



---

## FINAL NOTICE

---

To: **EFG Private Bank Ltd**  
FSA Reference Number: 144036  
Date: 28 March 2013

### 1. ACTION

- 1.1. For the reasons given in this Notice, the FSA hereby impose on EFG Private Bank Ltd (EFG or the Firm) a financial penalty of £4,200,000 for breaches of Principle 3 (management and control) of the FSA's Principles for Businesses (the Principles) which occurred between 15 December 2007 and 25 January 2011 (the Relevant Period).
- 1.2. EFG agreed to settle at an early stage of the FSA's investigation. The Firm 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 £6,000,000 on EFG.

### 2. SUMMARY OF REASONS

- 2.1. EFG 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 were identified by the Firm as presenting a higher risk of money laundering for the purposes of the 2007 Regulations (higher risk customers), including those customers deemed to be a politically exposed person (PEP).
- 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 respect to higher 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 maintenance of market confidence enshrined in statute. Both of these objectives are endangered by failures in this regard.

2.3. The failings at EFG were serious, systemic and continued for more than three years. The weaknesses in EFG's controls resulted in an unacceptable risk of it handling the proceeds of crime. In particular, the Firm did not at all times:

- (1) maintain adequate and effective systems and controls to identify, assess and manage potential money laundering risks associated with higher risk customers;
- (2) gather sufficient levels of enhanced due diligence (EDD) information in relation to certain higher risk customers; and
- (3) conduct the appropriate level of ongoing monitoring for its existing higher risk customers.

2.4. As part of its investigation, the FSA reviewed a sample of 99 of EFG's higher risk customer files, each relating to separate individuals or entities, which between them related to the affairs of 72 individuals. 54 of the files related to PEPs (30 individuals). The FSA found that in a substantial majority of the files, EFG had failed to do one or more of the following:

- (1) document that potential money laundering risks posed by prospective higher risk customers had been fully considered and appropriate action taken to mitigate those risks through the Firm's records;
- (2) demonstrate that it had followed the Firm's policies and procedures consistently to manage money laundering risks associated with higher risk customers;
- (3) adequately establish, or record how it had established, the source of wealth and funds of higher risk customers; and
- (4) conduct ongoing reviews of higher risk customer files periodically to ensure the information and risk assessment was up-to-date and that the activity on accounts was consistent with expected activity.

2.5. In addition to the breach of FSA Principle 3, EFG also breached the Senior Management Arrangements, System and Controls (SYSC) rules in the FSA Handbook specifically SYSC 6.1.1R, SYSC 6.3.1R and previously applicable versions of these rules.

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

- (1) EFG provides private banking services to, and acts as a gateway to the UK financial system for, high net worth international customers, including some

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 identified by industry recognised sources as having a greater level of corruption.

- (2) The failings continued for a period of over three years.
- (3) The failings were not identified by the Firm.
- (4) The failings in this Notice also 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, 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.

2.7. In deciding upon the appropriate sanction, the FSA has taken the following into account:

- (1) Since the discovery of the failings in January 2011, EFG 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.
- (2) A number of improvements have already been, or are being, implemented. These include significant remedial work to the Firm's higher risk customer files to ensure that appropriate due diligence information about its customers has been assessed and recorded.

### **3. DEFINITIONS**

3.1. The definitions below are used in this Notice:

- (1) "the 2007 Regulations" or "the Regulations" means the Money Laundering Regulations 2007, which came into force on 15 December 2007.
- (2) "the Act" means the Financial Services and Markets Act 2000.
- (3) "AML" means anti-money laundering.
- (4) "CDD" means customer due diligence measures, defined in Regulation 5 of the 2007 Regulations.
- (5) "Compliance" means the compliance department within the Firm.
- (6) "CRO" means client relationship officer, an employee of the Firm who manages customer relationships.
- (7) "DEPP" means the FSA's Decision Procedures and Penalties Guide.

- (8) “EDD” means enhanced due diligence measures. The circumstances where EDD should be applied are included in Regulation 14 of the 2007 Regulations.
- (9) “EFG” means EFG Private Bank Ltd.
- (10) “EFGI” means EFG International AG.
- (11) “EFGI Group” or “Group” means EFGI and its subsidiaries, including EFG.
- (12) “the Firm” means EFG.
- (13) “the FSA” means the Financial Services Authority.
- (14) “higher risk customers” mean individual and corporate customers, including those customers deemed to be a politically exposed person (PEP), that present a higher risk of money laundering or terrorist financing for the purposes of the 2007 Regulations.
- (15) “JMLSG” means the Joint Money Laundering Steering Group.
- (16) “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.
- (17) “PEP” means a 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.
- (18) “the Relevant Period” means 15 December 2007 to 25 January 2011.

