Financial Services Authority

FINAL NOTICE

To:	**Habib Bank AG Zurich**
FSA Reference Number:	**113991**
Address:	**42 Moorgate, London EC2R 6JJ**
Date:	**4 May 2012**

1. ACTION

1.1. For the reasons given in this Notice, the FSA hereby imposes a financial penalty of £525,000 on Habib Bank AG Zurich ("Habib") for breach of Principle 3 (management and control) of the FSA's Principles for Businesses.

1.2. Habib agreed to settle at an early stage of the FSA's investigation. It therefore qualified for a 30% (Stage 1) discount under the FSA's executive settlement procedures. Were it not for this discount, the FSA would have imposed a financial penalty of £750,000 on Habib.

2. SUMMARY OF REASONS

2.1. Habib breached Principle 3 because it failed to take reasonable care to establish and maintain adequate anti-money laundering ("AML") systems and controls between 15 December 2007 and 15 November 2010 ("the Relevant Period").

2.2. 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 regard to high risk customers, they risk leaving themselves open to abuse by money launderers. This action supports the FSA's statutory objectives of the reduction of financial crime and the maintenance of confidence in the financial system.

2.3. The failings at Habib continued for almost three years and exposed Habib to an unacceptable risk of handling the proceeds of crime. In particular, Habib failed to:

a) establish and maintain an adequate procedure for assessing the level of money laundering risk posed by prospective and existing customers (including maintaining a flawed High Risk Country List);

b) conduct sufficient enhanced due diligence ("EDD") in relation to higher risk customers;

c) carry out adequate reviews of its AML systems and controls; and

d) revise training adequately to address shortcomings in AML practice identified by the MLRO and to maintain sufficient records of staff completion of AML training and of all AML steps taken on individual customer accounts.

2.4. As part of its investigation, the FSA reviewed some of Habib's customer files and found one or more of the following significant failings in 46 of the 68 files it reviewed:

a) the customer's account had been inappropriately regarded as normal risk rather than higher risk;

b) the EDD conducted was inadequate; and/or

c) EDD had not been conducted prior to transactions occurring on the account.

2.5. In addition to the breach of Principle 3, Habib also breached the following Senior Management Arrangements, Systems and Controls ("SYSC") rules in the FSA Handbook: SYSC 6.1.1 R, SYSC 6.3.1 R, SYSC 6.3.3 R and SYSC 9.1.1 R in that Habib failed to:

a) establish adequate systems and controls to counter the risk of it being used to further financial crime;

b) ensure that it had appropriate AML systems and controls;

c) carry out regular assessments of the adequacy of its AML systems; and

d) keep sufficient records to demonstrate that it had complied with its regulatory requirements.

2.6. Habib's failings merit the imposition of a significant financial penalty. The FSA considers the failings to be particularly serious because:

a) approximately 45% of Habib's 15,500 customers were based outside the UK and these customers accounted for 70% of its deposits. Moreover, approximately one third of Habib's customers (and approximately 50% of Habib's deposits) came from jurisdictions which did not have AML requirements equivalent to those in the UK and/or carried a higher risk of money laundering because they were perceived to have greater levels of corruption (such as Pakistan, from where almost 20% of Habib's customers originated). It was therefore particularly important that Habib had effective systems and controls to prevent and detect money laundering given that it acted as a gateway to the UK financial system for international customers and regularly did business with customers from jurisdictions which presented a higher risk of money laundering;

b) Habib's policy of excluding Pakistan and Kenya from its High Risk Country List was seriously misconceived as the higher risk of money laundering they presented was not negated by Habib's physical presence in those countries or any specialist knowledge of them. When Habib added Pakistan and Kenya to its High Risk Country List in November 2010 following the recommendation of a skilled person required by the FSA to report on various AML matters, it resulted in the reclassification of 170 accounts from normal to higher risk. This represented approximately 8% of the number of higher risk accounts operated by Habib during the Relevant Period;

c) its failings continued for a period of almost three years;

d) the failings were initially identified through the skilled person's report. Habib may not otherwise have identified the failings itself; and

e) the FSA has repeatedly stressed the importance of effective AML controls through its Financial Crime Newsletters, speeches and other communications and the failings in this Notice occurred in a period during which the FSA brought and published other Enforcement cases against a number of institutions for shortcomings in their financial crime systems and controls. As such, Habib ought to have been aware of the importance of adequate systems and controls to prevent and detect all types of financial crime, including money laundering.

