
FINAL NOTICE

To: **Coutts & Company**
FSA
Reference
Number: 122287

Address: 440 Strand, London, WC2R 0QS
Date: 23 March 2012

ACTION

1. For the reasons given in this notice, the FSA hereby imposes on Coutts & Company (Coutts or the Firm) a financial penalty of £8.75 million for breach of Principle 3 (management and control) of the FSA's Principles for Businesses which occurred between 15 December 2007 and 15 November 2010 (the Relevant Period).
2. Coutts agreed to settle at an early stage of the FSA's investigation. It therefore qualified for a 30% (Stage 1) discount pursuant to the FSA's executive settlement procedures. Were it not for this discount, the FSA would have imposed a financial penalty of £12.5 million on Coutts.

SUMMARY OF REASONS

3. Coutts breached Principle 3 because it failed to take reasonable care to establish and maintain effective anti-money laundering (AML) systems and controls in relation to customers that posed a higher money laundering risk than standard customers (high risk customers).
4. The laundering of money through UK financial institutions undermines the UK financial services sector. It is the responsibility of UK financial institutions to ensure that they are not used for criminal purposes and, in particular, that they do not handle the proceeds of crime. Unless firms have in place robust systems and controls in relation to AML, particularly with respect to high risk customers, they risk leaving themselves open to abuse by money launderers. The FSA has the regulatory objectives of the reduction of

financial crime and market confidence enshrined in statute. Both of these objectives are endangered by failures in this regard.

5. The failings at Coutts were serious, systemic and were allowed to persist for almost three years. Coutts was expanding its customer base during the Relevant Period and staff were incentivised in part to increase the number of customers taken on. As such, it was important that there were appropriate systems and controls in place, including with respect to the risk of money laundering. The weaknesses in Coutts' controls resulted in an unacceptable risk of handling the proceeds of crime. In particular, the Firm did not:
 - i. assess adequately the level of money laundering risk posed by prospective and existing high risk customers. This included failing properly to identify and record all politically exposed persons (PEPs);
 - ii. gather the appropriate level of due diligence information about a large number of prospective high risk customers;
 - iii. apply robust controls when establishing relationships with high risk customers. In particular, the AML team failed to provide an appropriate level of scrutiny and challenge;
 - iv. consistently apply appropriate ongoing monitoring to its existing high risk customers to ensure that changes in circumstances and risk profiles were identified, assessed and managed appropriately and that all unusual transactions would be identified; and
 - v. carry out adequate reviews of its AML systems and controls for high risk customers.
6. The FSA reviewed 103 high risk customer files, and identified deficiencies in 73 files (71%) as a result of the Firm's failure to gather appropriate due diligence when accepting a new customer and/or the Firm's failure to conduct appropriate ongoing monitoring of existing customers. Specifically, the FSA identified that Coutts had failed to do one or more of the following in each of the 73 files:
 - i. gather sufficient information about its prospective PEP and other high risk customers to establish their sources of wealth and income;
 - ii. establish the source of the funds received at the outset of the high risk customer relationship with Coutts;
 - iii. gather sufficient information about prospective high risk corporate customers, such as information concerning business activities, ownership and control structures and the intended purpose of the business relationship;
 - iv. identify and/or assess adverse intelligence about prospective and existing high risk customers properly and take appropriate steps in relation to such intelligence;
 - v. keep the information held on its existing PEP and other high risk customers up-to-date; and
 - vi. scrutinise transactions made through PEP and other high risk customer accounts appropriately.
7. In addition to the breach of Principle 3, Coutts also breached the following Senior Management Arrangements, Systems and Controls (SYSC) rules in the FSA Handbook: SYSC 6.1.1R and SYSC 6.3.1R (which are listed in the Appendix to this Notice).

8. Coutts' failings merit the imposition of a significant financial penalty. The FSA considers the failings to be particularly serious because:
 - i. Coutts is a high profile bank with a leading position in the private banking market and is a gateway to the UK financial system for high net worth international customers. It was particularly important, therefore, that Coutts had robust systems and controls to prevent and detect money laundering;
 - ii. the markets and customers that the Firm was targeting included certain jurisdictions with AML requirements which were not equivalent to those in the UK and which carried an inherently high risk in respect of money laundering;
 - iii. the Firm provided financial services to a large number of high risk customers, the number of which approximately doubled during the Relevant Period, and it handled considerable sums of money on behalf of those customers;
 - iv. the failings persisted for a period of almost three years;
 - v. the failings were not identified by the Firm;
 - vi. the Firm, along with three other institutions within The Royal Bank of Scotland Group, was fined in August 2010 for failing to put in place adequate financial crime systems and controls, in that case in relation to UK financial sanctions; and
 - vii. the failings in this Notice also occurred in a period during which the FSA successfully brought and published other Enforcement cases against a number of institutions for shortcomings in their financial crime systems and controls. As such, the Firm ought to have been aware of the importance of systems and controls to prevent and detect all types of financial crime, including money laundering.
9. In deciding upon the appropriate disciplinary sanction, the FSA has taken the following into account:
 - i. RBS Group had commenced a group-wide review of AML systems and controls prior to the FSA visit, which had been due to encompass a review of Coutts' AML systems and controls in November 2010, but which was suspended as a result of that visit;
 - ii. once the FSA had identified concerns, the Firm took steps to address deficiencies in its AML systems and controls, including engaging a third party consultant to review and overhaul its AML processes, revise its training programme for private bankers and review its PEP and other high risk customer files;
 - iii. as a result of that review, a number of improvements and recommendations have already been, or are being, implemented. These include significant remedial amendments to the Firm's PEP and other high risk customer files to ensure that appropriate due diligence information about its customers has been assessed and recorded. The Firm has also exited a number of high risk customer relationships; and
 - iv. since the discovery of the failings in October 2010, Coutts and its senior management have co-operated fully with the FSA's investigation and demonstrated commitment to identifying areas for improvement in the Firm's AML systems and controls and overseeing the implementation of those improvements.

DEFINITIONS

10. The definitions below are used in this Final Notice:

“**the 2007 Regulations**” means the Money Laundering Regulations 2007, which came into force on 15 December 2007.

“**the Act**” means the Financial Services and Markets Act 2000.

“**AML**” means anti-money laundering.

“**the AML team**” means the team within Coutts which had responsibility for AML systems and controls.

“**CDD**” means customer due diligence measures, defined in Regulation 5 of the 2007 Regulations.

“**Coutts**” means Coutts & Company.

“**DEPP**” means the FSA’s Decision Procedures and Penalties Guide as at 15 December 2007.

“**EDD**” means enhanced due diligence measures. The circumstances where EDD should be applied are included in Regulation 14 of the 2007 Regulations.

“**the Firm**” means Coutts & Company.

“**the FSA**” means the Financial Services Authority.

“**high risk customers**” mean individual and corporate customers, including trusts, charities and other legal entities, that were identified by Coutts, in accordance with its AML legal and regulatory obligations, as posing a higher risk for money laundering assessment purposes than standard customers.

