', banks can choose to send their payments by the 'serial method' in which an MT103 is sent by the originator's bank to its correspondent asking for payment (and the corresponding covering funds) to be made available to the payee via his bank.*

5.5.2. The impact on major banks

259. Adoption of this new SWIFT message type had a significant impact on all major banks, which needed to be able both to send and receive MT202COVs in the required timescale.

260. First and foremost, this entailed changing, building and testing payment applications. For at least one bank, this had to be the subject of a global project with group-wide representation. However, implementing the MT202COV also resulted in a large rise in the number of sanctions and AML alerts for review.

One major investment bank told us that it was difficult to determine the precise impact of the MT202COV on total alerts, because it coincided with increases in transaction volumes and other new regulatory requirements. Nevertheless, alerts had increased by approximately 35% in the year after the MT202COV's introduction.

261. Some major banks with high volumes of market-driven bank-to-bank transactions and smaller numbers of customer-related cover payments had seen no need to recruit additional staff to handle a marked increase in alerts. In contrast, one major bank with operations in many countries had recruited more staff to cope with a huge anticipated increase in sanctions alerts from November 2009.

262. All the major banks perceived the introduction of the MT202COV to have gone smoothly across SWIFT's membership, with only relatively minor problems including:

- Some banks not using, or misusing the MT202COV.

One major bank searched the text of fields 21 and 72 of MT202 messages for the word 'cover' in order to identify potential cover payments where an MT202COV was not being used. This generated a number of alerts, as many SWIFT messages contain terms like 'cash cover'. However, following manual analysis, only one to two payments per day were found to be genuine cover payments where the MT202COV was not being used.

- Issues in some 'emerging markets', where clearing systems had not been upgraded to deal with MT202COVs being transposed into a clearing format.
- A problem with one country, where banks were not ready to receive MT202COV messages on the implementation date. As a result, payments traffic to and from that country had to be redirected, so that only serial MT103s were sent on behalf of customers to beneficiaries in that country.
- Delays to their own customers' payments, resulting from different banks applying different processes to sanctions screening with the MT103s and MT202COVs they received.

One bank told us they experienced an increase in 'beneficiary claiming non-receipt' enquiries when there was a delay in receiving funds from a correspondent bank following the introduction of the MT202COV.

263. One major investment bank said it had reviewed all its respondents' use of MT202s and MT 202COVs and had introduced use of the MT202COV as an element of the CDD review process. Another major retail bank said that it was currently considering whether to incorporate implementation of the MT202COV as an additional element of enhanced due diligence on its correspondent banking clients.

5.5.3. The impact on smaller banks

264. Among smaller banks, we found differing levels of knowledge and experience of the MT202COV and estimated use of the new message type by smaller banks varied considerably. Some small banks admitted that they made no use of the MT202COV.

> *One bank said that 2-5% of its outgoing customer payments were sent with matching MT202COVs. Another bank said it sent only one per fortnight whereas another used it solely for a particular payment, in one currency, made every quarter. In contrast, a fourth bank said that it received 10-15 cover payments by MT202COV daily.*

265. But small banks that did use it had not experienced any implementation difficulties. In one case, the bank had been able to issue and receive MT202COV traffic on a single stand-alone system.

266. One small bank offered some insights into the benefit and decision to use the MT202COV for a smaller bank:

- first, it reduced the number of enquiries from correspondent banks about the purpose of MT202 payments; and
- second, it was usually the value date on the customer payment that determined whether or not a SWIFT MT202COV would be sent with a matching MT103. Where the customer requested same day value, the paying bank would always use an MT202COV: for a future value date, the MT202COV would not necessarily be used.

5.5.4. Implementation of SWIFT MT202COV – examples of good and poor practice

Good 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 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.

Poor practice

- Continuing to use the MT202 for all bank-to-bank payments, even if the payment is cover for an underlying customer transaction.

6. Case studies – high-risk customer relationships

267. During our review, we identified some relationships which caused us concern for a variety of reasons including:

- banks' failure to identify PEP accounts;
- banks' failure to conduct enhanced due diligence on accounts which were high risk;
- inadequate challenge from banks' AML and compliance staff when high-risk factors were clearly apparent; and
- banks accepting customers or continuing relationships when serious allegations about criminal activity had not been properly considered.

