Financial Services Authority

FINAL NOTICE

To:	**Alpari (UK) Limited**
Of:	**201 Bishopsgate** **London** **EC2M 3AB**
Firm Reference Number:	**448002**
Date:	**5 May 2010**

TAKE NOTICE: The Financial Services Authority of 25 The North Colonnade, Canary Wharf, London E14 5HS ("the FSA") gives Alpari (UK) Limited final notice about a requirement to pay a financial penalty.

1. THE PENALTY

1.1. The FSA gave Alpari (UK) Limited ("Alpari") a Decision Notice on 5 May 2010 which notified Alpari that pursuant to section 206 of the Financial Services and Markets Act 2000 ("the Act"), the FSA has decided to impose a financial penalty of £140,000 on Alpari. This penalty is in respect of breaches of Principle 3 of the Principles for Businesses ("the Principles"), between 8 September 2006 and 25 November 2008 ("the relevant period") in relation to its regulated activities.

1.2. Alpari 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 £200,000 on Alpari.

1.3. Alpari confirmed on 22 April 2010 that it would not refer the matter to the Upper Tribunal (Tax and Chancery Chamber).

1.4. Accordingly, for the reasons set out below, the FSA imposes a financial penalty on Alpari in the amount of £140,000.

2. REASONS FOR THE ACTION

2.1. On the basis of the facts and matters described below, the FSA has imposed a financial penalty on Alpari for breaching Principle 3. These breaches relate to failings in the adequacy of Alpari's anti money laundering systems and controls.

Summary of breaches

2.2. In summary, Alpari failed to:

(1) carry out adequate risk assessments of the money laundering and financial crime risks that Alpari was exposed to;

(2) resource its compliance and anti-money laundering area adequately, in line with the growth of Alpari;

(3) screen customers against U.K. and global sanctions lists and determine whether they were politically exposed persons (PEP);

(4) have in place adequate customer due diligence procedures, in relation to customers from higher risk jurisdictions, at the account opening stage;

(5) carry out adequate on-going monitoring of the business relationship with the customer; and

(6) adequately train employees, on an on-going basis, in relation to financial crime and money laundering.

2.3. These failings were particularly serious because of the following factors:

(1) Alpari's customer base included customers from higher risk jurisdictions such as Nigeria;

(2) Alpari's relationship with its customers was not face to face making it more important that adequate due diligence on them was carried out; and

(3) the FSA has repeatedly stressed the importance of effective anti-money laundering controls through its Financial Crime Newsletters, speeches and other communications. The FSA has on previous occasions taken disciplinary action against regulated firms for failing to meet the FSA's anti-money laundering requirements.

2.4. The FSA has also taken into account the following steps taken by Alpari which have served to mitigate its failings:

(1) Alpari had identified the weaknesses in its anti money laundering systems and controls before the identification of these failings by the FSA;

(2) Alpari had also begun to address these weaknesses by recruiting a senior member of staff to hold the CF10 and CF11 functions, and increasing the number of people employed within the compliance department;

(3) Alpari has since commenced a remedial programme which is on-going and is being monitored by external consultants; and

(4) Alpari has co-operated fully with the FSA's investigation.

2.5. The FSA has concluded that the nature and seriousness of the breaches outlined above warrant the imposition of a financial penalty. The FSA therefore has imposed a financial penalty of £140,000 on Alpari.

2.6. This action supports the FSA's statutory objectives of maintaining market confidence and reducing financial crime.

3. RELEVANT STATUTORY AND REGULATORY PROVISIONS AND GUIDANCE

3.1. The relevant statutory provisions, regulatory requirements and Joint Money Laundering Steering Group ("the JMLSG") guidance sections are set out at Annex A to this Final Notice.

3.2. The FSA has had regard to the guidance issued by the JMLSG. The JMLSG is a body made up of the leading U.K. trade associations in the financial services industry, whose aim is to promulgate good practice in countering money laundering and to give practical assistance in interpreting the U.K. money laundering regulations. Since 1990 it has provided advice on anti-money laundering controls by issuing guidance for the financial sector ("JMLSG guidance"). Subsequent editions of the JMLSG guidance have taken into account relevant legal changes and evolving practice within the financial services industry.