“**JMLSG**” means the Joint Money Laundering Steering Group.

“**JMLSG Guidance**” means the guidance issued by the JMLSG in December 2009 on compliance with the legal requirements in the 2007 Regulations, regulatory requirements in the FSA Handbook and evolving practice within the financial services industry. Similar provisions were contained in the previous version of the Guidance, dated December 2007.

“**PEP**” means Politically Exposed Person. A PEP is defined in the 2007 Regulations as “*an individual who is or has, at any time in the preceding year, been entrusted with a prominent public function*” and an immediate family member, or a known close associate, of such a person. The definition only applies to those holding such a position in a state outside the UK, or in a European Community institution or an international body.

“**RBS**” means The Royal Bank of Scotland plc.

“**the Relevant Period**” means 15 December 2007 to 15 November 2010.

“**Risk**” means the area within Coutts which had oversight of the Firm’s business and regulatory risks.

FACTS AND MATTERS

Background

The Firm

11. Coutts is wholly owned by RBS. It is a private bank that provides a range of financial services to customers, including deposit-taking accounts, mortgage lending, wealth management services and tax planning. Coutts’ customers are predominantly high net worth individuals and businesses. Coutts has been authorised to perform regulated activities by the FSA since 1 December 2001.

High risk customers

12. Throughout the Relevant Period, the Firm aimed to expand its international customer base, including in jurisdictions which posed increased risks of money laundering and corruption. During this time, the Firm entered into and maintained business relationships with customers that were of a high risk nature.
13. During the Relevant Period, the Firm had between 600 and 1,200 personal and corporate customers which it had classified as high risk (approximately 1% of its total customer base). Customers were primarily classified as high risk due to their country of origin, incorporation or domicile, particularly where the jurisdiction did not have AML controls equivalent to those in the UK, or the jurisdiction was known to have high levels of corruption. The Firm also had regard to factors including a customer’s profession, business interests and reputation.

PEPs

14. Some of these high risk customers were also classified as PEPs. Coutts, in accordance with RBS policy, applied a PEP definition that was wider than that contained in the 2007 Regulations (as set out in the Definitions section of this Notice) as Coutts also included individuals who held public office within the UK. For the purposes of this Notice, the FSA’s findings in relation to PEPs are findings in relation to those customers who were PEPs according to the definition contained in the 2007 Regulations, and not the wider definition as applied by Coutts.

Due diligence and monitoring requirements

15. Due diligence and monitoring requirements are designed to make it more difficult for the financial services industry to be used for money laundering.
16. CDD obligations require a firm to gather documents, data or other information about a prospective customer. This is in order to identify and verify the identity of the customer, including that of a corporate entity’s beneficial owner. Where the customer is a corporate entity, a trust or other legal entity or arrangement, the firm must take measures to understand the ownership and control structure of the customer. Firms must also obtain from the customer information about the purpose and intended nature of the proposed business relationship.

17. If a firm has assessed that the business relationship with the customer is high risk, including where the customer is a PEP, it must apply EDD. EDD includes, for PEPs and in other appropriate high risk cases, taking adequate measures to establish the source of the customer's wealth and the source of funds which will be involved in the business relationship.
18. A firm must conduct ongoing monitoring of all business relationships. Where the customer is considered to be a high risk customer, that monitoring must be enhanced. Enhanced ongoing monitoring is important to understand any changes to the money laundering risks posed by the customer. It includes keeping relevant information obtained about the customer up-to-date.
19. In addition, a firm must scrutinise transactions conducted by customers. This is to identify any unusual or suspicious activity that may be related to money laundering.

JMLSG Guidance

20. The JMLSG is a body comprising the leading UK trade associations in the financial services industry. Since 1990, the JMLSG has produced advice, which is approved by a Treasury Minister, for the financial services sector on AML controls. The JMLSG Guidance during the Relevant Period provided guidance on compliance with the legal requirements in the 2007 Regulations, regulatory requirements in the FSA Handbook and evolving practice within the financial services industry.
21. When considering whether to take enforcement action in relation to the Firm's breaches, the FSA has had regard to whether the Firm followed the relevant provisions in the JMLSG Guidance (which are listed in the Appendix to this Notice).

The FSA Thematic Review

22. The FSA conducted a thematic review of how banks operating in the UK were managing money laundering risk in higher risk situations. One area of focus for the review was how banks manage the risks arising from PEP and other high risk customers. The FSA's findings were reported in June 2011.
23. In the course of the thematic review, the FSA visited Coutts in October 2010 to assess its AML systems and controls. The results of this visit gave serious cause for concern and a further short notice visit was carried out by the FSA to review a larger sample of PEP and other high risk customer files.
24. After further investigation, including further file reviews¹, the FSA identified failings in respect of Coutts' AML systems and controls in relation to its PEP and other high risk customer relationships. These failings are described below.

¹ In total the FSA reviewed 103 files comprising 55 PEP customer files and 48 files for customers otherwise considered to be high risk.

Risk assessment of prospective and existing customers.

25. The assessment of prospective and existing customers for money laundering risk purposes during the Relevant Period was inadequate and failed to identify all PEP customers. This gave rise to an unacceptable risk that such customers would not be subject to appropriate money laundering controls.

Identification of PEPs

26. New personal or commercial customers would be assigned a private banker who would manage the relationship with that customer.

27. The assigned private banker was responsible for the initial identification of whether a prospective client was a PEP, using information obtained about the customer and by use of software for identification of PEPs. Prospective customers identified as PEPs were then referred to the AML team for approval. As a check on the private bankers' assessments, each month, the AML team tested 5% of customer files that had not been assessed as being PEPs or otherwise high risk. Throughout the Relevant Period, the AML team reported a 100% pass rate for such files.

28. However, Coutts identified in 2011 that a large number of customers (approximately 20% of its high risk customer population) had not been correctly assessed and/or recorded as PEPs. In total, 233 additional personal customers or beneficial owners of corporate customers meeting the Firm's definition of a PEP were identified, of whom 45 were PEPs by virtue of their own positions and the remainder were PEPs by reason of being family members or having a close association with such individuals.

29. Of those 233 customers, 93 were PEPs as defined in the 2007 Regulations. The other 140 held public office within the UK or were close associates and therefore met Coutts' wider definition of a PEP.

30. Of the 93 customers who fell within the definition of PEPs contained in the 2007 Regulations:

- i. 41 were accepted by Coutts as customers during the Relevant Period. In 40 of those cases, the Firm did not identify that the customer was a PEP; in the other case, the customer was not added to the appropriate database as a result of administrative errors; and
- ii. the remaining 52 were existing customers when the 2007 Regulations came into force in December 2007 and the Firm failed to identify that they were in fact PEPs in the course of its ongoing monitoring.

31. This was not an isolated or localised failing. The incorrect classifications of PEPs arose in a number of different private banking teams and during every year of the Relevant Period.

Due diligence on prospective customers

32. The assigned private banker was responsible for gathering the appropriate level of due diligence information for a prospective customer. The Firm had various controls in place

to review this information. All prospective customers identified as PEPs or other high risk customers were subject to approval by the AML team.