#### **4. FACTS AND MATTERS**

##### **Background**

- 4.1. EFG is the UK private banking subsidiary of the EFGI Group. The EFGI Group is a global private banking group offering private banking and asset management services in 30 countries and with 2,300 employees. EFGI is a limited liability company incorporated and domiciled in Switzerland and listed on the SIX Swiss Exchange.
- 4.2. EFG supplies private banking and wealth management services, comprising investment management, banking and credit services and financial planning. During the Relevant Period, 41% of EFG’s customers were based in the UK, the remainder based in overseas jurisdictions. EFG has been authorised by the FSA since 1 December 2001. In the Relevant Period EFG employed approximately 200 private

banking and wealth management staff.

- 4.3. EFG provides private banking services to high net worth individuals, including some from overseas jurisdictions identified by industry recognised sources as presenting a higher risk of money laundering and/or bribery and corruption. As at the end of 2011, around 12% (or around 400) of EFG's 3,342 customer accounts were held by customers deemed by the Firm to pose a higher risk of money laundering or reputational risk, 94 of which were held by PEPs. In addition to PEPs that met the definition as contained in the 2007 Regulations, EFG's PEP population contained six UK domestic PEPs and a further 23 that met the Swiss legal definition of a PEP. Once a customer is rated as PEP, they are considered by EFG to be in the highest risk category.

#### ***AML legal and regulatory obligations***

- 4.4. Firms are required by the 2007 Regulations and the FSA Handbook to implement and maintain systems and controls to prevent and detect money laundering. Further to the 2007 Regulations a firm must also be able to demonstrate to its supervisory authority that the extent of the customer due diligence measures it applies is appropriate in view of the risks of money laundering and terrorist financing it faces.
- 4.5. 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.
- 4.6. The FSA's SYSC rules provide that when considering whether a breach of its rules on systems and controls against money laundering has occurred, the FSA will have 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***

- 4.7. In June 2011 the FSA reported on the findings of a thematic review of how banks operating in the UK were managing money laundering risk in higher risk situations including the risks arising from PEPs and other higher risk customers.
- 4.8. As part of the thematic review, the FSA visited EFG on 25 and 26 January 2011 to assess its AML systems and controls. The results of this visit gave the FSA serious cause for concern.
- 4.9. After further investigation, including further file reviews, the FSA identified failings in respect of EFG's AML systems and controls in relation to its PEP and other high risk customer relationships. These failings are described below.

## Management of the Firm's money laundering risks

- 4.10. To implement its obligations under the 2007 Regulations, EFG was required to put in place adequate and risk-sensitive AML policies and procedures. This means that EFG had to identify and assess its money laundering risk and put in place systems and controls adequately to manage and mitigate this risk.
- 4.11. EFG's policies and procedures set out the risk factors which had been identified as higher risk for the Firm for the purpose of managing the money laundering risks faced by the business. These included PEP risk, country risk, occupational risk and criminal connections risk. In addition EFG's policy dictated the controls in place to manage these risks, including not accepting or maintaining relationships with individuals found to pose an unacceptable risk.
- 4.12. As part of a prior anti-money laundering review in 2009, the FSA had found that EFG's written policies and procedures were compliant with the 2007 Regulations. This included the review of a small sample of customer files, including some higher risk files, which did not highlight any compliance issues.
- 4.13. However, the FSA found during its investigation that of the 36 files opened during the Relevant Period, there were 17 customer files where EFG's customer due diligence process highlighted adverse information, including allegations of fraud or corruption, but where there was insufficient or inadequate information on the files to understand how senior management had, under the Firm's own policies and procedures, adequately recognised, evaluated and mitigated the associated risk of money laundering at account opening or during the course of the relationship.
- 4.14. In one case a note from the CRO suggested that the prospective client had acquired their wealth through their father's business activities and connections. Further research suggested that there were allegations that the customer's father had been connected to organised crime, money laundering and murder. Despite these serious allegations, there was insufficient information on file to understand how EFG had concluded that the increased risk associated with the account was acceptable and how these risks were evaluated or how they would be mitigated. Similarly, in another file a third party intelligence report commissioned by EFG concluded that establishing or maintaining a business relationship with the customer's father, who was recorded as their source of funds, *'could expose (EFG) to heightened reputational and/or financial risks.'* Nevertheless, an account was opened for this customer and there was no evidence on file of how these comments were addressed or how any risks would be mitigated.
- 4.15. The lack of appropriate records as to steps taken to mitigate risks also meant that there was a potential impact on the effectiveness of the Firm's on-going monitoring of higher risk customer files.
- 4.16. By not fully documenting the assessment of the money laundering risks which it had identified during due diligence and ongoing monitoring, EFG was exposed to a heightened risk of handling the proceeds of crime.
- 4.17. EFGI Group policies during the Relevant Period precluded EFG from entering into