4. FACTS AND MATTERS RELIED ON

4.1. Alpari provides, on an execution only basis, rolling spot foreign exchange contracts for speculative investment purposes. It was authorised on 8 September 2006 and serves retail and institutional customers through an internet based platform. Alpari is permitted by the FSA to carry on the following regulated activities:

(1) advising on investments (except on pension transfers and pension opt outs);

(2) agreeing to carry on a regulated activity;

(3) arranging (bringing about) deals in investments;

(4) arranging safeguarding and administration of assets;

(5) dealing in investments as principal;

(6) making arrangements with a view to transactions in investments; and

(7) safeguarding and administration of assets (without arranging).

4.2. In July 2007, it had approximately 400 live customer accounts, of which approximately 136 were funded. At the end of June 2008, Alpari had approximately 9,500 accounts. By 25 July 2008, the date of Alpari's annual MLRO report, it had 11,500 accounts. Of these 4,000 were funded and Alpari was receiving approximately 50 deposits a day. Alpari has an international customer base, which includes customers from higher risk jurisdictions (from a money laundering perspective)

including Nigeria. Alpari operated a non face to face account opening identification process.

4.3. The FSA's investigation found evidence of the following failures:

Failure to carry out adequate risk assessments of the money laundering and financial crime risks that Alpari was exposed to.

4.4. Alpari set out its anti money laundering policy in its compliance manual. Alpari identified that it faced an increased risk of money laundering because of the geographical location of some of its customers and therefore it had a system to categorise its customers as either medium or high risk.

4.5. However, Alpari did not carry out at any time a formal risk assessment or gap analysis of Alpari's position in relation to the Money Laundering Regulations 2007, Proceeds of Crime Act 2002, Terrorism Act 2000 or the JMLSG Guidance to establish the way it might be used to facilitate financial crime and how it could mitigate these risks. There also appeared to be no specific on-going consideration given to changing issues it may face with various higher risk jurisdictions and how to keep the procedures relating to these countries up-to-date.

4.6. In conclusion, although Alpari had conducted an initial identification of the risks that it was exposed to, it failed to assess its position fully in relation to the relevant regulatory requirements and guidance and failed to monitor this position on an ongoing basis. This meant that it was exposed to the risk that it might not maintain anti money laundering systems which were appropriate to its business as it grew.

Inadequate compliance and anti-money laundering resource

4.7. Despite the significant growth in business between mid 2007 and mid 2008 and Alpari's awareness towards the end of 2007 that its approach to compliance and anti money laundering functions needed to be more focused on the risks to its actual business, Alpari only recruited an additional junior member of compliance staff in July 2008. During this period the holder of the CF10 and CF11 functions was heavily involved in growing the business as well as undertaking the compliance and anti money laundering functions. Alpari placed too much responsibility on the holder of the CF10 and CF11 functions and failed to provide him with adequate support in the roles. It was not until November 2008 that Alpari appointed an additional person to take over the CF10 and CF11 functions and to run a larger compliance department.

4.8. Alpari should have identified and managed the risk that its growth was a risk to its ability to operate and maintain adequate money laundering and financial crime systems and controls.

Inadequate system for screening of customers against U.K. and global sanctions lists and for determining whether a customer is a politically exposed person ("PEP")

4.9. HM Treasury maintains a Consolidated List of targets listed by the United Nations, European Union and U.K. This list includes all individuals and entities that are subject to financial sanctions in the U.K. It is a criminal offence to make payments,

or to allow payments to be made, to targets on this list. This is set out in detail in Chapter 5 of the JMLSG guidance.

4.10. A PEP is an individual who has, or has had, a high political profile, or holds or has held, public office. They can pose a higher money laundering risk to a firm. The JMLSG guidance sets out its guidance on PEPs in Chapter 5.5.18 – 5.5.29.

4.11. Alpari did not make any assessments as to the risk based procedures it might apply and it failed to have an adequate system in place for screening against UK and global sanctions lists or for checking whether customers were PEPs either at the account opening stage or periodically after that.

4.12. Alpari mistakenly believed that its electronic system checked against sanctions lists and checked for PEPs when it did not. This meant that no checks against the sanctions lists or for PEPs were carried out during the relevant period and Alpari was exposed to the risk that it might accept customers in these categories without being aware of this fact. There was also confusion at Alpari over the difference between sanctions and PEP checks.

Inadequate customer due diligence procedures, in relation to higher risk customers, at the account opening stage

4.13. Section 5.3.1 of the JMLSG guidance sets out that a firm should identify its customers and verify their identity. Also, according to the JMLSG guidance "a firm must apply enhanced due diligence measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing."

4.14. Alpari's policy in relation to customer identity verification was that it classified its customers into two categories: medium and high risk. The medium risk category included all the customers from the old 25 members of the European Union and a number of other countries which had robust regulatory systems, such as Australia, New Zealand, U.S., Canada and Japan. For customers from these countries, Alpari accepted emailed copies of passports and a utility bill, bank statement or similarly reliable document as proof of identification.

4.15. In addition, from 2007 Alpari used an electronic identity verification system, to screen documents provided by customers who were UK citizens.

4.16. Customers from all other jurisdictions were categorised as high risk. Any customers from these countries had to provide copies of the same documents but these had to be notarised or certified by a lawyer, banker or person in a similar position of authority.

4.17. During the review of the twelve customer files, the FSA found that the identity verification for the six customers with a medium risk categorisation was completed in accordance with Alpari's policy. However, of the six files that came from the higher risk jurisdictions only two contained certified copies of documents, in accordance with Alpari's policy. Both of these two were customers from Nigeria and Alpari had no way of verifying the authenticity of the issuer of the certification.

4.18. Three files contained uncertified documents from Nigeria and one file contained un-translated documents from China. There was no further due diligence carried out on higher risk customers when compared to medium risk customers.

4.19. Therefore, although Alpari had a system which it followed for carrying out identification and verification of its classification of medium risk customers, it did not always follow its own risk based system for identification and verification of its customers from higher risk jurisdictions.

Inadequate on-going monitoring of the business relationship with the customer

4.20. The JMLSG sets out its guidance on monitoring customer activity in Chapter 5.7 of its guidance. It sets out that a firm must conduct ongoing monitoring of the business relationship with their customers and sets out examples.

4.21. Alpari gathered only high level information at the account opening stage and did not have an adequate system in place to assess whether transactions were consistent with their knowledge of the customer and his/her financial circumstances.

4.22. Gathering more detailed information about customers, such as source of funds, would have been particularly relevant as although the compliance department at Alpari carried out spot checks on customer files as part of the compliance monitoring plan, it was the responsibility of customer facing staff to alert the compliance department of any suspicious activities.

4.23. No checks were carried out to compare a customer's income to how much he was spending on his account. This was because the customer account opening teams, who would have access to this information, were separate to the payments team, who processed all the transactions.

4.24. The JMLSG guidance sets out appropriate on-going monitoring of customer activity as an alternative to additional due diligence at the point of account opening. In this respect, although Alpari had a system for monitoring activity, it was not adequate.

Inadequate training

4.25. The JMLSG guidance sets out in Chapter 7.1 "that one of the most important controls over the prevention and detection of money laundering is to have staff who are alert to the risk of money laundering/terrorist financing and well trained in the identification of unusual activities which may prove to be suspicious."

4.26. Alpari gave informal one to one training when employees joined and updated staff on an ad-hoc basis. This was inadequate as demonstrated by the failings identified in the files reviewed by the FSA. Alpari placed reliance on employees noticing and notifying the compliance department of any suspicious payments from customers, particularly customers from higher risk jurisdictions. Given the growth of its business, including from higher risk jurisdictions, Alpari should have given more consideration to the changing risks it faced from higher risk jurisdictions and the importance of its anti money laundering checks and provided refresher training to staff accordingly.

4.27. In relation to the role of the MLRO, Alpari failed to demonstrate that any additional training was provided to the MLRO so that he remained competent and up-to-date.

5. ANALYSIS OF BREACHES

5.1. By reason of the facts and matters referred to in paragraphs 4.1 to 4.27, the FSA considers that Alpari failed to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems in breach of Principle 3. This placed it at risk of being used to further financial crime and that when taken together the combination of failings significantly increased the risk of Alpari being used for a purpose connected to financial crime.

6. ANALYSIS OF SANCTION

6.1. The FSA has had regard to the relevant provisions in its Decision Procedure and Penalties Manual ("DEPP"). In particular, the FSA has had regard to its policy on imposing financial penalties on authorised persons, contained in DEPP 6.

6.2. Pursuant to DEPP 6.2.3G, the FSA has also had regard to whether Alpari has followed the relevant provisions of the JMLSG Guidance when considering whether to take action against it for a financial penalty or censure in respect of a breach of Principle 3.

6.3. In addition, the FSA has had regard to the corresponding provisions of Chapter 13 of the Enforcement Manual ("ENF") in force during the relevant period until 27 August 2007 and Chapter 7 of the Enforcement Guide ("EG"), in force thereafter.

6.4. The principal purpose of a financial penalty is to promote high standards of regulatory conduct by deterring firms who have committed breaches from committing further breaches, and helping to deter other firms from committing similar breaches, as well as demonstrating generally the benefits of compliant behaviour.

6.5. In determining whether a financial penalty is appropriate the FSA is required to consider all the relevant circumstances of a case. Applying the criteria set out in the DEPP 6.2.1 (regarding whether or not to take action for a financial penalty or public censure) and 6.4.2 (regarding whether to impose a financial penalty or a public censure), the FSA considers that a financial penalty is an appropriate sanction, given the serious nature of the breaches and the need to send out a strong message.

6.6. DEPP 6.5.2 sets out a non-exhaustive list of factors that may be of relevance in determining the level of a financial penalty. The FSA considers that the following factors are particularly relevant in this case.

Deterrence (DEPP 6.5.2(1))

6.7. A financial penalty will deter Alpari from further breaches of regulatory rules and Principles. In addition, other firms will be deterred from allowing similar failings to occur and it will therefore promote the message to the industry that the FSA expects firms to maintain high standards of regulatory conduct. The financial penalty will reinforce the message that the FSA expects firms to establish and maintain effective systems and controls for countering the risk that they may be used to further financial

crime and that senior management actively engage in ensuring that firms are compliant.

The nature, seriousness and impact of the breach in question (DEPP 6.5.2(2))

6.8. In determining the appropriate sanction, the FSA has had regard to the seriousness of the breaches, including the nature of the requirements breached, the duration and frequency of the breaches, whether the breaches revealed serious failings in Alpari's systems and controls.

6.9. Alpari's failings in the relevant period are viewed as being serious as they exposed Alpari to the risk of being used to facilitate financial crime. The breaches took place over a period of approximately two years and although Alpari had identified some of its weaknesses early on in this period, it should have reacted more promptly to develop its compliance and AML function alongside the rest of the business.

6.10. The FSA has also taken into account the following steps taken by Alpari which have served to mitigate its failings:

(1) Alpari had identified weaknesses in its compliance and AML function before identification of these by the FSA;

(2) Alpari had recruited a senior member of staff to hold the CF10 and CF11 functions and had begun to increase the number of people employed within the compliance department;

(3) Alpari has since commenced a remedial programme which is on-going and is being monitored by external consultants, as set out in paragraph 2.4 above;

(4) Alpari has co-operated fully with the FSA's investigation.

The extent to which the breach was deliberate or reckless (DEPP 6.5.2(3))

6.11. The FSA has found no evidence to show that Alpari acted in a deliberate or reckless manner.

The size, financial resources and other circumstances of Alpari (DEPP 6.5.2(5))

6.12. In determining the level of penalty, the FSA has considered Alpari's latest financial statements and considers that the level of financial penalty is appropriate.

Disciplinary record and compliance history (DEPP 6.5.2(9))

6.13. Alpari has not been the subject of previous disciplinary action.

Other action taken by the FSA (DEPP 6.5.2(10))

6.14. In determining the level of financial penalty, the FSA has taken into account penalties imposed by the FSA on other authorised persons for similar behaviour.

7. CONCLUSION

7.1. Having regard to the seriousness of the breaches and the risk posed to the customers the FSA considers a financial penalty of £200,000 (before discount for early settlement) to be appropriate.

8. DECISION MAKERS

8.1. The decision which gave rise to the obligation to give this Final Notice was made by the Settlement Decision Makers on behalf of the FSA.

9. IMPORTANT

9.1. This Final Notice is given to Alpari in accordance with section 390 of the Act.

Manner of and time for Payment

9.2. The financial penalty must be paid in full by Alpari to the FSA by no later than 19 May 2010, 14 days from the date of the Final Notice.

If the financial penalty is not paid

9.3. If all or any of the financial penalty is outstanding on 20 May 2010, the FSA may recover the outstanding amount as a debt owed by Alpari and due to the FSA.

Publicity

9.4. 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.

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

FSA contacts

9.6. For more information concerning this matter generally, Alpari should contact Anna Hynes at the FSA (direct line: 0207 066 9464) of the Enforcement and Financial Crime Division of the FSA.

……

Tom Spender
Head of Department
FSA Enforcement and Financial Crime Division

ANNEX A

RELEVANT STATUTORY PROVISIONS, REGULATORY REQUIREMENTS AND GUIDANCE

1. Statutory provisions

1.1. The FSA's regulatory objectives are set out in section 2(2) of the Act and include market confidence, public awareness, the protection of consumers and the reduction of financial crime.

1.2. Section 138 of the Act provides that the FSA may make such rules applying to authorised persons as appear to it to be necessary or expedient for the purpose of protecting consumers.

1.3. The FSA has the power, pursuant to section 206 of the Act, to impose a financial penalty of such amount as it considers appropriate where the FSA considers an authorised person has contravened a requirement imposed on him by or under the Act.

2. Relevant Handbook provisions

2.1. In exercising its power to impose a financial penalty, the FSA must have regard to relevant provisions in the FSA Handbook of rules and guidance ("the FSA Handbook"). The main provisions relevant to the action specified above are set out below.

Principles for Businesses (PRIN)

2.2. Under the FSA's rule-making powers as referred to above, the FSA has published in the FSA Handbook the Principles for Business ("Principles") which apply either in whole, or in part, to all authorised persons.

2.3. The Principles are a general statement of the fundamental obligations of firms under the regulatory system and reflect the FSA's regulatory objectives. A firm may be liable to disciplinary sanction where it is in breach of the Principles.

2.4. The Principle relevant to this matter is Principle 3 (management and control) which states that "a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems."

Decision Procedure and Penalties Manual ("DEPP")

2.5. Guidance on the imposition and amount of penalties is set out in Chapter 6 of DEPP.

2.6. DEPP 6.1.2G provides that the principal purpose of imposing a financial penalty is to promote high standards of regulatory and/or market conduct by deterring persons who have committed breaches from committing further breaches, helping to deter other persons from committing similar breaches, and demonstrating generally the benefits

of compliant behaviour. Financial penalties are therefore tools that the FSA may employ to help it to achieve its regulatory objectives.

2.7. DEPP 6.5.1G (1) provides that the FSA will consider all the relevant circumstances of a case when it determines the level of financial penalty (if any) that is appropriate and in proportion to the breach concerned.

2.8. DEPP 6.5.2 sets out a non-exhaustive list of factors that may be relevant to determining the appropriate level of financial penalty to be imposed on a person under the Act. The following factors are relevant to this case:

Deterrence: DEPP 6.5.2G (1)

2.9. When determining the appropriate level of financial 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.

The nature, seriousness and impact of the breach in question: DEPP 6.5.2G (2)

2.10. The FSA will consider the seriousness of the breach in relation to the nature of the rule, requirement or provision breached, which can include considerations such as the duration and frequency of the breach, 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, the nature and extent of any financial crime facilitated, occasioned or otherwise attributable to the breach and the loss or risk of loss caused to consumers, investors or other market users.

The extent to which the breach was deliberate or reckless: DEPP 6.5.2G (3)

2.11. The FSA will regard as more serious a breach which is deliberately or recklessly committed, giving consideration to factors such as whether the person has given no apparent consideration to the consequences of the behaviour that constitutes the breach. 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.

Whether the person on whom the penalty is to be imposed is an individual: DEPP 6.5.2G (4)

2.12. When determining the amount of 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.

Conduct following the breach: DEPP 6.5.2G (8)

2.13. The FSA may take into account the degree of co-operation the person showed during the investigation of the breach by the FSA.

Other action taken by the FSA (or a previous regulator): DEPP 6.5.2G (10)

2.14. The FSA seeks to apply a consistent approach to determining the appropriate level of penalty. The FSA may take into account previous decisions made in relation to similar misconduct.

FSA guidance and other published materials: DEPP 6.5.2G (12)

2.15. 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.

3. Relevant extracts from Part I and Part II of the Joint Money Laundering Steering Group Guidance

Chapter 5 – Customer due diligence

5.1 Meaning of customer due diligence measures and ongoing monitoring

3.1. Paragraph 5.1.4 - Firms must determine the extent of their CDD measures and ongoing monitoring on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction. They must be able to demonstrate to their supervisory authority that the extent of their CDD measures and monitoring is appropriate in view of the risks of money laundering and terrorist financing.

5.3 Application of CDD measures

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

3.3. Paragraph 5.3.41 - The United Nations, European Union, and United Kingdom are each able to designate persons and entities as being subject to financial sanctions, in accordance with legislation explained below. Such sanctions normally include a comprehensive freeze of funds and economic resources, together with a prohibition on making funds or economic resources available to the designated target. A Consolidated List of all targets to whom financial sanctions apply is maintained by HM Treasury, and includes all individuals and entities that are subject to financial sanctions in the UK. This list is at: www.hm-treasury.gov.uk/financialsanctions.

3.4. Paragraph 5.3.42 - The obligations under the UK financial sanctions regime apply to all firms, and not just to banks. The Consolidated List includes all the names of designated persons under UN and EC sanctions regimes which have effect in the UK. Firms will not normally have any obligation under UK law to have regard to lists issued by other organisations or authorities in other countries, although a firm doing business in other countries will need to be aware of the scope and focus of relevant financial sanctions regimes in those countries. The other websites referred to below

may contain useful background information, but the purpose of the HM Treasury list is to draw together in one place all the names of designated persons for the various sanctions regimes effective in the UK. All firms to whom this guidance applies, therefore, whether or not they are FSA-regulated or subject to the ML Regulations, will need either:

- for manual checking: to register with the HM Treasury update service (directly or via a third party, such as a trade association); or
- if checking is automated: to ensure that relevant software includes checks against the relevant list and that this list is up to date.

Mitigation of impersonation

3.5. Paragraph 5.3.82 - Where identity is verified electronically, or copy documents are used, a firm should apply an additional verification check to manage the risk of impersonation fraud. The additional check may consist of robust anti-fraud checks that the firm routinely undertakes as part of its existing procedures, or may include:

- requiring the first payment to be carried out through an account in the customer's name with a UK or EU regulated credit institution or one from an equivalent jurisdiction;
- verifying additional aspects of the customer's identity, or of his electronic 'footprint' (see paragraph 5.3.25);
- telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise), or a "welcome call" to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;
- communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, might be required to be returned completed or acknowledged without alteration);
- internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address;
- other card or account activation procedures;
- requiring copy documents to be certified by an appropriate person.