33. From the sample of 103 files selected for review by the FSA, there were 61 PEP and other high risk customer files where the business relationship with Coutts began during the Relevant Period. The FSA identified failures with the steps taken by Coutts when establishing the relationship in 38 of these 61 files (62%).
34. The failure to gather the appropriate level of due diligence about prospective high risk customers meant that there was a lack of understanding within Coutts about the money laundering risks associated with those high risk customers and their transactions. This meant that the Firm was unable to analyse and deal with those risks appropriately. This, in turn, led to an unacceptable risk of handling the proceeds of crime.

Customer Due Diligence

35. CDD consists of the fundamental checks that apply to all new customers, whether or not they are high risk. The FSA identified that the CDD gathered was inadequate in 11 of the 61 high risk customer files (18%) reviewed by the FSA where the relationship began during the Relevant Period. Specifically, the FSA identified failings with:
 - i. 11 high risk corporate accounts (relating to five business relationships) where the Firm had failed to question whether there was a legitimate rationale for the complex or opaque ownership and control structures used by the customer. For example, in three cases, the use of bearer shares was not properly considered; and
 - ii. two cases where the Firm had not gathered enough information to understand the business activities of the corporate customer concerned or the intended purpose of the business relationship with Coutts.

Enhanced Due Diligence

36. The gathering of EDD during the Relevant Period for PEP and other high risk customers was inadequate. As a result, matters which should have been considered as part of the EDD process, such as the customers' source of wealth and the source of funds which would be involved in the business relationship with Coutts, were not consistently identified or considered.
37. Coutts' written procedures included a table which set out the minimum standard of verification that was required for high risk customers. However, the procedures were inadequate. The table stated only that due diligence should be enhanced for high risk customers, but it did not give any guidance to the private banker, who was responsible for gathering the appropriate level of due diligence information about a customer, about the types of evidence to gather over and above the standard requirements in order to meet the 'enhanced' requirement.
38. When gathering due diligence information the private bankers were required to complete a checklist designed by the AML team. However, private bankers did not receive proper training in how to complete this document. Nor did the checklist contain any guidance regarding how the private banker should establish the customer's source of wealth, and only contained limited references to considerations relevant to assessing the source of

funds received by Coutts at the outset of the relationship. Such information is important to enable a firm to assess whether subsequent transactions made by the customer are legitimate, for example, to assess whether they are in line with the customer's stated business activities and financial circumstances.

39. The EDD information was insufficient in 35 of the 61 PEP and other high risk customer files (57%) reviewed by the FSA where the business relationship began during the Relevant Period. In particular, the FSA identified the following failings with EDD:
- i. the Firm either failed to establish adequately or failed to evidence that it had established adequately the customer's source of wealth in 30 files (49%). This included cases where the customer's ownership and/or directorship of his/her companies and the income that the customer received from those companies was not established; and
 - ii. the Firm either failed to establish adequately or failed to evidence that it had established adequately the source of funds received at the outset of the relationship in 16 cases (26%). The source of funds was in six cases stated to be the proceeds from the ownership and/or sale of an asset, for example a property or business. However, the Firm did not gather sufficient information to ensure that it had established, for example, the ownership of the asset, the income arising from it or, where appropriate, the subsequent sale of the asset and the proceeds arising from that sale.

Ineffective checks by the AML team

40. Following the initial assessments by the private banker, prospective customers were required to be approved by a senior manager in private banking. All those identified as PEPs or other high risk customers were then required to be further approved by the AML team. The private banker completed an authorisation request form in respect of each such customer and provided that form, together with the due diligence information that had been gathered, to the AML team.
41. The assessment by the AML team of the money laundering risk posed by prospective PEP and other high risk customers during the Relevant Period was inadequate.
42. The Firm operated a performance appraisal and bonus reward scheme for private bankers. This measured performance against a number of financial, risk and compliance criteria. Private bankers' performance appraisals and bonus awards would, in part, be determined by whether they had met their targets for new customer relationships and income for the year. In circumstances where staff are incentivised to bring in business, particularly where the new relationships include high risk customers, it is important that the Firm implements robust controls over the approval process. The assessment by the AML team was meant to be a fundamental control in that approval process.
43. During the Relevant Period, the AML team received approximately 700 formal requests from private bankers to approve customer relationships. Of those formal requests the AML team declined 35 (approximately 5% of all requests). In addition, a smaller number of prospective customers were declined by the AML team following initial approaches by private bankers who did not subsequently seek formal approval.

44. The AML team, however, failed to provide an appropriate level of challenge to the private bankers. This resulted in the possibility that the Firm would accept business relationships involving an unacceptable money laundering risk, or where the risk was not adequately understood. In particular, the AML team relied on the reputation and experience of the private banker involved to an inappropriate extent in making their assessments of customers. This prevented the AML team from fulfilling its role as a robust and independent control over decisions made by private bankers.
45. For example, in two cases reviewed by the FSA, private bankers did not conduct appropriate checks on the customers and, as a result, failed to identify serious criminal allegations against those customers. The AML team, apparently relying on the assessment carried out by the private bankers, approved the customers without gathering further detailed intelligence despite the information gathered by the private banker being limited. Adverse intelligence about the customers was later identified but only by offshore institutions within RBS when the customers applied for international products and services.
46. Further, in the files reviewed by the FSA there were five cases where adverse intelligence about a customer had been identified from credible sources, including allegations of criminal activity. In each case the customers were approved without proper consideration of whether further steps were necessary in order to mitigate risk, notwithstanding that adverse information had been identified by the Firm prior to that approval. That adverse intelligence included allegations of misappropriation of state funds and close business and/or personal associations with individuals wanted by law authorities (in two such cases, there were current international arrest warrants in force).
47. In two cases, the AML team gave insufficient weight to adverse intelligence and approved customers without appropriate further enquiry on the basis that the intelligence revealed only allegations of criminal conduct rather than actual convictions, or because the AML team considered that sufficient time had elapsed since the allegations were first raised. In a third case, RBS had issued a notice to all companies in its group some years before requiring them to close any relationships with a particular family due to their political support for a criminal. The notice was subsequently rescinded but further adverse intelligence about the family came into the public domain. Despite being aware of that adverse intelligence, appropriate steps to mitigate the risks posed by the family were not taken. Whilst the AML team stipulated at account opening that the private banker should establish and document the family members' source of wealth, no checks were made that appropriate steps had been taken and as a result, the information gathered about source of wealth was inadequate.

Level of approval

48. During the Relevant Period, the level of approval that was required by the Firm's policy to begin business relationships with prospective PEP and other high risk customers was reduced. In particular, Coutts' procedures initially required that, after approval by the AML team, approval was given by senior managers within Risk, which was responsible for oversight of the Firm's business and regulatory risks. From 2009 onwards, however, Risk senior management delegated their responsibilities to the AML team. This meant that prospective PEP and other high risk customers were approved by members of the AML team without further senior management oversight.