2.7. In deciding upon the appropriate disciplinary sanction, the FSA has taken into account that Habib and its senior management have co-operated fully with the FSA's investigation and that Habib took prompt steps to implement a number of AML improvements recommended in the skilled person's report of November 2010. Habib has also agreed to take such further remedial steps as are necessary to ensure that its AML procedures are now suitably robust.

3. DEFINITIONS

3.1. The following definitions are used in this Final Notice:

"**the ML Regulations**" mean the Money Laundering Regulations 2007;

"**the Act**" means the Financial Services and Markets Act 2000;

"**AML**" means anti-money laundering;

"**beneficial owner**" means the term as defined in Regulation 6 of the ML Regulations;

"**CP Index**" means the Corruption Perception Index published by Transparency International;

"**DEPP**" means the FSA's Decisions Procedure and Penalties manual;

"**EDD**" means enhanced due diligence measures. The circumstances where EDD should be applied are included in Regulation 14 of the ML Regulations;

"**the FSA**" means the Financial Services Authority;

"**Habib**" means Habib Bank AG Zurich;

"**High Risk Country**" means a country included in Habib's High Risk Country List;

"**High Risk Country List**" means Habib's list from time to time of High Risk Countries;

"**JMLSG**" means the Joint Money Laundering Steering Group;

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

"**money laundering**" means as defined in the FSA Handbook Glossary;

"**money laundering risk**" means the risk, as described at SYSC 6.3.2G, 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;

"**MLRO**" means Habib's money laundering reporting officer;

"**PEP**" means a politically exposed person. A PEP is defined in the ML Regulations as "an individual who is or has, at any time in the preceding year, been entrusted with a prominent public function by: i) a state other than the UK; ii) a European Community institution; or iii) an international body". The definition includes immediate family members and known close associates of such a person;

"**the Relevant Period**" means the period from 15 December 2007 to 15 November 2010; and

"**the Tribunal**" means the Upper Tribunal (Tax and Chancery Chamber).

4. FACTS AND MATTERS

Background

4.1. Habib is a privately owned Swiss bank. Its operations during the Relevant Period consisted of twelve branches in the UK with a total of approximately 15,500 account holders and approximately 200 staff. Habib offered deposit products (including current accounts and term deposits), private banking, trade finance, correspondent banking, and other products (such as remittance services) to personal and corporate customers. Habib's primary sources of new business were referrals from existing customers or from staff, existing customers referred from group overseas branches, and existing customers seeking new or additional products and services. Habib has been authorised by the FSA since 1 December 2001.

4.2. During the Relevant Period, approximately 45% of Habib's customers were based outside the UK. Habib's target markets included East Africa and South Asia.

Inadequate risk assessment

4.3. During the Relevant Period, Habib operated a risk assessment procedure whereby customers' accounts were automatically regarded as higher risk if they met certain specified criteria (for example, customers who were PEPs, unregistered charities or money service businesses) or accumulated a risk score of three or more points.

4.4. The basic risk scoring criteria were:

a) one point if the customer (or the beneficial owner(s) of the account) was a national of a High Risk Country, as included in Habib's High Risk Country List;

b) two points if the customer was domiciled in a High Risk Country; and

c) two points if the volume of assets (i.e. balance) in the account was over certain thresholds (namely £250,000 for personal accounts, £500,000 for corporate accounts and £1 million for private banking accounts).

4.5. Habib's policy during the Relevant Period was to compile its High Risk Country List by reference to the prevailing CP Index. All countries with a score below three on the CP Index were to be included, with the significant exception of any country in which Habib had a group office. As a result, Pakistan and Kenya were excluded from the High Risk Country List throughout the Relevant Period even though they had CP Index scores below three. Habib's rationale for the exclusion of these countries was that it had specialist knowledge of them as regions in which it operated.