relationships with customers which they could or should suspect may be involved in criminal activity or know or should reasonably be expected to know have been charged or convicted of criminal offences such as, but not limited to, narcotics trafficking, corruption, embezzlement of public funds or money laundering.

- 4.18. Out of the 17 files referred to in paragraph 4.13 above, the FSA found 13 files where EFG had established a business relationship with customers subject to allegations of criminal activity or where they had been charged with criminal offences including corruption and money laundering. The Firm accepted them as customers after concluding that the allegations were unsubstantiated or politically motivated, but without sufficient evidence being placed on the file of the justification for how the Firm came to that view.
- 4.19. In addition, the FSA found evidence in a very small number of files that specific controls, including account restrictions, put in place by the Firm to mitigate AML risks were not implemented or amended without any recorded justification. These ranged from requiring all funds deposited into the account to be properly verified by supporting documentation or the accounts being restricted to not accept deposits at all. The fact that such controls were not implemented exposed the Firm to an unacceptable risk of handling the proceeds of crime.
- 4.20. In one example, an account was set up to allow the customer to obtain an investor visa. Due to the customer's husband, the customer's source of wealth/funds, being implicated in a bribery case the account was restricted to transactions relating to the investor visa. Despite this, soon after the account was set up, substantial funds unrelated to the visa were remitted to the account. As the account was blocked this was identified and queried by Compliance which was told by the CRO that this activity had been approved by senior management. However, there was no contemporaneous record to explain what change in circumstances had justified the decision by senior management to amend the restrictions.

### **Inadequate EDD**

- 4.21. In accordance with the 2007 Regulations a firm must, on a risk sensitive basis, apply enhanced due diligence measures when:
  - (1) the customer is not physically present for identification purposes;
  - (2) the firm proposes to have a correspondent banking relationship with a respondent institution from a non-EEA state;
  - (3) the firm proposes to enter into a business relationship with, or conduct an occasional transaction for, a PEP; or
  - (4) in any other situation which, by its nature, presents a higher risk of money laundering.
- 4.22. The main objective of EDD is to ensure a firm has a better understanding of the risks associated with particular customers thereby enabling a firm to decide whether to establish or continue with the business relationships and, where necessary, to mitigate

any risk of money laundering. A firm must be able to demonstrate that the extent of the enhanced due diligence measures it applies is commensurate with the money-laundering and any terrorist financing risks posed by the particular customer.

- 4.23. 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.
- 4.24. EDD measures include taking adequate measures to establish the customer's source of wealth and source of funds which are involved in the business relationship or occasional transaction.

#### ***Establishing source of wealth***

- 4.25. Consistent with its regulatory obligations, EFG's procedures required CROs to produce an explanation of a customer's source of wealth with appropriate supporting documentation.
- 4.26. The FSA found that the majority of the 36 files opened during the Relevant Period recorded an explanation of customer's wealth but failed to hold adequate supporting documentation. Whilst all files contained some supporting documentation, in the majority of cases this was insufficient to demonstrate that the Firm had obtained information that fully supported the recorded explanation of the source or sources of wealth. For instance, where the source of wealth was recorded as being from companies of which the customer was the beneficial owner, the file contained information about the company, often from the internet, but insufficient documentation adequately to demonstrate the customer's ownership.
- 4.27. In some instances, Compliance requested further information or evidence from CROs, which was not forthcoming or resulted in insufficient responses, which were not queried. In one example, the CRO from an overseas EFGI group company responded to a query regarding the funds used to purchase investments, from which the customer's wealth was derived '*I do not know where the funds for her original investment came from as I did not know her at that thiem (sic) but they were her funds and not anyone else's,*' the implication being the customer's wealth was not as a result of her father who was implicated in a substantial corruption case. However, there was no evidence on file to show how the further investigation carried out by the Firm was sufficient to satisfy itself that this was the position.
- 4.28. In some cases, a failure to verify a higher risk customer's source of wealth meant that the Firm was unable to demonstrate how it satisfied itself of the legitimacy of the source of that customer's wealth. As a result EFG, in those cases, could not make an informed decision about accepting customers associated with higher money laundering risks or take steps to mitigate adequately any money laundering risks.