49. This resulted in a diminution in the rigour of the AML approval and control process over the course of the Relevant Period despite the fact that, throughout the Relevant Period, the Firm aimed to expand its international customer base, including in jurisdictions which posed increased risks of money laundering and corruption.

The New Business team

50. Before a prospective customer was formally accepted by Coutts, the customer due diligence file was checked for completeness by the New Business team and a Due Diligence Manager in that team. This was a central team that checked the documents gathered and processed the opening of the business relationship with the customer. For PEP and other high risk customers this review was in addition to any checks made by the AML team. Whilst the New Business team received training about the AML team's work they did not have formal AML expertise. It was not apparent from the files reviewed by the FSA, including the files considered deficient by the FSA, that the New Business team had raised concerns about the adequacy of the EDD gathered. Accordingly, these checks were not sufficient to remedy deficiencies in the due diligence that had been collected.

Ongoing monitoring

51. Of the 103 PEP and other high risk customer files reviewed by the FSA, there were 50 (49%) where serious concerns with the Firm's ongoing monitoring of the customer were identified. In particular, Coutts failed to ensure that the information it held relevant to its assessment of money laundering risks posed by customers was kept up-to-date. Even where the Firm implemented specific periodic reviews of PEPs and other high risk customers, the reviews were inadequate to ensure that information was updated and the risks posed by customers were properly assessed and managed on a regular basis. In addition, the Firm failed to carry out adequate scrutiny of customer transactions.

52. As a result, the Firm created a significant and unacceptable risk that it would not identify changes in the money laundering risk posed by a customer or unusual or suspicious transactions that may be related to money laundering. Details of these failings are provided below.

Updating information

53. Coutts failed to take appropriate steps to update the information it held about its high risk customers.

54. The FSA's review identified that in 27 of the 103 files (26%) the information gathered about the customer had either not been adequately updated or it was not apparent that the private banker had taken appropriate steps to ensure that the information was kept up-to-date after the business relationship had been established. This included, in a number of cases, where it was not apparent from the file that the private banker had undertaken any regular reviews of the information held, including contacting the customer or searching information in the public domain about the customer's circumstances. As a result, the customers in question had been customers of Coutts, sometimes for a number of years, without relevant changes to their circumstances being noted.

55. In three of the cases reviewed by the FSA, significant adverse intelligence about the customer came into the public domain after the business relationship had been established. However, Coutts failed to identify the adverse intelligence in circumstances where it should easily have been available to the Firm. In addition, in a further three cases reviewed by the FSA, even where adverse intelligence was identified during monitoring, the Firm did not take reasonable steps to assess the risks and take appropriate action to manage those risks.
56. The Firm did not implement adequate systems and procedures to ensure that the information it held on its PEP and other high risk customers was reviewed and assessed on a regular basis. For example, there was no central repository where information on a customer was held. Information was recorded on disparate systems which meant it was difficult for private bankers to have a full appreciation of the nature of a relationship with a particular customer, and of the risk arising from it. Coutts was taking steps to address this issue during the Relevant Period with a proposed new IT system. However, the Firm was unable to implement the new system in a timely manner. Despite this known time lag, the Firm did not implement any mitigating measures, for example by prompting private bankers to check all relevant systems when reviewing the customer's circumstances. The Firm did not identify until 2010, when RBS reviewed its processes, that there was a risk that private bankers did not review all relevant information and that monitoring of its PEP and other high risk customer relationships would, therefore, be ineffective.
57. Even where, in 10 files reviewed by the FSA, the private banker had identified that there were gaps in information (for example, the file noted that source of wealth was "not known") no steps had been taken to rectify the gap.
58. These failings gave rise to an unacceptable risk that material information held about high risk customers was not kept up-to-date.

Annual reviews of PEPs

59. For PEP customers, private bankers were required to conduct an annual review of the customer's circumstances and make a record of the review conducted. In 17 of the 55 (31%) PEP files the FSA reviewed, however, there were inadequacies in the annual review that had been undertaken. This included reviews where the same information had been recorded in the annual review from year to year without an update being considered and where private bankers had confirmed that there had been no changes in the customer's circumstances when they had not in fact sought up-to-date information.
60. The annual review template, designed by the AML team, did not prompt the private banker to update any information or due diligence. There was also no guidance or training given to private bankers on how to complete the annual review template, nor what information was expected to be gathered, assessed and recorded during the annual PEP review, and no guidance or training on the circumstances in which matters should be escalated to the AML team. This meant that changes in customers' risk profiles, even those that would significantly increase the money laundering risks posed by the customer, would not necessarily have been considered by a member of the AML team. Moreover, whilst private bankers were required to confirm on the Firm's systems that annual reviews had taken place, the AML team checked only a small number of the completed reviews each year. This review was insufficient to ensure that the annual reviews were

being conducted properly. This affected the Firm's ability to assess its risk exposure and take appropriate steps where the money laundering risk was high.

61. The Firm has been unable to find the documentation for one or more annual PEP reviews that its systems suggested took place for 14 of the 55 (25%) PEP customer files reviewed by the FSA. It is unclear therefore whether annual reviews were conducted on all PEPs. As a result of the FSA's investigation, the Firm has also identified that, even where reviews were conducted, a number of annual reviews were not saved appropriately on its systems and hard copies were not retained on file, with the result that staff did not, or could not, refer to them when necessary. This further confirms that the value of annual reviews as an AML risk management tool was significantly compromised during the Relevant Period.

Senior management review of PEPs

62. A meeting of senior management from private banking, the AML team, Risk and the senior executive of the Firm was held approximately twice a year to consider the Firm's PEP customers. However, these reviews were insufficient to remedy the deficiencies in the annual PEP reviews conducted by private bankers.
63. The minutes of the meetings during the Relevant Period demonstrate that the discussions related largely to administrative matters, for example, updating management information where the private banker assigned to a customer had changed. The meetings did not routinely consider the EDD held or whether any adverse intelligence had been identified about a customer. The meetings were not therefore sufficient to ensure that any changes in the risks posed by a customer were considered and managed appropriately.

Transaction monitoring

64. Coutts monitored large transactions made through all PEP and other high risk customer accounts for unusual or suspicious activity. Where a large transaction was made, Coutts' procedures required the assigned private banker to review the details of the transaction. For PEP customers, private bankers were also required to confirm annually that they had reviewed all transactions (whether large or otherwise) for the previous year and that they had no suspicions of money laundering. Further monitoring of transactions was also undertaken at RBS Group level.
65. These reviews were however insufficient to identify where transactions were made by PEP and high risk customers outside of their expected account activity. As part of its file review the FSA found seven cases where funds were paid into or out of a customer's account on more than one occasion outside of the expected activity on the account and the transactions were not appropriately identified and assessed by Coutts at the time that the transactions were made. For example, in one case large transfers were made to the customer from a party with no clear connection to the customer. The transfers were not identified as being unusual at the time that they were made and were subsequently noted only during the third party consultant's review of customer files in 2011.
66. The failure to scrutinise transactions appropriately meant that the Firm was unable to assess whether transactions were unusual or suspicious and could be related to money laundering.