4.6. Habib's risk assessment procedures were inadequate in a number of respects. In particular:

a) Habib's policy of excluding Pakistan (from where almost 20% of its customers originated) and Kenya from its High Risk Country List was seriously misconceived as the higher risk of money laundering presented by these jurisdictions was not negated by its physical presence in those countries or any specialist knowledge of them (although specialist knowledge may assist to identify and manage such risks). This policy had the effect that, for accounts where the risk scoring criteria applied, customers who were domiciled in, or nationals of, Pakistan and Kenya were treated as having the same risk profile as those from a country with a lower perceived risk of corruption, such as customers based in Norway or New Zealand. When Habib added Pakistan and Kenya to its High Risk Country List in November 2010, following the recommendation of a skilled person required by the FSA to report on various AML matters, the classification of approximately 170 accounts was changed from normal to higher risk as a result. This represented approximately 8% of the number of higher risk accounts operated by Habib during the Relevant Period;

b) other countries with a CP Index score below three were omitted in error from the High Risk Country List. The Maldives and Mauritania had scores below three in the 2008 and 2009 CP Indexes but were not included. Further, Gabon, Kiribati and Tanzania (the latter from which Habib had approximately 160 customers) all had scores below three in the 2009 CP Index but were not included in Habib's subsequent 2010 High Risk Country List;

c) Habib was unable to provide any explanation for its selection of a score of three on the CP Index as its cut-off point. Given Habib's customer base and product range and in light of the overall approach which Habib took to the risk assessment of accounts, a score of below three on the CP Index was too low a threshold for determining which countries were high risk. This had the effect that some customers who potentially presented a higher risk of money laundering by reason of their domicile or nationality (for example, Madagascar, Sri Lanka and India which had scores of 3, 3.1 and 3.4 respectively in the 2009 CP Index) were inappropriately treated by Habib as normal risk by default;

d) whilst the CP Index is an appropriate resource to use for the purpose of considering what countries may present a high risk of corruption, Habib should not have used it as its only source for determining its High Risk Country List. The CP Index does not assess the level of perceived corruption for every jurisdiction and during the Relevant Period did not cover some jurisdictions from where Habib had customers (for example, Anguilla and the Turks & Caicos Islands). As a result, Habib treated customers from such countries as normal risk by default, without undertaking any analysis of the prevailing risk of money laundering presented by them;

e) Habib also failed to consider and assess whether the following types of customer (which the JMLSG Guidance suggests are examples of higher risk situations) should be regarded as higher risk:

   i companies incorporated in off-shore jurisdictions as non-resident companies with no local operations but managed from another country;

   ii companies registered in high risk jurisdictions;

   iii where beneficial owners with a significant interest in a corporate customer were resident in a high risk jurisdiction; and

   iv those who were not physically present for identification purposes;

f) Habib's procedures failed to take any account of the jurisdiction in which corporate customers were operating. For example, a company incorporated in the UK but which had operations in Sudan or Zimbabwe would not have been assessed any differently from a UK company with exclusively UK operations; and

g) there was no, or no sufficient, analysis carried out by Habib to ensure that the financial parameters used within the risk scoring system were at an appropriate level to identify adequately customers who posed a higher risk of money laundering.

4.7. The FSA found in its review of 68 of Habib's customer files that:

a) 15 corporate accounts represented a higher risk of money laundering due to the structure and domicile of the legal entity and/or the nature and location of the customers' business activities, but had been inappropriately graded as normal risk;

b) eight accounts were erroneously graded as normal risk despite Habib having gathered information which indicated that the customer did or would meet its higher risk criteria.

4.8. In addition, 11 accounts would have met Habib's high risk criteria had Pakistan and Kenya been included in its High Risk Country List.

Inadequate EDD

4.9. A firm must, on a risk-sensitive basis, apply enhanced due diligence measures when:

a) the customer is not physically present for identification purposes;

b) the firm proposes to have a correspondent banking relationship with a respondent institution from a non-EEA state;

c) the firm proposes to enter into a business relationship with, or conduct an occasional transaction for, a PEP; or

d) in any other situation which, by its nature, presents a higher risk of money laundering.

4.10. EDD includes 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. The central objective of EDD measures is for a firm to better understand the risk associated with a customer so as to be able to decide whether to establish or continue with the business relationship, and, if so, how to mitigate the associated money laundering risk. The information gathered for EDD purposes also forms a basis for a firm's understanding of its customer's affairs so that it may properly undertake enhanced ongoing monitoring of transactions in the light of the higher risk of money laundering which has been identified.