5.5 Enhanced due diligence

3.6. 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 (see section 5.3) is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer.

3.7. Paragraph 5.5.2 - As a part of a risk-based approach, therefore, firms may need to hold sufficient information about the circumstances and business of their customers for two principal reasons:

- to inform its risk assessment process and therefore manage its money laundering/terrorist finance risk 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 or terrorist financing.

3.8. Paragraph 5.5.4 - In practice, under a risk-based approach, it will not be appropriate for every product or service provider to know their customers equally well, regardless of the purpose, use, value, etc., of the product or service provided. Firms' information demands need to be proportionate, appropriate and discriminating, and to be able to be justified to customers.

3.9. Paragraph 5.5.9 - The ML Regulations prescribe three specific types of relationship in respect of which EDD measures must be applied. These are:

- where the customer has not been physically present for identification purposes (see paragraphs 5.5.10ff);
- in respect of a correspondent banking relationship (see Part II, sector 16: Correspondent banking);
- in respect of a business relationship or occasional transaction with a PEP (see paragraphs 5.5.18ff).

3.10. Paragraph 5.5.17 - Non face-to-face identification and verification carries an inherent risk of impersonation fraud, and firms should follow the guidance in paragraph 5.3.82 to mitigate this risk.

Politically exposed persons (PEPs)

3.11. 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.

3.12. 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.

3.13. Paragraph 5.5.20 - Although under the definition of a PEP an individual ceases to be so regarded after he has left office for one year, firms are encouraged to apply a risk-based approach in determining whether they should cease carrying out appropriately enhanced monitoring of his transactions or activity at the end of this period. In many cases, a longer period might be appropriate, in order to ensure that the higher risks associated with the individual's previous position have adequately abated.

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

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

Risk-based procedures

3.15. Paragraph 5.5.26 - The nature and scope of a particular firm's business will generally determine whether the existence of PEPs in their customer base is an issue for the firm, and whether or not the firm needs to screen all customers for this purpose. In the context of this risk analysis, it would be appropriate if the firm's resources were focused in particular on products and transactions that are characterised by a high risk of money laundering.

On-going monitoring

3.16. 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

3.17. 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.

3.18. 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.

Chapter 7 – Staff awareness, training and alertness

3.19. Paragraph 7.1 - One of the most important controls over the prevention and detection of money laundering is to have staff who are alert to the risks of money laundering/terrorist financing and well trained in the identification of unusual activities or transactions which may prove to be suspicious.

3.20. Paragraph 7.2 - The effective application of even the best designed control systems can be quickly compromised if the staff applying the systems are not adequately trained. The effectiveness of the training will therefore be important to the success of the firm's AML/CTF strategy.

3.21. Paragraph 7.3 - It is essential that firms implement a clear and well articulated policy for ensuring that relevant employees are aware of their obligations in respect of the prevention of money laundering and terrorist financing and for training them in the identification and reporting of anything that gives grounds for suspicion. This is especially important for staff who handle customer transactions or instructions. Temporary and contract staff carrying out such functions should also be covered by these training programmes.

Part II

Chapter 10 –Execution only stockbrokers

Verification of identity

3.22. Paragraph 10.8 - The risk level of execution only broking, however, depends on whether the services are offered and operated on a face-to-face basis. The ML Regulations identify non-face-to-face business as higher risk for money laundering that face-to-face business. In view of this, firms need to have in place additional measures to neutralise the higher risk when opening and operating accounts for non face-to-face business. This can take the form of additional due diligence at the point of account opening, appropriate monitoring of customer activity or both.

Additional customer information

3.23. Paragraph 10.10 - ExO business is driven by the customer and, as mentioned earlier, customer behaviour may vary widely, from the occasional transaction in a FTSE 100 share to day trading in a variety of instruments. As there are no suitability obligations for ExO stockbrokers, firms will have little or no information about the customer. Given the reasonably narrow range of services provided by ExO stockbrokers, no additional information is likely to be required to establish the purpose and intended nature of the business relationship.