Inadequate reviews of the Firm's AML procedures for high risk customers

67. Coutts conducted gap analyses of its AML procedures against RBS standards and guidelines and FSA standards in 2007, 2008 and 2009. The Firm identified that appropriate steps were not being taken to keep information up-to-date for some low risk customers. However, the Firm did not identify that there was a similar deficiency for high risk customers despite the introduction of the 2007 Regulations, which came into force on 15 December 2007 and which introduced new measures for high risk customers. The introduction of these requirements should have prompted the Firm to consider whether its procedures for high risk customers were adequate.

FAILINGS

68. On the basis of the facts and matters set out above, the FSA considers that the Firm breached Principle 3 in that it did not take reasonable care to establish and maintain effective AML systems and controls in relation to high risk customers. These failures were systemic and included the absence of appropriate controls to identify, assess, manage and monitor the money laundering risk posed by the Firm's PEP and other high risk customers. As a result, the Firm did not:

- i. assess adequately the level of money laundering risk posed by prospective and existing high risk customers. This included failing properly to identify and record all politically exposed persons (PEPs);
- ii. gather the appropriate level of due diligence information about a large number of prospective high risk customers;
- iii. apply robust controls when establishing relationships with high risk customers. In particular, the AML team failed to provide an appropriate level of scrutiny and challenge;
- iv. consistently apply appropriate ongoing monitoring to its existing high risk customers to ensure that changes in circumstances and risk profiles were identified, assessed and managed appropriately and that all unusual transactions would be identified; and
- v. carry out adequate reviews of its AML systems and controls for high risk customers.

69. These weaknesses in the Firm's systems and controls resulted in an unacceptable risk of Coutts' handling the proceeds of crime through its PEP and other high risk customer relationships.

70. As well as a breach of Principle 3, these failings amounted to breaches of SYSC 6.1.1R and SYSC 6.3.1R.

SANCTION

71. The FSA's policy on the imposition of financial penalties is set out in Chapter 6 of the Decision Procedure & Penalties Manual ("DEPP") which forms part of the FSA Handbook. Since the majority of the misconduct occurred before the introduction of the FSA's new penalty regime on 6 March 2010, the FSA has applied the penalty regime that was in place before that date. DEPP 6.5.2G sets out the factors that may be of particular

relevance in determining the appropriate level of financial penalty for a firm or approved person. The criteria are not exhaustive and all relevant circumstances of the case are taken into consideration. In determining the appropriate level of sanction, the FSA has had regard to the factors from DEPP 6.5.2G listed below.

Deterrence

72. The financial penalty is required to promote high standards of regulatory conduct by deterring firms which have breached regulatory requirements from committing further contraventions, helping to deter other firms from committing contraventions, and demonstrating generally to firms the benefits of compliant behaviour. It strengthens the message to the industry that it is vital to take proper steps to ensure that AML systems and controls are adequate.

Seriousness of the breaches

73. The FSA has had regard to the seriousness of the breaches, including the nature of the requirements breached, the number and duration of the breaches and the systemic character of the Firm's failings. For the reasons set out in paragraph 8 of this Notice, the FSA considers Coutts' breaches, which persisted for nearly three years, to be particularly serious. The weaknesses in the Firm's systems and controls resulted in an unacceptable risk of Coutts' handling the proceeds of crime through its high risk customer relationships.

The extent to which the breaches were deliberate or reckless

74. The FSA does not consider that Coutts deliberately or recklessly contravened regulatory requirements.

The size, financial resources and other circumstances of the Firm

75. There is no evidence to suggest that Coutts is unable to pay the penalty.

Conduct following the breaches

76. Once the FSA had identified concerns, the Firm engaged a third party consultant to review and overhaul its AML processes, revise its training programme for private bankers and review its PEP and other high risk customer files.

77. As a result of that review, a number of improvements and recommendations have already been, or are being, implemented. These include significant remedial amendments to the Firm's PEP and other high risk customer files to ensure that appropriate due diligence information about its customers has been assessed and recorded. The Firm has also exited a number of high risk customer relationships.

78. Further details of the steps taken by the Firm are set out earlier in this Notice.

Disciplinary record and compliance history

79. Coutts was one of four institutions within RBS which were fined in August 2010 for failing to have adequate systems and controls in place to prevent breaches of UK financial sanctions. Between 15 December 2007 and 31 December 2008 the Firm failed

to adequately screen both its customers, and the payments they made and received, against the sanctions list.

Previous action taken by the FSA in relation to similar findings

80. In determining whether and what financial penalty to impose on Coutts, the FSA has taken into account action taken by the FSA in relation to other authorised persons for comparable behaviour.

FSA guidance and other published material

81. Pursuant to DEPP 6.2.3G and SYSC 6.3.5G, the FSA has had regard to whether Coutts followed the relevant provisions of the JMLSG Guidance when considering whether to take action in respect a breach of its rules on systems and controls against money laundering.

PROCEDURAL MATTERS

Decision maker

82. The decision which gave rise to the obligation to give this Notice was made by the Settlement Decision Makers.

83. This Final Notice is given under, and in accordance with, section 390 of the Act.

Manner of and time for payment

84. The financial penalty must be paid in full by Coutts to the FSA by no later than 6 April 2012, 14 days from the date of the Final Notice.

If the financial penalty is not paid

85. If all or any of the financial penalty is outstanding on 7 April 2012, the FSA may recover the outstanding amount as a debt owed by Coutts and due to the FSA.

Publicity

86. Sections 391(4), 391(6) and 391(7) of the Act apply to the publication of information about the matter to which this notice relates. Under those provisions, the FSA must publish such information about the matter to which this notice relates as the FSA considers appropriate. The information may be published in such manner as the FSA considers appropriate. However, the FSA may not publish information if such publication would, in the opinion of the FSA, be unfair to Coutts or prejudicial to the interests of consumers.

87. The FSA intends to publish such information about the matter to which this Final Notice relates as it considers appropriate.

FSA contacts

88. For more information concerning this matter generally, contact Tepo Din (direct line: 020 7066 6834/fax: 020 7066 6835) of the Enforcement and Financial Crime Division of the FSA.

.....

William Amos
FSA Enforcement and Financial Crime Division

APPENDIX

THE FSA'S PRINCIPLES FOR BUSINESSES

1. Principle 3

A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

RULES AND GUIDANCE

For the period from 15 December 2007 to 31 March 2009

2. SYSC 6.1.1R

A common platform firm must 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.

3. SYSC 6.3.1R

A common platform firm must ensure the policies and procedures established under SYSC 6.1.1 R include systems and controls that:

- (1) enable it to identify, assess, monitor and manage money laundering risk; and
- (2) are comprehensive and proportionate to the nature, scale and complexity of its activities.

4. SYSC 6.3.2G

"Money laundering risk" is the risk that a firm may be used to further money laundering. Failure by a firm to manage this risk effectively will increase the risk to society of crime and terrorism.