4.11. Habib's EDD arrangements were inadequate as:

a) Habib's procedures failed to require that customers who were not physically present for identification purposes were to be classified as higher risk and accordingly needed to be subject to EDD and enhanced ongoing monitoring; and

b) The FSA found in its file review that EDD had been conducted on 34 files (i.e. those which Habib had regarded as higher risk) and that of these 34 files:

i in 21 files the information gathered by Habib during the EDD process was either insufficient (particularly regarding the customer or beneficial owner's source of wealth and source of funds) and/or not supported by appropriate evidence. For example, where a customer's source of wealth or funds was stated to be the proceeds of a property sale, Habib did not obtain any evidence of the ownership of the property, the occurrence of a sale or the arising proceeds. On other files, where Habib (who applied a wider definition of PEPs than required by the ML Regulations) categorised customers as PEPs on the basis of their connection with a person holding public office (who was thereby a PEP), the EDD it undertook focused on the person who held public office and paid insufficient regard to the account holder and the increased money laundering risk arising from that relationship. In relation to one PEP, who was a customer from Pakistan, Habib was aware of allegations regarding corruption but failed to take sufficient steps to understand the allegations and assess the extent of the money laundering risk posed by the account; and

ii in 14 files EDD was not completed within an appropriate timeframe and/or was only conducted after transactions had already been processed on the account.

4.12. By failing to verify information where appropriate, Habib exposed itself to an increased risk of being used to further money laundering. In addition, by failing always to conduct EDD at the point that an account was first considered to present a higher risk, Habib was unable to use such information to inform its decision as to how to mitigate the increased money laundering risk (which might, in some instances, include declining to open the account or discontinuing the business relationship). Failing to conduct EDD in a timely manner leaves a firm under-informed of money laundering risk and undermines its efforts to undertake adequate enhanced ongoing monitoring of transactions.

Inadequate regular assessment of AML arrangements

4.13. A firm must carry out regular assessments of the adequacy of its AML systems and controls to ensure that they continue to enable it to identify, assess, monitor and manage money laundering risk adequately, and are comprehensive and proportionate to the nature, scale and complexity of its activities.

4.14. During the Relevant Period Habib's assessments of its AML arrangements were inadequate and failed to ensure that its senior management received appropriate information on the operation and effectiveness of its AML systems and controls. In particular, Habib's Annual Statements of Compliance (which also served as the annual reports by the MLRO to senior management):

a) provided descriptions of Habib's policies and procedures rather than an assessment of whether the arrangements had been adequate and effective in practice over the previous year;

b) failed to justify the adequacy and effectiveness of, or even address at all, Habib's transaction monitoring arrangements (in particular the automated monitoring thresholds); and

c) failed to justify the adequacy and effectiveness of, or even address at all, Habib's risk scoring arrangements (in particular the volume of assets thresholds).

Inadequate AML training and record keeping

4.15. During the Relevant Period shortcomings in the AML practice of various staff were regularly identified during the MLRO's branch audit visits and reported by the MLRO for rectification. This would result in written requests from senior management to branch managers for urgent rectification and/or clarification of the matters identified. Habib failed to use these findings to identify AML training needs amongst staff and inform future training. Further, the regularity and recurrence of these shortcomings demonstrates that some staff did not have a sufficient understanding of Habib's AML policy.

4.16. In addition, during the Relevant Period senior executives and branch managers were required by Habib to attend a minimum of one AML training session each year and all other staff a minimum of one AML training session every two years. However, there were discrepancies between Habib's AML training records and the general training records maintained for individual members of staff. Further, some staff were not recorded as having attended AML training in line with Habib's policy. A firm cannot be assured that it has met its legal obligation to provide its staff with adequate AML training without sufficient training records.

4.17. The FSA's file review exercise also identified that Habib did not always maintain sufficient records of all of the AML steps it took in relation to individual customer accounts, including:

a) whether personal customers and the beneficial owners of non-resident corporate customers had been physically present for identification; and

b) whether the risk classification of individual customer accounts had been re-considered as part of regular account reviews.

4.18. The lack of clear records on these matters made it difficult for the FSA to assess whether Habib had complied with the relevant legal and regulatory requirements and its own policy.

5. FAILINGS

5.1. The regulatory provisions relevant to this Final Notice are referred to in the Appendix.

5.2. Habib breached Principle 3 because during the Relevant Period it failed to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. This included the failings in respect of its AML systems and controls set out below.

Risk management and AML systems and controls

5.3. Habib's risk assessment procedures in relation to AML were inadequate in a number of respects. In particular, it excluded Pakistan and Kenya from its High Risk Country List on the basis that it had specialist knowledge of them, which was inappropriate as this failed to negate the higher risk of money laundering presented by these jurisdictions. When Habib added Pakistan and Kenya to its High Risk Country List in November 2010, following the recommendation of a skilled person required by the FSA to report on various AML matters, the risk classification of 170 accounts was changed from normal to higher risk as a result. This represented approximately 8% of the number of higher risk accounts operated by Habib during the Relevant Period.