268. The following are examples of such relationships and we have highlighted the associated weaknesses to the banks involved. In line with the rest of this report, we have anonymised the information in this section.

Relationship 1

This account for an ex-state governor in a high-risk country was held by a small bank. The account opening form contained no employment details but the customer's annual income was stated as $1m. In addition, the customer's residential address stated on the account opening form was different from the address given on documents to verify his address but this had apparently not been noticed by the bank.

No details of expected account activity were given on the account opening form, which stated the customer had been referred by the Chairman. There was a handwritten note to explain that the only deposit to the account was from an 'existing customer and [the bank's] Chairman'; there was no explanation why the bank's Chairman was crediting this account. There was no evidence of senior management sign-off for this PEP account.

Relationship 2

This PEP account was held by a small bank for a politician from a high risk country with a stated annual income of around £100k. The bank had received a three-month term deposit of over £500k from a bank in an offshore centre in 2009. There was no explanation of source of wealth or other business interests on file and no evidence of senior management sign-off for this account.

Relationship 3

This account for a customer from a high-risk country had not been classified as a PEP account by a small bank despite the bank's own files showing the customer had held senior political, diplomatic and judicial positions. This contravened the bank's policy to continue to classify former public officials as PEPs after they leave office. There were also no details on file about the anticipated turnover on the account and the customer's source of wealth was stated as 'business'.

Relationship 4

This account for a former PEP in an offshore centre was funded by rental income. The CDD file contained allegations of fraud surrounding the rental property and its construction. These allegations had apparently been identified by Compliance but no obvious investigation or other action was taken as a result.

Relationship 5

This account was not classified as high risk by a small bank but we decided to review it as it had a balance of around £1m. The file contained no address verification for the customer. When the account was opened in 2007, the customer, a restaurateur, said expected annual income to the account was £20k-£30k. However, the transaction report for the account showed large amounts of £150k, £40k, £50k, £70k, £100k, £800k, £1.1mn and £900k being paid into the account in the next three years.

When we asked the bank's MLRO about these payments, he could not explain them and said that 'by themselves or as a one-off they are generally ok but you [the FSA] may have a point about all of the payments as a whole'.

Relationship 6

In early 2010, the private banking arm of a major banking group established a relationship with a former government minister from a high risk country. The customer, who appears to have continuing political influence, opened a personal bank account and a bank account for a company he owned entirely. The source of wealth was described in the CDD file as 'sale of [a significant business asset], properties in the UK'. There were no address details for the customer.

Around the same time, the customer made a separate approach to an offshore banking arm of the same banking group. An internal intelligence report was commissioned as part of the offshore banking arm's CDD. This report stated that the business asset sold by the customer was awarded to him by a former senior military official who was the subject of serious and credible allegations of corruption. We were told that the offshore banking arm decided not to establish a banking relationship with the customer on the basis of this report which was also made available to the private banking arm.

The private banking arm's AML team told us the offshore banking arm of the Group was 'very sensitive' about the former senior military officer. However, the private bank was initially 'not minded' to exit the relationship based solely on the information in the intelligence report but, 'in order to maintain a consistent Group line', they took the decision to close the accounts.

Two other banks we visited during our review also held accounts for this individual and we are aware of one other bank which has recently accepted hundreds of millions of dollars in deposits from him. One of the two banks we visited was not aware of any allegations of corruption about this individual; the other had conducted good EDD but we were concerned that a paper presented to a key customer approval committee failed to mention the individual's connection to the former senior military officer.

Relationship 7

This relationship was approved in principle by the MLRO of the private banking arm of a major banking group in early 2010.

An account opening form included a statement from the RM that 'We understand they are considered PEPs due to family ties, however I believe the bank can do good business with [these customers] and could generate further business in relatively untapped areas'.

We had a number of concerns about this relationship. First, the MLRO had approved the relationship without verifying the customers' identity, or obtaining details on source of wealth. In addition, an intelligence report on file highlighted:

- Close links between the customers' family and a former head of state.
- Allegations that a relative of the customers had embezzled millions of dollars of state funds. The same individual was also charged with evading millions of dollars in tax.

- Multi-million pound mortgage business for the same relative of the customers being turned away by another part of the same banking group in 2003 due to concerns over the family, their political associations and various sanctions in place in relation to that political regime. Following this approach, a notice was issued asking all entities in the banking group to identify and exit any relationships with the 'entire family'. There was no indication in the intelligence report that this notice had been rescinded.

The intelligence report concluded that 'the reputational and regulatory risks of developing a relationship with these individuals should be given careful consideration' and that 'it will be important to understand and document what is known about the customers and the source of their wealth and ultimately the source of the…family wealth'. It also recommended that an external intelligence report on the customers should be considered. However, a note on file from one of the bank's AML team stated that, as the customers' relatives 'have been removed from sanctions lists', he was not in favour of this due to the cost and the possibility an external report might not yield useful information.

Notes on file from the AML team stated that the 'family has been influential and wealthy in the region for many years, notwithstanding any unjust enrichment that may have taken place during the conflicts in the region'.

Another email from a member of the AML team stated that 'In my view, provided there is sufficient business to justify the risk then I am happy to recommend we proceed.' The prospective customers, however, decided not to open an account with the bank after all.

Relationship 8

This account was opened at the private banking arm of a major banking group in 2009 for an existing customer's wife who, according to the CDD file, had no personal wealth and was dependent on her husband for income.

The file showed her husband was on the Interpol wanted list for fraud at the time the bank account was opened. The source of funds was a multi-million pound transfer from the foreign bank account of a company (based in an offshore tax haven) owned by the customer. The funds being transferred were said to be a bonus paid to her husband. An internal intelligence report on the customer's husband concluded '…entering into a banking relationship with a person who is wanted by Interpol poses a high reputational risk'.

This account was initially classified by the RM as low risk for money laundering and there was no evidence of account reviews once the account was opened.

Relationship 9

These customers had been identified as PEPs by the private banking arm of a major banking group for reasons including their business partnership with a senior politician in a high risk country. The account was opened in early 2006.

The CDD file contained a general lack of EDD evidenced by the bank's apparent failure to identify that the customers' business partner was (and, at the time of writing, remains) on the EU, UK Treasury, Swiss and OFAC sanctions lists, among others.

The account was reviewed by the bank in late 2006, 2007 and 2008, but the review forms were identical and did not identify that the customers' business partner was on sanctions lists. Although there were no adverse allegations about the customers themselves, it was a matter of concern that the bank had apparently failed to consider the money-laundering risks of dealing with close business associates of a politician subject to sanctions.

Relationship 10

This customer had been classified as a high-risk customer by the private banking arm of a major banking group which opened an account for him in 2010.

Now a successful businessman, the customer already held an account with the Group's private bank in another country. An internal intelligence report on the bank's CDD file showed that the customer had been a partner in a firm involved in 'shadowy contracts from corrupt governments' which allegedly resulted in the payment of mining rights and diamonds. The report also detailed international condemnation of the firm's activities and stated that, '[the customer] has never been charged but no one has yet bottomed out the allegations of corruption from mining resources'.

The report concluded that 'the risk of regulatory action and reputational risk is very high' if the private bank were to open an account for him.

We had serious concerns that the bank had not properly reviewed whether the customer had acquired his successful businesses and wealth as a result of corruption. In addition, the RM for the customer initially proposed that the customer should be treated as low risk for money laundering.

Relationship 11

This PEP customer, a student based in London, was a close relative of a foreign politician/businessman. The relevant account was opened in 2008 with the initial funding of around £1m coming from the politician. The bank had not taken adequate steps to establish the politician's source of wealth.

Our research revealed that the politician was the subject of charges of large-scale misappropriation of state funds and a court order freezing his assets worldwide.

There was no indication from our file review that the bank had identified this relevant adverse information and no evidence of annual reviews being conducted on this account. The bank exited this account for commercial reasons in late 2010.

Relationship 12

We reviewed a correspondent banking relationship maintained by a major bank. The CDD file contained a substantial amount of adverse information dating back several years, centring on the respondent bank's connection with a state-owned company involved in an extractive industry in its home country. The state-owned company was a direct shareholder in the respondent bank and two of the company's executives apparently held four additional stakes in the bank through offshore shell companies. There was no explanation for these opaque corporate structures.

Much of this adverse information was included in a report by a major western government, which alleged that large numbers of allegedly corrupt PEPs either banked with, or controlled, the respondent bank. The bank we visited was considering whether to continue this relationship.

Relationship 13

A major bank had held this correspondent banking account for several years. The respondent bank was connected with several PEPs from a high-risk country through management and ownership.

The CDD file identified that a PEP who co-owned the majority stake in the respondent bank had previously been implicated in a serious bribery scandal. A European government had apparently blocked 'suspect funds' held in a bank account and had denied the PEP's appeal to unblock the account.

An assessment of this information in 2010 conducted by the RM for the respondent bank simply concluded 'I suggest to keep the relationship' with no reasons given for this decision. Following our visit, the bank decided to exit this relationship.

Relationship 14

A large bank with almost exclusive UK business held an account for the wife of the former senior politician of a high-risk country. Her file showed an income of £30k a year.

Information on the CDD file showed that her husband was arrested on multiple counts of corruption and theft from aid funds, amounting to many millions of dollars, but later cleared. However, he had since been rearrested in relation to further corrupt activity.

Our review of bank statements found that around £80k was paid into the account in six months in 2007 and over £300k in 2008. Some of this money appeared to have been received directly from the governments of other high risk countries with no apparent explanation.

Since our visit, this account has been closed.

Relationship 15

A small private bank had decided not to open a company account for a customer because they identified during the take-on process that he had been charged with false accounting and money laundering in Gibraltar. There was a note on file indicating that existing relationships with the customer would be reviewed but we saw no evidence this had been done and his other accounts appeared to remain active.

Relationship 16

Company A is a UK incorporated company which has an account with the private banking arm of a major UK group. The ultimate beneficial owner of Company A is a PEP whose husband is a former politician from a higher risk country.

There were many allegations over a sustained period from various sources, including reputable newspapers, on the customer's CDD file about the customer's business making large profits as a result of her husband abusing political power.

At the time of our visit, the bank had just decided to exit all relationships with the customer.

Relationship 17

This PEP customer of a small private bank is a UK resident from a high-risk country and a housewife. The file states her source of funds as a transfer from a UK bank and the source of wealth as 'money made from dividend payments', real estate and oil.

An intelligence report on file revealed that two close relatives had held high office in her home country and that one had been the subject of serious allegations of corruption.

There was some evidence on the file of Compliance questioning the customer's source of wealth; the customer explained that it was from 'her own investment business' and that her English was not good enough to allow her to provide greater detail. The RM stated that 'her family had been relatively wealthy even [under a previous regime]' and that 'I don't know how much she originally invested. I do not know where the funds for her original investment came from as I did not know her at that time – but they were her funds and not anyone else's'. It appeared from our file review that this explanation satisfied Compliance.

The file also contained an article from a credible source, which appeared to have been found as part of a regular review of the relationship. It quoted an individual convicted of corruption who stated in an affidavit that he had been instructed to set up a trust for the benefit of the customer in order to launder the proceeds of corruption by one of her relatives. There was no evidence that the bank had considered the implications of this information.

7. Consolidated examples of good and poor practice – proposed guidance

7.1. High-risk customers and PEPs

High-risk customers and PEPs – examples of good and poor practice	
Examples of good practice	Examples of poor practice
AML policies and procedures	
• Senior management take money laundering risk seriously and understand what the Regulations are trying to achieve. • Keeping AML policies and procedures up-to-date to ensure compliance with evolving legal and regulatory obligations. • A clearly articulated definition of a PEP (and any relevant sub-categories) which is well understood by relevant staff. • Considering the risk posed by former PEPs and 'domestic PEPs' on a case-by-case basis. • 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. • Providing good quality training to relevant staff on the risks posed by higher risk customers including PEPs and correspondent banks. • Ensuring RMs 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. • 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.	• A lack of commitment to AML risk management among senior management and key AML staff. • Failing to conduct quality assurance work to ensure AML policies and procedures are fit for purpose and working in practice. • Informal, undocumented processes for identifying, classifying and declassifying customers as PEPs. • 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. • Giving waivers from AML policies without good reason. • Considering the reputational risk rather than the AML risk presented by customers. • Using group policies which do not comply fully with UK AML legislation and regulatory requirements. • Using consultants to draw up policies which are then not implemented. • Failing to allocate adequate resources to AML.

High-risk customers and PEPs – examples of good and poor practice

Examples of good practice	Examples of poor practice
AML policies and procedures	
	• 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.
Risk assessment	
• Using robust risk assessment systems and controls appropriate to the nature, scale and complexities of the bank's business. • 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. • Risk assessment policies which reflect the bank's risk assessment procedures and risk appetite. • Clear understanding and awareness of risk assessment policies, procedures, systems and controls among relevant staff. • Quality assurance work to ensure risk assessment policies, procedures, systems and controls are working effectively in practice. • 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.	• Allocating higher risk countries with low risk scores to avoid having to conduct EDD. • MLROs who are too stretched or under resourced to carry out their function appropriately • Failing to risk assess customers until shortly before an FSA visit. • Allowing RMs to override customer risk scores without sufficient evidence to support their decision. • Inappropriate customer classification systems which make it almost impossible for a customer to be classified as high risk.

High-risk customers and PEPs – examples of good and poor practice

Examples of good practice	Examples of poor practice
Customer take-on	
• Ensuring files contain a customer overview covering risk assessment, documentation, verification, expected account activity, profile of customer or business relationship and ultimate beneficial owner. • Having all new PEP or other high-risk relationships checked by the MLRO or the AML team. • 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. • Using, where available, local knowledge and open source internet checks to supplement commercially available databases when researching potential high risk customers including PEPs. • Having clear risk-based policies and procedures setting out the EDD required for higher risk and PEP customers, particularly in relation to source of wealth. • Effective challenge of RMs and business units by banks' AML and compliance teams, and senior management. • Reward structures for RMs which take into account good AML/compliance practice rather than simply the amount of profit generated. • Clearly establishing and documenting PEP and other high-risk customers' source of wealth. • 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.	• Failing to give due consideration to certain political connections which fall outside the Money Laundering Regulations 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. • Poor quality, incomplete or inconsistent CDD. • Relying on Group introductions where overseas standards are not UK-equivalent or where CDD is inaccessible due to legal constraints. • Inadequate analysis and challenge of information found in documents gathered for CDD purposes. • Lacking evidence of formal sign-off and approval by senior management of high-risk and PEP customers and failure to document appropriately why the customer was within AML risk appetite. • Failing to record adequately face-to-face meetings that form part of CDD. • Failing to carry out EDD for high risk/PEP customers. • Failing to conduct adequate CDD before customer relationships are approved. • Over-reliance on undocumented 'staff knowledge' during the CDD process. • Granting waivers from establishing a customer's source of funds, source of wealth and other CDD without good reason. • Discouraging business units from carrying out adequate CDD, for example by charging them for intelligence reports.

High-risk customers and PEPs – examples of good and poor practice

Examples of good practice	Examples of poor practice
Customer take-on	
• Understanding and documenting ownership structures complex or opaque corporate structures and the reasons for them. • Face-to-face meetings and discussions with high-risk and PEP prospects before accepting them as a customer. • Making clear judgements on money-laundering risk which are not compromised by the potential profitability of new or existing relationships. • 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. • Allowing accounts to be used for purposes inconsistent with the expected activity on the account (eg 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.

High-risk customers and PEPs – examples of good and poor practice

Examples of good practice	Examples of poor practice
Enhanced monitoring of high-risk relationships	
• Transaction monitoring which takes account of up-to-date CDD information including expected activity, source of wealth and source of funds. • Regularly reviewing PEP relationships at a senior level based on a full and balanced assessment of the source of wealth of the PEP. • Monitoring new clients more closely to confirm or amend the expected account activity. • A risk-based framework for assessing the necessary frequency of relationship reviews and the degree of scrutiny required for transaction monitoring. • Proactively following up gaps in, and updating, CDD during the course of a relationship. • Ensuring transaction monitoring systems are properly calibrated to identify higher risk transactions and reduce false positives. • 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. • A good knowledge among key AML staff of a bank's highest risk/PEP customers. • 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. • Global consistency when deciding whether to keep or exit relationships with high-risk customers and PEPs. • Assessing RMs' performance on ongoing monitoring and feed this into their annual performance assessment and pay review. • Lower transaction monitoring alert thresholds for higher risk customers.	• Failing to carry out regular reviews of high-risk and PEP customers in order to update CDD. • Reviews carried out by RMs with no independent assessment by money laundering or compliance professionals of the quality or validity of the review. • Failing to disclose suspicious transactions to SOCA • Failing to seek consent from SOCA on suspicious transactions before processing them. • Unwarranted delay between identifying suspicious transactions and disclosure to SOCA. • Treating annual reviews as a tick-box exercise and copying information from the previous review. • Annual reviews which fail to assess AML risk and instead focus on business issues such as sales or debt repayment. • Failing to apply enhanced ongoing monitoring techniques to high-risk clients and PEPs. • Failing to update CDD based on actual transactional experience. • Allowing junior or inexperienced staff to play a key role in ongoing monitoring of high-risk and PEP 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.

7.3 Correspondent banking

Correspondent banking – examples of good and poor practice	
Examples of good practice	Examples of poor practice
Risk assessment of respondent banks	
• Regularly 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. • More robust monitoring respondents identified as presenting a higher risk. • Risk scores that drive the frequency of relationship reviews. • Taking into consideration publicly available information from national government bodies and non-governmental organisations and other credible sources.	• Failing to consider the money-laundering risks of correspondent relationships. • Inadequate or no documented policies and procedures setting out how to deal with respondents. • 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. • 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.
Customer take-on	
• Assigning clear responsibility for the CDD process and the gathering of relevant documentation. • EDD for respondents that present greater risks or where there is less publicly available information about the respondent. • 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. • Screening the names of senior managers, owners and controllers of respondent banks to identify PEPs and assessing the risk that identified PEPs pose. • Independent quality assurance work to ensure that CDD standards are up to required standards consistently across the bank.	• Inadequate CDD on parent banks and/or group affiliates, particularly if the respondent is based in a high-risk jurisdiction. • Collecting CDD information but failing to assess the risks. • Over-relying on the Wolfsberg Group AML questionnaire. • Failing to follow up on outstanding information that has been requested during the CDD process. • Fail to follow up on issues identified during the CDD process.

Correspondent banking – examples of good and poor practice

Examples of good practice	Examples of poor practice
Customer take-on	
• Discussing with overseas regulators and other relevant bodies about the AML regime in a respondent's home country. • Identifying risk in particular business areas (eg informal value transfer such as 'hawala', tax evasion, corruption) through discussions with overseas regulators. • Visiting, or discuss with, respondent banks to discuss AML issues and gather CDD information. • Gathering information about procedures at respondent firms for sanctions screening and identifying/managing PEPs. • Understanding respondents' processes for monitoring account activity and reporting suspicious activity. • 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.	• Relying on parent banks to conduct CDD for a correspondent account and taking no steps to ensure this has been done. • Collecting AML policies etc but making no effort to assess them. • Having no information on file for expected activity volumes and values. • Failing to consider adverse information about the respondent or individuals connected with it. • No senior management involvement in the approval process for new correspondent bank relationships or existing relationships being reviewed.
Ongoing monitoring of respondent accounts	
• Review periods driven by the risk rating of a particular relationship; with high risk relationships reviewed more frequently. • Obtaining an updated picture for the purpose of the account and expected activity. • Updating screening of respondents and connected individuals to identify individuals/entities with PEP connections or on relevant sanctions lists. • Involving senior management and AML staff in reviews of respondent relationships and consideration of whether to maintain or exit high risk relationships. • Where appropriate, using intelligence reports to help decide whether to maintain or exit a relationship.	• Copying periodic review forms year after year without challenge from senior management. • Failing to take account of any changes to key staff at respondent banks. • Carrying out annual reviews of respondent relationships but fail to consider money-laundering risk adequately. • Failing to assess new information gathered during ongoing monitoring of a relationship. • Failing to consider money laundering alerts generated since the last review.

Correspondent banking – examples of good and poor practice

Examples of good practice	Examples of poor practice
Ongoing monitoring of respondent accounts	
• Carrying out ad-hoc reviews in light of materisal 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.

7.3 Wire transfers

Wire transfers – examples of good and poor practice	
Examples of good practice	Examples of poor practice
Paying banks	
• 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.
Intermediary banks	
• 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 inadequate payer information. • Following processing, risk-based sampling for inward payments identify 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.	• 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.
Beneficiary banks	
• 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.

Wire transfers – examples of good and poor practice

Examples of good practice	Examples of poor practice
Implementation of SWIFT MT202COV	
• 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 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.	• Continuing to use the MT202 for all bank-to-bank payments, even if the payment is cover for an underlying customer transaction.

The Financial Services Authority
25 The North Colonnade Canary Wharf London E14 5HS
Telephone: +44 (0)20 7066 1000 Fax: +44 (0)20 7066 1099
Website: http://www.fsa.gov.uk