5. SYSC 6.3.4G

A common platform firm may also have separate obligations to comply with relevant legal requirements, including the Terrorism Act 2000, the Proceeds of Crime Act 2002 and the Money Laundering Regulations.

6. SYSC 6.3.5G

The FSA, when considering whether a breach of its rules on systems and controls against money laundering has occurred, will have regard to whether a firm has followed relevant provisions in the guidance for the United Kingdom financial sector issued by the Joint Money Laundering Steering Group.

7. SYSC 6.3.6G

In identifying its money laundering risk and in establishing the nature of these systems and controls, a common platform firm should consider a range of factors, including:

- (1) its customer, product and activity profiles;
- (2) its distribution channels;
- (3) the complexity and volume of its transactions;
- (4) its processes and systems; and

(5) its operating environment.

8. SYSC 6.3.7G

A common platform firm should ensure that the systems and controls include:

(1) appropriate training for its employees in relation to money laundering;

(2) appropriate provision of information to its governing body and senior management, including a report at least annually by that firm's money laundering reporting officer (MLRO) on the operation and effectiveness of those systems and controls;

(3) appropriate documentation of its risk management policies and risk profile in relation to money laundering, including documentation of its application of those policies (see SYSC 9);

(4) appropriate measures to ensure that money laundering risk is taken into account in its day-to-day operation, including in relation to:

(a) the development of new products;

(b) the taking-on of new customers; and

(c) changes in its business profile; and

(5) appropriate measures to ensure that procedures for identification of new customers do not unreasonably deny access to its services to potential customers who cannot reasonably be expected to produce detailed evidence of identity.

For the period from 1 April 2009 to 15 November 2010

9. Identical provisions applied during this period, save that the words “common platform firm” were replaced by “firm”.

For the whole of the Relevant Period

10. DEPP 6.2.3G

The FSA's rules on systems and controls against money laundering are set out in SYSC 3.2 and SYSC 6.3. The FSA, when considering whether to take action for a financial penalty or censure in respect of a breach of those rules, will have regard to whether a firm has followed relevant provisions in the Guidance for the UK financial sector issued by the Joint Money Laundering Steering Group.

11. DEPP 6.5.2G

The following factors may be relevant to determining the appropriate level of financial penalty to be imposed on a person under the Act:

(1) Deterrence

When determining the appropriate level of penalty, the FSA will have regard to the principal purpose for which it imposes sanctions, namely to promote high standards of regulatory and/or market conduct by deterring persons who have committed breaches from committing further breaches and helping to deter other persons from committing similar breaches, as well as demonstrating generally the benefits of compliant business.

(2) The nature, seriousness and impact of the breach in question

The FSA will consider the seriousness of the breach in relation to the nature of the rule, requirement or provision breached. The following considerations are among those that may be relevant:

- (a) the duration and frequency of the breach;
- (b) whether the breach revealed serious or systemic weaknesses in the person's procedures or of the management systems or internal controls relating to all or part of a person's business;
- (c) in market abuse cases, the FSA will consider whether the breach had an adverse effect on markets and, if it did, how serious that effect was, which may include having regard to whether the orderliness of, or confidence in, the markets in question has been damaged or put at risk. This factor may also be relevant in other types of case;
- (d) the loss or risk of loss caused to consumers, investors or other market users;
- (e) the nature and extent of any financial crime facilitated, occasioned or otherwise attributable to the breach; and
- (f) in the context of contraventions of Part VI of the Act, the extent to which the behaviour which constitutes the contravention departs from current market practice.

(3) The extent to which the breach was deliberate or reckless

The FSA will regard as more serious a breach which is deliberately or recklessly committed. The matters to which the FSA may have regard in determining whether a breach was deliberate or reckless include, but are not limited to, the following:

- (a) whether the breach was intentional, in that the person intended or foresaw the potential or actual consequences of its actions;
- (b) where the person has not followed a firm's internal procedures and/or FSA guidance, the reasons for not doing so;
- (c) where the person has taken decisions beyond its or his field of competence, the reasons for the decisions and for them being taken by that person;
- (d) whether the person has given no apparent consideration to the consequences of the behaviour that constitutes the breach;
- (e) in the context of a contravention of any rule or requirement imposed by or under Part VI of the Act, whether the person sought any professional advice before the contravention occurred and whether the person followed that professional advice. Seeking professional advice does not remove a person's responsibility for compliance with applicable rules and requirements.

If the FSA decides that the breach was deliberate or reckless, it is more likely to impose a higher penalty on a person than would otherwise be the case.

(4) Whether the person on whom the penalty is to be imposed is an individual

When determining the amount of a penalty to be imposed on an individual, the FSA will take into account that individuals will not always have the resources of a body corporate, that enforcement action may have a greater impact on an individual, and further, that it may be possible to achieve effective deterrence by imposing a smaller penalty on an individual than on a body corporate. The FSA will also consider whether the status, position and/or responsibilities of the individual are such as to make a breach committed by the individual more serious and whether the penalty should therefore be set at a higher level.

(5) The size, financial resources and other circumstances of the person on whom the penalty is to be imposed

(a) The FSA may take into account whether there is verifiable evidence of serious financial hardship or financial difficulties if the person were to pay the level of penalty appropriate for the particular breach. The FSA regards these factors as matters to be taken into account in determining the level of a penalty, but not to the extent that there is a direct correlation between those factors and the level of penalty.

(b) The purpose of a penalty is not to render a person insolvent or to threaten the person's solvency. Where this would be a material consideration, the FSA will consider, having regard to all other factors, whether a lower penalty would be appropriate. This is most likely to be relevant to a person with lower financial resources; but if a person reduces its solvency with the purpose of reducing its ability to pay a financial penalty, for example by transferring assets to third parties, the FSA will take account of those assets when determining the amount of a penalty.

(c) The degree of seriousness of a breach may be linked to the size of the firm. For example, a systemic failure in a large firm could damage or threaten to damage a much larger number of consumers or investors than would be the case with a small firm: breaches in firms with a high volume of business over a protracted period may be more serious than breaches over similar periods in firms with a smaller volume of business.

(d) The size and resources of a person may also be relevant in relation to mitigation, in particular what steps the person took after the breach had been identified; the FSA will take into account what it is reasonable to expect from a person in relation to its size and resources, and factors such as what proportion of a person's resources were used to resolve a problem.

(e) The FSA may decide to impose a financial penalty on a mutual (such as a building society), even though this may have a direct impact on that mutual's customers. This reflects the fact that a significant proportion of a mutual's customers are shareholder-members; to that extent, their position involves an assumption of risk that is not assumed by customers of a firm that is not a mutual. Whether a firm is a mutual will not, by itself, increase or decrease the level of a financial penalty.

(6) The amount of benefit gained or loss avoided

The FSA may have regard to the amount of benefit gained or loss avoided as a result of the breach, for example:

(a) the FSA will propose a penalty which is consistent with the principle that a person should not benefit from the breach; and

(b) the penalty should also act as an incentive to the person (and others) to comply with regulatory standards and required standards of market conduct.

(7) Difficulty of detecting the breach

A person's incentive to commit a breach may be greater where the breach is, by its nature, harder to detect. The FSA may, therefore, impose a higher penalty where it considers that a person committed a breach in such a way as to avoid or reduce the risk that the breach would be discovered, or that the difficulty of detection (whether actual or perceived) may have affected the behaviour in question.

(8) Conduct following the breach

The FSA may take the following factors into account:

- (a) the conduct of the person in bringing (or failing to bring) quickly, effectively and completely the breach to the FSA's attention (or the attention of other regulatory authorities, where relevant);
- (b) the degree of co-operation the person showed during the investigation of the breach by the FSA, or any other regulatory authority allowed to share information with the FSA, such as an RIE or the Takeover Panel. Where a person has fully co-operated with the FSA's investigation, this will be a factor tending to reduce the level of financial penalty;
- (c) any remedial steps taken since the breach was identified, including whether these were taken on the person's own initiative or that of the FSA or another regulatory authority; for example, identifying whether consumers or investors or other market users suffered loss and compensating them where they have; correcting any misleading statement or impression; taking disciplinary action against staff involved (if appropriate); and taking steps to ensure that similar problems cannot arise in the future; and
- (d) whether the person concerned has complied with any requirements or rulings of another regulatory authority relating to the breach (for example, where relevant, those of the Takeover Panel).

(9) Disciplinary record and compliance history

The FSA may take the previous disciplinary record and general compliance history of the person into account. This will include:

- (a) whether the FSA (or any previous regulator) has taken any previous disciplinary action against the person;
- (b) whether the person has previously undertaken not to do a particular act or engage in particular behaviour;
- (c) whether the FSA (or any previous regulator) has previously taken protective action in respect of a firm using its own initiative powers, by means of a variation of a firm's Part IV permission, or has previously requested the firm to take remedial action and the extent to which that action has been taken.
- (d) the general compliance history of the person, including whether the FSA (or any previous regulator) has previously brought to the person's attention, including by way of a private warning, issues similar or related to the conduct that constitutes the breach in respect of which the penalty is imposed.

A person's disciplinary record could lead to the FSA imposing a higher penalty, for example where the person has committed similar breaches in the past.

In assessing the relevance of a person's disciplinary record and compliance history, the age of a particular matter will be taken into account, although a long-standing matter may still be relevant.

(10) Other action taken by the FSA (or a previous regulator)

Action that the FSA (or a previous regulator) has taken in relation to similar breaches by other persons may be taken into account. This includes previous actions in which the

FSA (whether acting by the RDC or the settlement decision makers) and a person on whom a penalty is to be imposed have reached agreement as to the amount of the penalty. As stated at DEPP 6.5.1 G (2), the FSA does not operate a tariff system. However, the FSA will seek to apply a consistent approach to determining the appropriate level of penalty.

(11) Action taken by other domestic or international regulatory authorities

Considerations could include, for example:

(a) action taken or to be taken against a person by other regulatory authorities which may be relevant where that action relates to the breach in question;

(b) the degree to which any remedial or compensatory steps required by other regulatory authorities have been taken (and whether taken promptly).

(12) FSA guidance and other published materials

(a) A person does not commit a breach by not following FSA guidance or other published examples of compliant behaviour. However, where a breach has otherwise been established, the fact that guidance or other published materials had raised relevant concerns may inform the seriousness with which the breach is to be regarded by the FSA when determining the level of penalty.

(b) The FSA will consider the nature and accessibility of the guidance or other published materials when deciding whether they are relevant to the level of penalty and, if they are, what weight to give them in relation to other relevant factors.

(13) The timing of any agreement as to the amount of the penalty

The FSA and the person on whom a penalty is to be imposed may seek to agree the amount of any financial penalty and other terms. In recognition of the benefits of such agreements, DEPP 6.7 provides that the amount of the penalty which might otherwise have been payable will be reduced to reflect the stage at which the FSA and the person concerned reach an agreement.

RELEVANT EXTRACTS FROM PART I AND PART II OF THE JMLSG GUIDANCE

Part I, Chapter 5 – Customer due diligence

5.1 Meaning of customer due diligence measures and ongoing monitoring

12. Paragraph 5.1.4 - Firms must determine the extent of their 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 their supervisory authority that the extent of their CDD measures and monitoring is appropriate in view of the risks of money laundering and terrorist financing.

13. Paragraph 5.1.5 - The CDD measures that must be carried out involve:

(a) identifying the customer, and verifying his identity;

(b) identifying the beneficial owner, where relevant, and verifying his identity; and

(c) obtaining information on the purpose and intended nature of the business relationship.

14. Paragraph 5.1.6 - Where the customer is a legal person (such as a company) or a legal arrangement (such as a trust), part of the obligation on firms to identify any beneficial

15. Paragraph 5.1.9 - Firms must conduct ongoing monitoring of the business relationship with their customers. This is a separate, but related, obligation from the requirement to apply CDD measures.

5.2 Timing of, and non compliance with, CDD measures

16. Paragraph 5.2.6 - Where a firm is unable to apply CDD measures in relation to a customer, the firm

- (a) must not carry out a transaction with or for the customer through a bank account;
- (b) must not establish a business relationship or carry out an occasional transaction with the customer;
- (c) must terminate any existing business relationship with the customer;
- (d) must consider whether it ought to be making a report to SOCA, in accordance with its obligations under POCA and the Terrorism Act.

5.3 Application of CDD measures

17. Paragraph 5.3.1 - Applying CDD measures involves several steps. The firm is required to verify the identity of customers and, where applicable, beneficial owners. Information on the purpose and intended nature of the business relationship must also be obtained.

Nature and purpose of proposed business relationship

18. Paragraph 5.3.21 - A firm must understand the purpose and intended nature of the business relationship or transaction. In some instances this will be self-evident, but in many cases the firm may have to obtain information in this regard.

19. Paragraph 5.3.22 - Depending on the firm's risk assessment of the situation, information that might be relevant may include some or all of the following:

- nature and details of the business/occupation/employment;
- record of changes of address;
- the expected source and origin of the funds to be used in the relationship;
- the initial and ongoing source(s) of wealth and funds (particularly within a private banking or wealth management relationship);
- copies of recent and current financial statements;
- the various relationships between signatories and with underlying beneficial owners;
- the anticipated level and nature of the activity that is to be undertaken through the relationship.

Keeping information up to date

20. Paragraph 5.3.23 - Where information is held about customers, it must, as far as reasonably possible, be kept up to date. Once the identity of a customer has been satisfactorily verified, there is no obligation to re-verify identity (unless doubts arise as to the veracity or adequacy of the evidence previously obtained for the purposes of customer identification); as risk dictates, however, firms must take steps to ensure that they hold appropriate up-to-date information on their customers. A range of trigger

events, such as an existing customer applying to open a new account or establish a new relationship, might prompt a firm to seek appropriate evidence.