5.4. A number of other countries with a CP Index score below three were omitted, in error, from the High Risk Country List. Habib was unable to explain why it chose a score of three on the CP Index as its cut-off point for high risk. Given Habib's customer base and product range and in light of the overall approach which Habib took to risk assessment this was too low a threshold for determining which countries were high risk and meant that some customers who potentially presented a higher risk of money laundering by reason of their domicile or nationality were inappropriately treated by Habib as normal risk by default.

5.5. Habib failed to consider and assess the increased risk posed by, for example, corporate customers incorporated in off-shore jurisdictions as non-resident companies with no local operations or corporate companies operating in high risk jurisdictions.

5.6. In addition, Habib's EDD arrangements, which formed part of its AML systems and controls, were inadequate. For example, Habib's procedures failed to require that customers who were not physically present for identification purposes were to be classified as higher risk and accordingly needed to be subject to EDD and enhanced ongoing monitoring.

5.7. In a number of cases where EDD was conducted Habib gathered insufficient information (particularly regarding the customer or beneficial owner's source of wealth and source of funds) and/or did not support the information gathered by appropriate evidence. In a number of instances EDD was not completed within an appropriate timeframe and/or was only conducted after transactions had already been processed on the account.

5.8. For these reasons, Habib's failings in relation to risk management and the establishment of adequate AML controls as well as in relation to EDD demonstrate not only a breach of Principle 3 in that it failed to have appropriate systems and controls in place, but also a breach of SYSC 6.1.1R, because Habib failed to have adequate systems and controls in place to prevent it being used to further financial crime, and a breach of SYSC 6.3.1R, in that Habib failed to ensure that it had appropriate policies and procedures in place to enable it to identify, assess, monitor and manage money laundering risk.

Inadequate regular assessment of AML arrangements

5.9. Habib's assessments of its AML arrangements were inadequate and failed to ensure that its senior management received appropriate information on the operation and effectiveness of its AML systems and controls. The annual reports by the MLRO to senior management (Habib's Annual Statements of Compliance) did not assess whether the arrangements had been adequate and effective in practice over the previous year. These reports also failed to address Habib's transaction monitoring arrangements (in particular the automated monitoring thresholds) or its risk scoring arrangements (in particular the volume of assets thresholds).

5.10. Habib's failings in this regard demonstrate not only a breach of Principle 3 in that it failed to have appropriate systems and controls in place but also a breach of SYSC

6.3.3R in that it failed to carry out a sufficient assessment of these systems and controls to ensure that they continued to comply with SYSC 6.3.1R.

Inadequate AML training and record keeping

5.11. Habib failed to use findings of shortcomings in AML practices of staff identified by the MLRO to identify AML training needs amongst staff and inform future training.

5.12. Habib also failed to keep sufficient records of AML training provided to staff. In addition, it did not always maintain sufficient records of all of the AML steps it took in relation to individual customer accounts, including:

a) whether personal customers and the beneficial owners of non-resident corporate customers had been physically present for identification; and

b) whether the risk classification of individual customer accounts had been re-considered as part of regular account reviews.

5.13. The lack of clear records on these matters made it difficult for the FSA to assess whether Habib had complied with the relevant legal and regulatory requirements and its own policy. As well as demonstrating a breach of Principle 3 in that the systems and controls in place were inadequate, this failing was also a breach of SYSC 9.1.1R because Habib did not keep orderly records which were sufficient to enable the FSA to monitor its compliance with the requirements under the regulatory system.

6. SANCTION

Relevant guidance on sanction

6.1. The FSA has considered the disciplinary and other options available to it and has concluded that a financial penalty is the appropriate sanction in the circumstances of this particular case.

6.2. 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 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 whether a financial penalty is appropriate and the amount.

Deterrence

6.3. The FSA considers that the financial penalty will 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 benefit of compliant behaviour. It will strengthen the message to the industry that it is vital for firms to take proper steps to ensure that their AML systems and controls are adequate.

Seriousness of the breaches

6.4. The FSA has had regard to the seriousness of the breaches, including the nature of the requirements breached and the number and duration of the breaches. For the reasons set in paragraph 2.6 of this Notice, the FSA considers that Habib's breaches, which continued for nearly three years, are of a serious nature. The weaknesses in its systems and controls resulted in an unacceptable risk that Habib could have handled the proceeds of crime through its customer relationships.

The extent to which the breach was deliberate or reckless

6.5. The FSA does not consider that Habib deliberately or recklessly contravened regulatory requirements.

The size, financial resources and other circumstances of the Firm

6.6. The FSA has taken into account Habib's size and financial resources. There is no evidence to suggest that Habib is unable to pay the penalty.

Conduct following the breaches

6.7. Since the commencement of the FSA's investigation, Habib has worked in an open and cooperative manner with the FSA. Habib also took prompt steps to implement a number of improvements recommended in the skilled person's report.

Disciplinary record and compliance history

6.8. The FSA has taken into account the fact that Habib has not been the subject of previous disciplinary action.

Previous action taken by the FSA in relation to similar findings

6.9. In determining whether and what financial penalty to impose on Habib, 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

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

7. PROCEDURAL MATTERS

Decision makers

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

7.2. This Final Notice is given to Habib under and in accordance with section 390 of the Act.

Manner of and time for payment

7.3 The financial penalty must be paid in full by Habib to the FSA by no later than 18 May 2012, 14 days from the date of the Final Notice.

If the financial penalty is not paid

7.4 If all or any of the financial penalty is outstanding on 19 May 2012, the FSA may recover the outstanding amount as a debt owed by Habib and due to the FSA.

Publicity

7.5 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 Habib or prejudicial to the interests of consumers.

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

FSA contacts

7.7 For more information concerning this matter generally, you should contact Lance Ellison (direct line: 020 7066 2422 / fax: 020 7066 2423) of the Enforcement and Financial Crime Division of the FSA.

Signed:

....

William Amos

FSA Enforcement and Financial Crime Division

APPENDIX

THE FSA'S PRINCIPLES FOR BUSINESSES

Principle 3 states:

> *"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

1. SYSC 6.1.1 R states:

   "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."

2. SYSC 6.3.1 R states:

   "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."

3. SYSC 6.3.2 G states:

   ""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."

4. SYSC 6.3.3 R states:

   "A common platform firm must carry out a regular assessment of the adequacy of these systems and controls to ensure that they continue to comply with SYSC 6.3.1R."

5. SYSC 6.3.5 G states:

   "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."

6. SYSC 6.3.6 G states:

"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."*

7. SYSC 9.1.1 R states:

"*A firm must arrange for orderly records to be kept of its business and internal organisation, including all services and transactions undertaken by it, which must be sufficient to enable the FSA or any other relevant competent authority under MiFID or the UCITS Directive to monitor the firm's compliance with the requirements under the regulatory system, and in particular to ascertain that the firm has complied with all obligations with respect to clients*".

For the period from 1 April 2009 to 15 November 2010

8. Identical provisions applied during this period, save that the words *"common platform firm"* were removed and replaced by "*firm*".

For the whole of the Relevant Period

9. DEPP 6.2.3 G

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.

10. DEPP 6.5.2 G

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 the Money Laundering Regulations 2007

Enhanced customer due diligence and ongoing monitoring (Regulation 14)

(1) A relevant person must apply on a risk-sensitive basis enhanced customer due diligence measures and enhanced ongoing monitoring—

(a) in accordance with paragraphs (2) to (4);

(b) in any other situation which by its nature can present a higher risk of money laundering or terrorist financing.

(2) Where the customer has not been physically present for identification purposes, a relevant person must take specific and adequate measures to compensate for the higher risk, for example, by applying one or more of the following measures—

(a) ensuring that the customer's identity is established by additional documents, data or information;

(b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution which is subject to the money laundering directive;

(c) ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution.

(3) A credit institution ("the correspondent") which has or proposes to have a correspondent banking relationship with a respondent institution ("the respondent") from a non-EEA state must—

(a) gather sufficient information about the respondent to understand fully the nature of its business;

(b) determine from publicly-available information the reputation of the respondent and the quality of its supervision;

(c) assess the respondent's anti-money laundering and anti-terrorist financing controls;

(d) obtain approval from senior management before establishing a new correspondent banking relationship;

(e) document the respective responsibilities of the respondent and correspondent; and

(f) be satisfied that, in respect of those of the respondent's customers who have direct access to accounts of the correspondent, the respondent—

(i) has verified the identity of, and conducts ongoing monitoring in respect of, such customers; and

(ii) is able to provide to the correspondent, upon request, the documents, data or information obtained when applying customer due diligence measures and ongoing monitoring.

(4) A relevant person who proposes to have a business relationship or carry out an occasional transaction with a politically exposed person must—

(a) have approval from senior management for establishing the business relationship with that person;

(b) take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or occasional transaction; and

(c) where the business relationship is entered into, conduct enhanced ongoing monitoring of the relationship.

(5) In paragraph (4), "a politically exposed person" means a person who is—

(a) an individual who is or has, at any time in the preceding year, been entrusted with a prominent public function by—

(i) a state other than the United Kingdom;

(ii) a Community institution; or

(iii) an international body,

including a person who falls in any of the categories listed in paragraph 4(1)(a) of Schedule 2;

(b) an immediate family member of a person referred to in sub-paragraph (a), including a person who falls in any of the categories listed in paragraph 4(1)(c) of Schedule 2; or

(c) a known close associate of a person referred to in sub-paragraph (a), including a person who falls in either of the categories listed in paragraph 4(1)(d) of Schedule 2.

(6) For the purpose of deciding whether a person is a known close associate of a person referred to in paragraph (5)(a), a relevant person need only have regard to information which is in his possession or is publicly known.

Policies and procedures (Regulation 20)

(1) A relevant person must establish and maintain appropriate and risk-sensitive policies and procedures relating to—

(a) customer due diligence measures and ongoing monitoring;

(b) reporting;

(c) record-keeping;

(d) internal control;

(e) risk assessment and management;

(f) the monitoring and management of compliance with, and the internal communication of, such policies and procedures,

in order to prevent activities related to money laundering and terrorist financing.

(2) The policies and procedures referred to in paragraph (1) include policies and procedures—

(a) which provide for the identification and scrutiny of—

(i) complex or unusually large transactions;

(ii) unusual patterns of transactions which have no apparent economic or visible lawful purpose; and

(iii) any other activity which the relevant person regards as particularly likely by its nature to be related to money laundering or terrorist financing;

(b) which specify the taking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products and transactions which might favour anonymity;

(c) to determine whether a customer is a politically exposed person;

(d) under which—

(i) an individual in the relevant person's organisation is a nominated officer under Part 7 of the Proceeds of Crime Act 2002(1) and Part 3 of the Terrorism Act 2000(2);

ii) anyone in the organisation to whom information or other matter comes in the course of the business as a result of which he knows or suspects or has reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing is required to comply with Part 7 of the Proceeds of Crime Act 2002 or, as the case may be, Part 3 of the Terrorism Act 2000; and

(iii) where a disclosure is made to the nominated officer, he must consider it in the light of any relevant information which is available to the relevant person and determine whether it gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion that a person is engaged in money laundering or terrorist financing.

(3) Paragraph (2)(d) does not apply where the relevant person is an individual who neither employs nor acts in association with any other person.

(4) A credit or financial institution must establish and maintain systems which enable it to respond fully and rapidly to enquiries from financial investigators accredited under section 3 of the Proceeds of Crime Act 2002 (accreditation and training), persons acting on behalf of the Scottish Ministers in their capacity as an enforcement authority under that Act, officers of Revenue and Customs or constables as to—

(a) whether it maintains, or has maintained during the previous five years, a business relationship with any person; and

(b) the nature of that relationship.

(5) A credit or financial institution must communicate where relevant the policies and procedures which it establishes and maintains in accordance with this regulation to its branches and subsidiary undertakings which are located outside the United Kingdom.

(6) In this regulation—

"politically exposed person" has the same meaning as in regulation 14(4);

"subsidiary undertaking" has the same meaning as in regulation 15.

Training (Regulation 21)

A relevant person must take appropriate measures so that all relevant employees of his are—

(a) made aware of the law relating to money laundering and terrorist financing; and

(b) regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.

OTHER RELEVANT PROVISIONS

Relevant extracts from the JMLSG Guidance

Part I, Chapter 5 – Customer due diligence

5.5 *Enhanced due diligence*

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.

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.

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

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.

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.

Paragraph 5.5.25 - Firms are required, on a risk-sensitive basis, to:

a) have appropriate risk-based procedures to determine whether a customer is a PEP;
b) obtain appropriate senior management approval for establishing a business relationship with such a customer;
c) take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction; and

d) conduct enhanced ongoing monitoring of the business relationship.

Risk-based procedures

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

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.

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

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.

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.