#### ***Establishing source of funds***

- 4.29. In a majority of the 36 customer files reviewed that were opened during the Relevant Period, EFG had failed to adequately establish or failed to evidence that it had established the source of funds that had been used in customer relationships identified



by the Firm as higher risk. In some cases a failure to verify the source of funds where EFG would have been expected to have done so meant that EFG was exposed to heightened risks of handling the proceeds of crime. In one example, EFG accepted a multimillion pound deposit which it was told by the customer related to the sale of overseas property. Compliance requested a copy of the sale contract prior to accepting the funds, but none was provided and the funds were accepted regardless.

- 4.30. Without establishing a customer's source of funds, it is not clear how EFG satisfied itself that funds deposited in the EFG accounts originated from a legitimate source and ultimately that these accounts were not being used to launder the proceeds of crime.

#### **Inadequate enhanced ongoing monitoring**

- 4.31. In accordance with the 2007 Regulations, a firm must conduct ongoing monitoring of all business relationships. Where the customer is considered to be higher risk, that monitoring must be enhanced. Enhanced ongoing monitoring is important for understanding any changes to the money laundering risks posed by customers. It includes performing regular reviews of what is known about customers and taking steps to ensure that information obtained about customers remains current. It also requires heightened scrutiny of transactions undertaken in the course of the business relationship to ensure activity is consistent with what is known about a customer.
- 4.32. Ongoing monitoring includes keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date. For business relationships initiated prior to the 2007 Regulations coming into force, this may require the firm to obtain further documents, data and information to update customer due diligence to 2007 Regulation standards.
- 4.33. A small number of files opened prior to the Relevant Period held no supporting documentation in respect of the customer's source of wealth and/or source of funds. While these files were opened prior to the 2007 Regulations coming into force, these files should have been updated as appropriate as part of ongoing monitoring requirements in the 2007 Regulations.
- 4.34. Without an adequate and effective ongoing monitoring programme in place, a firm cannot properly re-assess the risk profiles of its customers as they develop over time. As a result, a firm may not be able to identify activity that could potentially involve money laundering.
- 4.35. Of the 99 PEP and other high risk customer files reviewed by the FSA 83 raised serious concerns with EFG's ongoing monitoring of the relationship.

#### ***Annual customer reviews***

- 4.36. In accordance with the Firm's policies, EFG was required to review PEP and higher risk customer relationships annually to ensure customer information was up to date and that the customer risk status was maintained appropriately.
- 4.37. EFG failed to carry out its 2008 PEP review and conducted no reviews of other higher

risk customers during the Relevant Period.

- 4.38. The FSA also found that PEP reviews carried out at the start of the Relevant Period were deficient. These reviews failed to review customers' risk profiles, highlight new adverse information, review information on customer files to ensure it was consistent with the particular customer's activity or update customer due diligence as appropriate to the standard required by the 2007 Regulations. These deficiencies continued until the PEP review process was updated in October 2009.
- 4.39. These failings meant that changes to a customer's risk profile, including those that had the potential to significantly increase the money laundering risks posed by the customer, would not necessarily have been highlighted and given full consideration until October 2009. They would also undermine the ability of EFG to conduct transaction monitoring effectively before this time.

#### ***Review of customer account activity***

- 4.40. EFG had a number of automated systems in place during the Relevant Period to monitor transactions for unusual or suspicious account activity, which continued throughout the Relevant Period. These were supplemented by manual procedures which included the rolling review of PEP and higher risk customers' transaction history against their account profile, the results of which were recorded on the customer file. However on customer files reviewed by the FSA, it was found that these rolling reviews of customers' transaction history ceased in September 2006 and did not recommence until March 2009.
- 4.41. By not consistently reviewing these transactions against the customers' profiles, the Firm's ability to assess sufficiently whether transactions were unusual or suspicious was weakened.

### **5. FAILINGS**

- 5.1. The FSA considers that EFG breached Principle 3 by failing to take reasonable care to establish and maintain effective AML systems and controls in relation to PEP and high risk customers. As a result, EFG did not:
- (1) document that potential money laundering risks posed by prospective higher risk customers had been fully considered and appropriate action taken to mitigate those risks through the Firm's records;
  - (2) demonstrate that it had followed the Firm's policies and procedures consistently to manage money laundering risks associated with higher risk customers;
  - (3) adequately establish, or record how it had established, the source of wealth and funds of higher risk customers; and
  - (4) conduct ongoing reviews of higher risk customer files periodically to ensure the information and risk assessment was up-to-date and that the activity on

accounts was consistent with expected activity.