5.5 Enhanced due diligence

21. Paragraph 5.5.1 - A firm must apply EDD measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. As part of this, a firm may conclude, under its risk-based approach, that the standard evidence of identity is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer.
22. Paragraph 5.5.5 - A firm should hold a fuller set of information in respect of those customers, or class/category of customers, assessed as carrying a higher money laundering or terrorist financing risk, or who are seeking a product or service that carries a higher risk of being used for money laundering or terrorist financing purposes.
23. Paragraph 5.5.9 - The ML Regulations prescribe three specific types of relationship in respect of which EDD measures must be applied. These are:
 - (a) where the customer has not been physically present for identification purposes;
 - (b) in respect of a correspondent banking relationship;
 - (c) in respect of a business relationship or occasional transaction with a PEP.

Politically exposed persons

24. Paragraph 5.5.18 - Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to firms as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the customer, or the beneficial owner, into a higher risk category.
25. Paragraph 5.5.19 - A PEP is defined as “an individual who is or has, at any time in the preceding year, been entrusted with prominent public functions and an immediate family member, or a known close associate, of such a person”. This definition only applies to those holding such a position in a state outside the UK, or in a Community institution or an international body.
26. Paragraph 5.5.25 - Firms are required, on a risk-sensitive basis, to:
 - have appropriate risk-based procedures to determine whether a customer is a PEP;
 - obtain appropriate senior management approval for establishing a business relationship with such a 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.

Risk-based procedures

27. Paragraph 5.5.28 - It is for each firm to decide the steps it takes to determine whether a PEP is seeking to establish a business relationship for legitimate reasons, and which measures it deems adequate to determine the source of funds and source of wealth. Firms may wish to refer to information sources such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include

information about an official's source of wealth and current business interests. Firms should note that not all declarations are publicly available and that a PEP customer may have legitimate reasons for not providing a copy. Firms should also be aware that some jurisdictions impose restrictions on their PEPs' ability to hold foreign bank accounts or to hold other office or paid employment.

On-going monitoring

28. Paragraph 5.5.30 - Guidance on the on-going monitoring of the business relationship is given in section 5.7. Firms should remember that new and existing customers may not initially meet the definition of a PEP, but may subsequently become one during the course of a business relationship. The firm should, as far as practicable, be alert to public information relating to possible changes in the status of its customers with regard to political exposure. When an existing customer is identified as a PEP, EDD must be applied to that customer.

5.7 Monitoring customer activity

29. Paragraph 5.7.1 - Firms must conduct ongoing monitoring of the business relationship with their customers. Ongoing monitoring of a business relationship includes:
- Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, his business and risk profile;
 - Ensuring that the documents, data or information held by the firm are kept up to date.
30. Paragraph 5.7.3 - The essentials of any system of monitoring are that:
- it flags up transactions and/or activities for further examination;
 - these reports are reviewed promptly by the right person(s); and
 - appropriate action is taken on the findings of any further examination.
31. Paragraph 5.7.12 - Higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring.

Part I, Chapter 7 - Staff awareness, training and alertness

32. Paragraph 7.23 - Relevant employees should be trained in what they need to know in order to carry out their particular role. Staff involved in customer acceptance, in customer servicing, or in settlement functions will need different training, tailored to their particular function. This may involve making them aware of the importance of the "know your customer" requirements for money laundering prevention purposes, and of the respective importance of customer ID procedures, obtaining additional information and monitoring customer activity. The awareness raising and training in this respect should cover the need to verify the identity of the customer, and circumstances when it should be necessary to obtain appropriate additional customer information in the context of the nature of the transaction or business relationship concerned.
33. Paragraph 7.24 - Relevant employees should also be made aware of the particular circumstances of customers who present a higher risk of money laundering or terrorist financing, or who are financially excluded. Training should include how identity should be verified in such cases, what additional steps should be taken, and/or what local checks can be made.

Part II, Chapter 5 – Wealth management

Customer due diligence

34. Paragraph 5.13 - In addition to the standard identification requirement in Part I, paragraphs 5.3.68 – 5.3.78, any wealth management service should have particular regard to the following:

- As a minimum requirement to counter the perceived and actual risks, the firm, and those acting in support of the business, must exercise a greater degree of diligence throughout the relationship which will be beyond that needed for normal retail banking purposes. The firm must endeavour to understand the nature of the client's business and consider whether it is consistent and reasonable, including:
 - the origins of the client's wealth
 - Where possible and appropriate, documentary evidence relating to the economic activity that gave rise to the wealth
 - the nature and type of transactions
 - the client's business and legitimate business structures
 - for corporate and trust structures - the chain of title, authority or control leading to the ultimate beneficial owner, settler and beneficiaries, if relevant and known
 - Where appropriate, the reasons a client is using complex structures
 - the use made by the client of products and services
 - the nature and level of business to be expected over the account
- The firm must be satisfied that a client's use of complex business structures and/or the use of trust and private investment vehicles, has a genuine and legitimate purpose.

Approval of new relationship

35. Paragraph 5.16 - All new wealth management clients should be subject to independent review, and appropriate management approval and sign off.

References

36. Paragraph 5.17 - Reputational searches should be undertaken as a normal part of customer due diligence, which will include checks for negative information. It will sometimes be appropriate to obtain a satisfactory written reference or references from a reputable source or sources before opening an account for a client. The relationship manager should document the nature and length of the relationship between the referee and the client. References should only be accepted when they are:

- received direct – not from the client or third parties
- specifically addressed only to the firm
- verified as issued by the referee

Review of client information

37. Paragraph 5.18 - The firm's policies and procedures should require that the information held relating to wealth management clients be reviewed and updated on a periodic basis, or when a material change occurs in the risk profile of a client. Periodic review of particular clients will be made on a risk-based basis. Wealth management firms should consider reviewing their business with higher risk clients on at least an annual basis.

Enhanced due diligence

38. Paragraph 5.19 - Greater diligence should be exercised when considering business with customers who live in high risk countries, or in unstable regions of the world known for the presence of corrupt practices. Firms must comply with the EDD requirements in the ML Regulations in respect of clients not physically present for identification purposes, and those who are PEPs, see Part I, section 5.5 and paragraph 5.21 below.
39. Paragraph 5.20 - Those types of client that pose a greater money laundering or terrorist financing risk should be subject to a more stringent approval process. Their acceptance as a client or the significant development of new business with an existing higher risk client should be subject to an appropriate approval process. That process might involve the highest level of business management for the wealth management operation in the jurisdiction. Firms should consider restricting any necessary delegation of that role to a recognised risk control function.
40. Paragraph 5.21 - In the case of higher risk relationships, appropriate senior personnel should undertake an independent review of the conduct and development of the relationship, at least annually.

Politically exposed persons

41. Paragraph 5.22 - Firms offering a wealth management service should have particular regard to the guidance in relation to PEPs set out in Part I, paragraphs 5.5.18 to 5.5.30. Relationship managers should endeavour to keep up-to-date with any reports in the public domain that may relate to their client, the risk profile or the business relationship.

Other clients

42. Paragraph 5.23 - Firms should consider conducting similar searches against the names of their prospects for business, including those that may only be known within the business development or marketing functions; and where practicable, third party beneficiaries to whom clients make payments.