- 5.2. These weaknesses in EFG's AML systems and controls resulted in an unacceptable risk of the Firm handling the proceeds of crime through its PEP and higher risk customer relationships.
- 5.3. As well as a breach of the FSA Principle 3, these failings amounted to breaches of SYSC 6.1.1R and SYSC 6.3.1R and previously applicable versions of these rules.

## **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 and 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 proposed 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 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**

- 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 out in paragraph 2.6 of this Notice, the FSA considers that EFG's breaches are of a serious nature.

### **The extent to which the breach was deliberate or reckless**

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

### **The size, financial resources and other circumstances of the Firm**

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

### **Disciplinary record and compliance history**

- 6.7. The FSA has taken into account the fact that EFG has not been the subject of previous disciplinary action.

### **Conduct following the breach**

- 6.8. Since the commencement of the FSA's investigation, EFG has worked in an open and cooperative manner with the FSA.

### **Previous action taken by the FSA in relation to similar findings**

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

## **7. PROCEDURAL MATTERS**

### **Decision makers**

- 7.1. The decision which gave rise to the obligation to give this Notice was made by the Settlement Decision Makers.
- 7.2. This Final Notice is given 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 EFG to the FSA by no later than 11 April 2013, 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 12 April 2013, the FSA may recover the outstanding amount as a debt owed by EFG 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 you 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, contact Guy Wilkes (direct line: 020 7066 7574) of Enforcement and Financial Crime Division of the FSA.

.....

Tom Spender

**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 6.1.1 R

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 6.3.1 R

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 6.3.2 G

"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 6.3.4 R

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 6.3.5 G

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 6.3.6 G

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.

**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 cooperation 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 cooperated 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 longstanding 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**

### ***Meaning of customer due diligence measures (Regulation 5)***

“Customer due diligence measures” means—

- (a) identifying the customer and verifying the customer’s identity on the basis of documents, data or information obtained from a reliable and independent source;
- (b) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant person is satisfied that he knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and
- (c) obtaining information on the purpose and intended nature of the business relationship.

### ***Application of customer due diligence measures (Regulation 7)***

(1) Subject to regulations 9, 10, 12, 13, 14, 16(4) and 17, a relevant person must apply customer due diligence measures when he—

- (a) establishes a business relationship;
- (b) carries out an occasional transaction;
- (c) suspects money laundering or terrorist financing;
- (d) doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

(2) Subject to regulation 16(4), a relevant person must also apply customer due diligence measures at other appropriate times to existing customers on a risk-sensitive basis.

(3) A relevant person must—

- (a) determine the extent of customer due diligence measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction; and
- (b) be able to demonstrate to his supervisory authority that the extent of the measures is appropriate in view of the risks of money laundering and terrorist

financing.

***Ongoing monitoring (Regulation 8)***

- (1) A relevant person must conduct ongoing monitoring of a business relationship.
- (2) “Ongoing monitoring” of a business relationship means—
  - (a) 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 relevant person’s knowledge of the customer, his business and risk profile; and
  - (b) keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date.
- (3) Regulation 7(3) applies to the duty to conduct ongoing monitoring under paragraph (1) as it applies to customer due diligence measures.

***Enhanced customer due diligence and ongoing monitoring (Regulation 14)***

- (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.

“

**OTHER RELEVANT PROVISIONS**

**Relevant extracts from the JMLSG Guidance**

**Part I, Chapter 5 – Customer due diligence**

***5.5 Enhanced due diligence***

11. 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.

12. Paragraph 5.5.2 – As a part of a risk-based approach, therefore, firms should hold sufficient information about the circumstances and business of their customers and, where applicable, their customers’ beneficial owners, for two principal reasons:
  - to inform its risk assessment process, and thus manage its money laundering/terrorist financing risks effectively; and
  - to provide a basis for monitoring customer activity and transactions, thus increasing the likelihood that they will detect the use of their products and services for money laundering and terrorist financing.
13. 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.
14. 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*

15. 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.
16. 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.
17. 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.

*On-going monitoring*

18. 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**

19. 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.
20. Paragraph 5.7.2 - Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps firms know their customers, assist them to assess risk and provides greater assurance that the firm is not being used for the purposes of financial crime.
21. 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.
22. Paragraph 5.7.12 - Higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring.