Financial Conduct Authority
25 The North Colonnade
Canary Wharf
London
E14 5HS

Tel: +44 (0)20 7066 1000
Fax: +44 (0)20 7066 1099
www.fca.org.uk

FINAL NOTICE

To:	**Deutsche Bank AG**
Firm Reference Number:	**150018**
Address:	**Winchester House** **1 Great Winchester Street** **London** **EC2N 2DB**
Date:	**30 January 2017**

1. ACTION

1.1. For the reasons given in this Notice, the Authority hereby imposes on Deutsche Bank AG (Deutsche Bank) a financial penalty of £163,076,224, comprising disgorgement of £9,076,224 and a penal element of £154,000,000, for breaches of Principle 3 (management and control) and Senior Management Arrangements, Systems and Controls (SYSC) rules 6.1.1 R and 6.3.1 R between 1 January 2012 and 31 December 2015 (Relevant Period).

1.2. Deutsche Bank agreed to settle at an early stage of the Authority's investigation and therefore qualified for a 30% (stage 1) discount under the Authority's executive settlement procedures. Were it not for this discount, the Authority would have imposed a financial penalty of £229,076,224 (comprising disgorgement of £9,076,224 and a penal element of £220,000,000).

2. SUMMARY OF REASONS

2.1. The laundering of money through UK financial institutions undermines the integrity of the UK financial system (the protection and enhancement of which is one of the Authority's operational objectives). UK financial institutions are responsible for minimising their risk of being used for criminal purposes, particularly the facilitation of money laundering or terrorist financing.

2.2. The Authority has investigated whether Deutsche Bank has taken reasonable care to organise and control its affairs responsibly and effectively and to establish and maintain an effective anti-money laundering (AML) control framework in its Corporate Banking & Securities (CB&S) division in the UK in the Relevant Period. The Authority has found the AML control framework was substantially inadequate, and the risks raised are highlighted by certain trading (further described below) arranged by Deutsche Bank's Russia-based subsidiary (DB Moscow) and booked to Deutsche Bank's trading books in London. The way these trades were conducted in combination with their scale and volume are highly suggestive of financial crime. The Authority's findings are made in the context of this finding and in consideration that these matters may give rise to additional investigation by other regulators and/or law enforcement agencies. For this reason, the Authority has requested and Deutsche Bank has undertaken to the Authority as part of this resolution to cooperate with any other regulator or law enforcement agency that is investigating or commences investigating any of the facts and matters stated in this Notice or anything arising from or related to those facts and matters.

2.3. Deutsche Bank notified the Authority in early 2015 of concerns regarding its AML control framework after it commenced an investigation into a form of suspicious securities trading, referred to in this Notice as "mirror trading", involving DB Moscow.

2.4. The mirror trades were used by customers of Deutsche Bank and DB Moscow that were connected to each other to transfer more than USD6 billion from Russia, through Deutsche Bank in the UK, to overseas bank accounts, including in Cyprus, Estonia, and Latvia. The orders for both sides of the mirror trades were received by DB Moscow's front office CB&S business (Moscow Front Office), which executed both sides at the same time.

2.5. There were more than 2,400 mirror trades between April 2012 and October 2014 that involved the following arrangement:

(1) a Russian customer of DB Moscow bought highly liquid Russian securities from DB Moscow, paying in Roubles (the Moscow Side); and

(2) at the same time, a non-Russian customer of Deutsche Bank (the onboarding of which had been initiated and facilitated by Moscow Front Office) sold the same number of the same securities to Deutsche Bank in exchange for US Dollars (the London Side).

2.6. The London Side of the mirror trades was executed by Moscow Front Office on behalf of Deutsche Bank via remote booking; a process by which Deutsche Bank offices in certain locations around the world, including DB Moscow, could directly book trades to Deutsche Bank's trading books in the UK.

2.7. Moscow Front Office was able to execute the mirror trades undetected for such a considerable period because of widespread deficiencies in Deutsche Bank's AML control framework, particularly in relation to the establishment of new customer relationships and ongoing monitoring of transactions. In addition, over the two and a half years that the mirror trades continued, Deutsche Bank missed a number of warning signs in relation to the trading.

2.8. The mirror trading customers were able to place their orders with Moscow Front Office on behalf of others whose identities and source of wealth were not known to Deutsche Bank. The effect of the mirror trades was to convert Roubles into US Dollars and to transfer more than USD6 billion out of Russia via Deutsche Bank in the UK to overseas bank accounts including in Cyprus, Estonia, and Latvia.

2.9. The customers on the Moscow and London Sides of the mirror trades were connected to each other and the amount and value of the securities was the same on both sides. Therefore, the evident purpose for the mirror trades was the conversion of Roubles into US Dollars and the covert transfer of those funds out of Russia, which is highly suggestive of financial crime.

2.10. Following the commencement of its investigation into the mirror trades, Deutsche Bank identified a further USD3.8 billion in suspicious securities trades executed during the Relevant Period by Moscow Front Office through the UK between January 2012 and February 2015. In this Notice, these trades are referred to as "one-sided trades" because the Authority takes the view that some, if not all of them, must have formed one side of an additional 3,400 mirror trades. Over 99 percent of these trades were sales, and were often conducted by the same customers that were involved in the mirror trading. On the basis that most if not all of the one-sided trades were part of mirror trades, approximately USD10

billion was transferred out of Russia, through Deutsche Bank, during the Relevant Period in a manner highly suggestive of financial crime.

2.11. As with the mirror trades, the one-sided trades were not detected because of deficiencies in Deutsche Bank's AML control framework, particularly in relation to the establishment of new customer relationships and ongoing monitoring of transactions.

2.12. The culture within the CB&S division failed to instil a sense of responsibility in the front office business for the identification and management of non-financial risks. As a result, Deutsche Bank's front office CB&S business (London Front Office) did not appreciate that it was ultimately responsible for Know Your Customer (KYC) obligations in respect of its customers. This lack of accountability was compounded by the firm's complex management structure, which failed to clearly define roles and responsibilities. Deutsche Bank's AML control framework therefore lacked appropriate oversight and supervision.

2.13. Deutsche Bank in the UK allowed certain overseas entities within the Deutsche Bank group of companies to initiate and facilitate the establishment of new customer relationships in the UK. However, Deutsche Bank did not oversee this process and it also failed to properly monitor trades that were remotely booked into the UK by overseas entities. These deficiencies were compounded by Deutsche Bank's reliance on inappropriate AML country risk ratings, which underestimated the money laundering risk in many of the jurisdictions in which Deutsche Bank operated.

2.14. Deutsche Bank's failure to properly consider its money laundering risk was exacerbated by the lack of sufficient resources for its AML function and the absence of an appropriate IT infrastructure to support the KYC process and AML transaction monitoring.

2.15. Deutsche Bank's deficient AML control framework meant that it conducted inadequate due diligence on customers, including those responsible for the suspicious trading. Consequently, Deutsche Bank failed to obtain sufficient information about its customers' businesses, which meant that their trading could not be effectively monitored, even if Deutsche Bank had had the facilities to do so.

2.16. The Authority therefore hereby imposes a financial penalty on Deutsche Bank in the amount of £163,076,224 pursuant to section 206 of the Act.

2.17. The Authority has found that the AML control framework failings identified in this Notice were not committed deliberately or recklessly. There is no evidence that senior management at Deutsche Bank or any Deutsche Bank employee in the UK was aware of the existence of or involved in the suspicious trading, including the mirror trades.

2.18. The Authority has also considered the nature and extent of co-operation provided by Deutsche Bank during the course of its investigation. Deutsche Bank has been extremely co-operative, it promptly notified the Authority following the discovery of the mirror trades, and it has taken significant steps to assist the Authority in its investigation. Deutsche Bank is continuing to undertake remedial action and has committed significant resources to improving its AML control framework. The Authority recognises the work already undertaken by Deutsche Bank in this regard.

3. DEFINITIONS

3.1. The definitions below are used in this Final Notice.

"2007 Regulations" means the Money Laundering Regulations 2007, which came into effect on 15 December 2007;

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

"AML" means Anti-Money Laundering;

"the Authority" means the body corporate previously known as the Financial Services Authority and renamed on 1 April 2013 as the Financial Conduct Authority;

"business relationship" (as defined under the 2007 Regulations) means a business, professional or commercial relationship between a relevant person and a customer, which is expected by the relevant person, at the time when contact is established, to have an element of duration;

"CB&S" means Deutsche Bank's Corporate Banking & Securities Division;

"CDD" means Customer Due Diligence Measures as defined in Regulation 5 of the 2007 Regulations (see the Annex to this Notice);

"CDD obligations" means those obligations in relation to CDD that a relevant person must apply - as set out in Regulation 7 of the 2007 Regulations (see Annex);

"COB" means customer onboarding and refers to the process by which a firm enters into a new business relationship with a customer;

"customer" means any party, including a counterparty, with whom a firm has a business relationship or with whom the firm conducts occasional transactions;

"DB Moscow" means Deutsche Bank Moscow Ltd, a Russia-based subsidiary of Deutsche Bank;

"DEPP" means the Authority's Decision Procedures and Penalties Manual;

"Deutsche Bank" means Deutsche Bank AG, which operates in London as a branch of an EEA authorised firm;

"EDD" means Enhanced Due Diligence and Ongoing Monitoring and the circumstances when EDD applies is set out in Regulation 14 of the 2007 Regulations (see Annex);

"Financial Crime Guide" means the Authority's consolidated guidance on financial crime, which is published under the name "*Financial crime: a guide for firms*";

"GEC" means Deutsche Bank's Group Executive Committee;

"JMLSG" means the Joint Money Laundering Steering Group, which is comprised of leading UK trade associations in the financial services sector;

"JMLSG Guidance" means the guidance issued by the JMLSG that has been approved by a Treasury Minister in compliance with the legal requirements in the 2007 Regulations, the regulatory requirements in the Authority's Handbook, and evolving practice within the financial services industry. The JMLSG Guidance sets out good practice for the UK financial services sector on the prevention of money laundering and combating terrorist financing;

"KYC" means Know Your Customer, which is a commonly used short-hand for the CDD and EDD obligations;

"London Front Office" means the front office of Deutsche Bank's CB&S business;

"mirror trading/trades" means the trading scheme that is described in paragraph 4.17 of this Notice;

"Moscow Front Office" means the front office of DB Moscow's CB&S business;

"occasional transaction" (as defined under the 2007 Regulations) means a transaction (carried out other than as part of a business relationship) amounting to EUR15,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked;

"one-sided trading/trades" means the trading scheme that is described in paragraph 4.42 of this Notice;

"orphan account" means an active customer account for which there is no apparent link to underlying KYC documentation either because the account was opened without the proper collection of KYC information or where Deutsche Bank has been unable to locate that information;

"PEP" means Politically Exposed Person as defined in regulation 14(5) of the 2007 Regulations;

"Relevant Period" means 1 January 2012 to 31 December 2015;

"remote booking" means the conducting of sales or trading activity, on behalf of Deutsche Bank in the UK by overseas entities within the Deutsche Bank group of companies, that is booked in the UK;

"RFA" means Request for Assistance;

"SAMLP" means the Authority's Systematic Anti-Money Laundering Programme;

"the Tribunal" means the Upper Tribunal (Tax and Chancery Chamber);

"Third Money Laundering Directive" means Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing; and

"UBO" means ultimate beneficial owner with "beneficial owner" being defined in Regulation 6 of the 2007 Regulations (see Annex).

4. FACTS AND MATTERS

Background

DEUTSCHE BANK IN THE UK AND RUSSIA

4.1. During the Relevant Period Deutsche Bank's AML control framework was overseen by the Management Board of Deutsche Bank. The Management Board was responsible for managing the global Deutsche Bank organisation, including Deutsche Bank in the UK. The Management Board was supported by a Group Executive Committee (GEC), which was comprised of, *inter alia*, senior managers from each of the different divisions as well as all of the members of the Management Board. The role of the GEC was to provide information to the Management Board and to coordinate Deutsche Bank's different product lines and regions.

4.2. DB Moscow was a Russian subsidiary of Deutsche Bank. Although DB Moscow had its own management and supervisory boards, Moscow Front Office and DB Moscow's Compliance functions, including in relation to AML, reported to and were overseen by Deutsche Bank in the UK during the Relevant Period.

LEGAL AND REGULATORY OBLIGATIONS

4.3. The Authority's operational objectives include protecting and enhancing the integrity of the UK financial system, which includes it not being used for a purpose connected with financial crime. To prevent the UK financial system from being exposed to financial crime risks, regulated firms are required to comply with certain obligations when entering into new business relationships and these obligations are set out in the Authority's Handbook. These obligations are supported by the 2007 Regulations, the JMLSG Guidance, and the Financial Crime Guide.

4.4. The Authority's SYSC rules provide that the Authority will have regard to whether a firm has followed the JMLSG Guidance when determining whether the firm has breached the Authority's rules.

4.5. Relevant extracts from the Authority's Handbook, the 2007 Regulations, the JMLSG Guidance, and the Financial Crime Guide are set out in the Annex to this Notice.

CUSTOMER ONBOARDING

4.6. Authorised firms subject to the 2007 Regulations, such as Deutsche Bank, should use their onboarding process to obtain and review information about a potential customer to satisfy their KYC obligations (i.e. their CDD and EDD obligations).

4.7. As set out in Regulation 7 of the 2007 Regulations, a relevant person must conduct CDD when it establishes a business relationship or carries out an occasional transaction. To effectively manage money laundering risks, a firm should hold sufficient information about its customers and, if applicable, the customers' underlying clients to inform the risk assessment process and to provide the means for monitoring customer transactions which will enable the firm to detect suspicious activity.

4.8. As set out in Paragraph 18.16 of Part II of the JMLSG Guidance, one of the main factors to consider when assessing the risk of undertaking business in the wholesale markets is the nature of the customer, including their source of funds. As noted in Paragraph 4.32 of Part I of the JMLSG Guidance, a risk-based approach to KYC should take into account the risks posed by a customer's behaviour, which could include whether the customer's source of wealth or funds can be easily verified.

4.9. As set out in Regulation 5(c) of the 2007 Regulations, a relevant person must understand the purpose and intended nature of its business relationship with a proposed customer. This information enables the relevant person to assess whether the proposed relationship is in line with its expectations and to provide it with a meaningful basis for ongoing monitoring.

4.10. If a relevant person establishes a business relationship with, or conducts an occasional transaction for, the underlying client of another business (e.g., an intermediary), Regulation 17 of the 2007 Regulations and Paragraph 5.6.4 of Part I the JMLSG Guidance permit the relevant person to rely on the CDD measures of the other business in certain circumstances. If the other business operates in a non-EEA jurisdiction, however, Regulation 17(2)(d) permits such reliance only if the other business is subject to both mandatory professional registration and to AML requirements equivalent to those set out in the Third Money Laundering Directive.

4.11. Deutsche Bank's process for conducting CDD and EDD on potential new customers was set out in its KYC policies and procedures, which in relation to Deutsche

Bank's CB&S business were supposed to be implemented by London Front Office and supported by the COB and AML teams.

4.12. During the Relevant Period, new customers could be onboarded with Deutsche Bank in the UK by other Deutsche Bank offices without the involvement of London Front Office personnel. For example, the Moscow Front Office onboarded non-Russian customers with Deutsche Bank in the UK via Deutsche Bank's UK COB team, which was largely based in India. The UK COB team reviewed the documentation that was obtained by Moscow Front Office as part of the KYC process. After being onboarded with Deutsche Bank in the UK, the relationship with the customer was managed by Moscow Front Office and there was no meaningful ongoing monitoring by Deutsche Bank of its business relationship with that customer.

4.13. For Russian customers of DB Moscow, DB Moscow had its own COB team that was based in Russia.

REMOTE BOOKING

4.14. Deutsche Bank in the UK was a key booking location for Deutsche Bank's global CB&S business. For example, during the Relevant Period, it was common practice for trades to be executed remotely by Moscow Front Office directly into Deutsche Bank's trading books in the UK. The conducting of sales or trading activity that was booked in the UK on behalf of Deutsche Bank by Deutsche Bank offices outside of the UK was known as "remote booking".

4.15. Deutsche Bank used remote booking to consolidate its risk management processes and to streamline its interactions with customers. Remote booking was widely used by Deutsche Bank throughout the Relevant Period. Approximately 30% of the assets on Deutsche Bank's UK balance sheet related to remotely booked activity from approximately 50 cities across 35 countries. In 2015, more than 500 traders were permitted to remotely book trades to the UK and there were approximately 2,000 books, corresponding to more than 150 business units, that were remotely booked to the CB&S balance sheet in the UK.

Mirror Trading

4.16. Between April 2012 and October 2014, mirror trades were used by Deutsche Bank and DB Moscow customers that were connected to each other to transfer more than USD6 billion from Russia, through Deutsche Bank in the UK, to overseas bank accounts including in Cyprus, Estonia, and Latvia. Given that the customers

were connected and the amount and value of the securities on both the Moscow and London Sides of the mirror trades was the same, the evident purpose for the mirror trades was the conversion of Roubles into US Dollars and the covert transfer of those funds out of Russia, which is highly suggestive of financial crime.

4.17. In this Notice, mirror trading refers to the following arrangement:

(1) a Russian customer of DB Moscow bought highly liquid Russian securities from DB Moscow, paying in Roubles (the Moscow Side); and

(2) at the same time, a non-Russian customer of Deutsche Bank (the onboarding of which had been initiated and facilitated by Moscow Front Office) sold the same number of the same securities to Deutsche Bank in exchange for US Dollars (the London Side).

4.18. The orders for both sides of the mirror trades were received by Moscow Front Office, which executed both sides at the same time. The London Side of the mirror trades was executed by Moscow Front Office on behalf of Deutsche Bank and remotely booked.

4.19. Moscow Front Office was able to execute the mirror trades undetected for such a considerable period because of widespread deficiencies in Deutsche Bank's AML control framework, particularly in relation to the establishment of new customer relationships and ongoing monitoring of transactions.

4.20. As a result of the deficiencies in Deutsche Bank's AML control framework, the mirror trading customers were able to place orders with Moscow Front Office on behalf of others whose identities and source of wealth were not known to Deutsche Bank.

MIRROR TRADING CUSTOMERS

4.21. The mirror trading customers were connected to each other through common directors, owners, employees, or addresses. The Moscow Side customers were incorporated and regulated in Russia and the London Side customers were non-regulated firms that were incorporated in a number of non-Russian jurisdictions.

4.22. The mirror trading customers were intermediaries that traded on behalf of undisclosed underlying clients. None of the mirror trading customers had a Deutsche Bank relationship manager and the London Front Office was not involved in the onboarding process. None of the mirror trading customers were regulated by the Authority.

4.23. Although the Moscow Side customers had a number of high risk characteristics, they were not categorised as high risk by Deutsche Bank. The London Side customers were categorised as either low or medium risk.

4.24. Although the onboarding of the London Side mirror trading customers with Deutsche Bank was initiated and facilitated by Moscow Front Office, the business relationship was with Deutsche Bank and therefore it was required to ensure that appropriate due diligence was performed. Deutsche Bank, however, did not ensure that sufficient information was obtained to verify the identities of the mirror trading customers. For example, the ownership structures were not reliably documented using independently sourced information and passport copies for the purported ultimate beneficial owners (UBOs) were not verified. Deutsche Bank was therefore unable to verify the identities of the mirror trading customers or determine whether there were any connections between them.

4.25. Deutsche Bank also failed to obtain an adequate explanation of the nature of the mirror trading customers' businesses (including their source of funds) and the purpose of their business relationships with Deutsche Bank. Some of the customers provided Deutsche Bank with informal documentation of unknown origin that described their business. Many of the customers provided CVs of their purported UBOs as evidence of source of funds. None of the mirror trading customers provided documentation regarding the purpose of their business relationship with Deutsche Bank. Deutsche Bank was therefore unable to ensure that its business relationships with the mirror trading customers were consistent with Deutsche Bank's AML risk profile. Deutsche Bank was also unable to verify the source of the more than USD6 billion that was transferred through its books via the mirror trades.

WARNING SIGNS AND MISSED OPPORTUNITIES

4.26. Deutsche Bank received several warning signs in relation to the mirror trading, but it failed to appreciate the nature and full extent of the money laundering risks until February 2015, more than three months after the last of the mirror trading customers had ceased that activity.

Internal trading reports

4.27. During the Relevant Period, London Front Office received regular trading reports that included data regarding certain trades executed by Moscow Front Office. The trading by the mirror trading customers sometimes appeared in these reports and, whilst occasionally this led to questions being asked of Moscow Front Office,

none of these enquiries were followed up properly or resulted in the identification of the mirror trades.

4.28. London Front Office sought information about the nature and activities of the mirror trading customers in December 2012, July 2013, and January 2014. The responses to these enquiries from Moscow Front Office did not provide sufficient clarity to understand either the nature of the trades or the customers and should have prompted further questions from Deutsche Bank but it did not follow up.

4.29. In addition, within Deutsche Bank it was identified in June 2014 that the trading information for one of the Moscow Side customers was anomalous because no commission appeared to have been generated from the trading. This observation prompted Deutsche Bank to ask Moscow Front Office if it was "*missing another leg to those trades?*" Moscow Front Office responded that it would check and revert but in fact no further response was ever provided and Deutsche Bank failed to follow up on the matter.

4.30. If Deutsche Bank had been more persistent in its enquiries of Moscow Front Office about the activities of the mirror trading customers, it could have discovered the existence of the mirror trades sooner.

Enquiry regarding a mirror trading customer

4.31. In January 2014, Deutsche Bank received a request for assistance (RFA), via SWIFT message, from a third-party bank regarding a review the third-party bank had conducted of wire transfer activity for one of its customers. The customer was one of the London Side customers. The third-party bank had identified wire transfers from Deutsche Bank to the customer totalling approximately USD444 million in 2013 and USD252 million in January 2014. The third-party bank asked Deutsche Bank to describe its relationship with the customer, to provide details of the transactions, and to confirm whether there was any reason to believe that the transactions were suspicious.

4.32. Deutsche Bank did not respond to the RFA in January 2014, and the third-party bank sent a reminder to Deutsche Bank in February 2014. Again, Deutsche Bank did not respond and in March 2014 the third-party bank contacted another Deutsche Bank regional office regarding the wire transfers. The regional office contacted Deutsche Bank in the UK and was informed that the relationship with the customer was managed by DB Moscow and that the matter had been escalated internally. The regional office then forwarded the enquiry from the third-party bank to Moscow Front Office to deal with.

4.33. In response to the RFA, Moscow Front Office assured the third-party bank that the mirror trading customer had been subjected to KYC procedures, that the transactions underlying the wire transfers were considered to be appropriate, and that there was no reason for concern.

Escalation to Deutsche Bank's AML team

4.34. In August 2014, DB Moscow's back-office trade settlement team discovered the existence of a mirror trade arrangement between two customers and the matter was escalated to Deutsche Bank's AML team in the UK. DB Moscow noted that it had discovered a suspicious scheme involving DB Moscow, Deutsche Bank, and two customers, one in Russia and the other in the UK.

4.35. The escalation noted that the large trading volumes were inconsistent with the profiles of the two mirror trading customers, with one customer being described as trading on behalf of "*no name*" companies.

4.36. In mid-September 2014, the Deutsche Bank AML team contacted DB Moscow's AML team to request more information about the mirror trading and the two customers. DB Moscow stated in its response that it was "*strongly convinced that they are a part of one* [money laundering] *scheme as there is no economic sense behind these transaction* [sic] *and the whole flow is organized to facilitate cross-border transfers and in order for them to look legitimate.*"

4.37. Although Deutsche Bank's AML team took steps to investigate the mirror trading, it did not obtain all of the relevant trading data. When it was informed by Deutsche Bank's Operations team that "*providing a spread-sheet will not be possible as this is done manually by a team member and capturing so many records will be painful*", the AML team did not persist with its enquiries. Therefore, although the AML team had learned that each of the two mirror trading customers had been involved in at least 900 transactions since the start of the year, it did not go further and obtain details of those trades. Such information would have shown the full extent of the trading and the potential for mirror trades to be used to facilitate large-scale money laundering.

4.38. Ultimately, in October 2014, members of the Deutsche Bank AML team addressed the mirror trading that was escalated by closing the relevant trading accounts. Of itself this would have achieved little in the way of preventing the mirror trading because the relevant customers used multiple identities.

4.39. Coincidentally, the mirror trading ceased at around the same time because DB Moscow ceased dealing with the Moscow Side customers. However at no point during this period was a wider review of relevant trading conducted and therefore the connections between the various mirror trading customers were not identified.

COMMENCEMENT OF INTERNAL INVESTIGATION

4.40. In February 2015, DB Moscow escalated further examples of mirror trading to Deutsche Bank's AML team in the UK. At the same time, DB Moscow also informed the London AML team of suspicious trading that DB Moscow had discovered in April 2014. The earlier trading had not been identified as mirror trades in April 2014 because at that time DB Moscow had not identified the London Side of the trades.

4.41. Deutsche Bank commenced an internal investigation into the mirror trades in February 2015, which led to it reporting the matter to the Authority, which opened its investigation shortly thereafter.

One-sided trades

4.42. During the Relevant Period, between January 2012 and February 2015, Moscow Front Office executed more than 3,400 securities trades through Deutsche Bank in the UK that are considered by the Authority to form one half of a mirror trade, but where the other side could not be identified. Over 99 percent of these one-sided trades were sales in which the customers sold securities to Deutsche Bank, for a total of USD3.8 billion. On the basis that most if not all of the one-sided trades were part of mirror trades, approximately USD10 billion was transferred out of Russia, through Deutsche Bank, during the Relevant Period in a manner highly suggestive of financial crime.

4.43. The customers involved in the one-sided trades included five mirror trading customers. The information provided to Deutsche Bank during the onboarding of these customers was insufficient for determining the purpose of the business relationship or the nature of the customers, including their source of wealth or funds.

Systematic Anti-Money Laundering Programme

4.44. The Authority launched its SAMLP in 2012. The programme is a supervisory tool that involves a series of AML assessments of major retail and investment banks in the UK. The Authority had already scheduled its assessment of Deutsche Bank's

AML control framework prior to the discovery of the mirror trades. The SAMLP assessment commenced in 2015 as planned shortly after the Authority was notified by Deutsche Bank in relation to the mirror trading. As part of this work, the Authority reviewed a sample of customer files and conducted interviews of numerous Deutsche Bank personnel.

4.45. The SAMLP assessment found serious deficiencies in Deutsche Bank's AML control framework and serious CDD, EDD, and ongoing monitoring failings as evidenced from a review of customer files, including those for the mirror trading customers. These failings and the failings that were identified through the investigation of the one-sided trades are set out at paragraphs 4.57 and 4.58 below.

Complex management structure and unclear responsibilities

4.46. Deutsche Bank operated a matrix management structure along regional, divisional, and product lines. Within that structure, roles and responsibilities were not clearly defined or communicated, including those relating to individuals within Deutsche Bank who held controlled functions, which resulted in significant confusion within Deutsche Bank as to the allocation of roles and responsibilities between London Front Office, the Operations team, and the AML team.

4.47. The impact of Deutsche Bank's management structure on the oversight of the onboarding process was recognised by Deutsche Bank in a 2014 presentation to an internal KYC steering committee, which stated that there were "*systemic KYC weaknesses due to a lack of clearly defined roles and responsibilities*" in multiple locations and that there was a lack of management information at the group management level "*to demonstrate governance of risk*".

Lack of resourcing

4.48. The AML functions of Deutsche Bank in the UK and of DB Moscow lacked sufficient resources. This undermined the effectiveness of the AML teams in the UK and Russia and restricted their ability to challenge the front office business and to provide effective oversight. In particular, resource constraints resulted in understaffing and prevented the implementation of appropriate KYC and AML transaction monitoring systems.

4.49. Between 2010 and 2012, Deutsche Bank mandated a global reduction in headcount and the offshoring of certain functions that resulted in a reduction in the number of staff within the Compliance function, including AML, in both the UK and Moscow. Although Deutsche Bank began recruiting additional AML personnel

in 2013, the rate at which new appointments could be made was insufficient to address the consequences of the under resourcing that affected both the quantity and quality of AML personnel at Deutsche Bank and DB Moscow.

4.50. Staff shortages in the UK AML team were regularly highlighted in reports to Deutsche Bank management. In 2012 and 2013, under resourcing was identified as the top key risk affecting the AML function in the UK. In 2012, a report to Deutsche Bank management noted that the UK AML team was "*currently stretched*" and that a resource proposal had been submitted to senior management to address the issue. In 2013, a report to Deutsche Bank management emphasised that although recently hired employees had integrated well into the UK AML team, a number of additional responsibilities had "*presented a significant challenge to the team given the current resource model*" and that it was "*clearly not going to be a sustainable model in the long term*". Insufficient headcount meant that AML personnel had to expedite their work and devote less time to oversight, supervision, training and professional development. For example the failure to appropriately address the August 2014 mirror trading escalation was due, in part at least, to a lack of resources.

4.51. DB Moscow raised concerns with Deutsche Bank on multiple occasions about under resourcing in DB Moscow's AML and COB functions. In one such communication, DB Moscow informed Deutsche Bank in December 2013 that the quality assurance of historic KYC files was "*very formalistic with no substance*", that the AML function was "*completely understaffed*", and the COB team required additional training and supervision to perform its function.

Inadequate Customer Due Diligence

4.52. Deutsche Bank's customer due diligence (CDD) was inadequate because: the culture in the CB&S division failed to instil a sense of responsibility in the London Front Office that it was ultimately responsible for Deutsche Bank's KYC obligations (see paragraphs 4.54 to 4.59 below); the customer risk rating methodology was flawed (see paragraphs 4.60 to 4.66 below); the KYC policies & procedures were deficient (see paragraphs 4.67 to 4.72 below); and the IT infrastructure was not fit for purpose (see paragraphs 4.73 to 4.75 below).

4.53. Deutsche Bank's inadequate CDD meant that it was unable to determine who many of its customers were or where their funds came from. As a result, Deutsche Bank's CB&S business was unable to assess or manage its level of money laundering risk.

ROLES AND RESPONSIBILITIES

4.54. London Front Office was primarily focused on financial risk and it failed to appreciate that it was ultimately responsible for Deutsche Bank's KYC obligations. Although London Front Office was the first line in Deutsche Bank's three lines of defence, and therefore had primary responsibility for KYC compliance, it regarded the COB team in Operations as being ultimately responsible for gathering customer information and for deciding whether a potential customer should be onboarded. The COB team, however, performed a process-driven administrative function in which it checked the completeness of KYC files. Furthermore, London Front Office often placed undue pressure on the COB team to onboard new clients, which stretched the COB team's resources and reduced its ability to perform its role.

4.55. London Front Office also placed undue reliance on the role of the UK AML team in the onboarding process. The AML team, however, only reviewed KYC information if the customer was classified as high risk or if the customer file was selected for quality assurance after onboarding. The KYC quality assurance function itself had an insufficient sampling rate of only 10 files per business line per quarter. The AML team considered this sampling rate to be too low for certain business lines that onboarded a significant number of new clients each quarter and that more resources should be made available to increase the rate.

4.56. Deutsche Bank's Group Executive Committee (GEC) recognised in 2013 that London Front Office did not appreciate that it was ultimately responsible for Deutsche Bank's KYC obligations. The GEC addressed these concerns by initiating a global KYC review programme. The implementation of the KYC review, however, was hampered by a lack of engagement from London Front Office. Several managers in London Front Office were so removed from the onboarding process that they were unaware of serious KYC issues until after Deutsche Bank commenced its internal investigation into the mirror trades.

4.57. The lack of accountability for KYC compliance contributed to the poor quality of information that was gathered during the onboarding process. All of the medium and low risk files reviewed during the SAMLP had inadequate CDD, including: missing identification and verification documents; inadequate information about UBOs; a lack of information about corporate ownership structures; poorly understood foreign-language documents; and a failure to identify PEPs as connected parties. Similarly, almost all of the higher risk files had inadequate EDD, with deficiencies such as: limited evidence of meetings with customers; and

inappropriate disregarding of negative press coverage. The common theme in both the CDD and EDD was a failure to evidence source of funds and wealth where appropriate and a lack of understanding of the customer's business.

4.58. Equivalent deficiencies were observed in the files of the customers involved in the mirror trading and one-sided trades. These deficiencies included: a lack of evidence regarding source of wealth and funds, with reliance on unverified customer CVs; a lack of information regarding the purpose of the business relationship; a failure to obtain independent verification of the ownership structure provided by the customer; and a failure to either identify the UBOs of the customers or a failure to draw attention to those customers that shared the same UBO or representative.

4.59. Deutsche Bank also notified the Authority of several thousand customer accounts, internally referred to as orphan accounts, that the front office business had opened without the proper collection of KYC information, or where they had been unable to locate that information. These orphan accounts were active customer accounts for which Deutsche Bank's systems could not generate a link to underlying KYC documentation. Concerns about orphan accounts were first raised within Deutsche Bank in 2012, and in 2014 Deutsche Bank recognised that approximately 5,000 active customers had not been onboarded in line with KYC requirements. Despite these KYC deficiencies, orphan accounts could still be used for trading. Deutsche Bank initiated a remediation programme in late 2014 to improve controls around the onboarding process.

AML RISK RATING METHODOLOGY

4.60. Deutsche Bank was unable to evaluate its level of money laundering risk partly because its customer and country risk rating methodologies were inadequate. In the CB&S business, Deutsche Bank underestimated the level of AML risk associated with its customers, with less than 5% being categorised as high risk; significantly out of line with its peers.

4.61. Deutsche Bank also failed to assign appropriate AML risk ratings to the different jurisdictions associated with its customers. The country risk rating determined the outcome of the customer risk rating if no other money laundering risk factors were present.

4.62. The AML country risk ratings were developed by Deutsche Bank in the UK using an informal and opaque methodology and the ratings were then implemented globally. Only 33 countries were categorised as high risk jurisdictions. Russia

was not one of those countries. Deutsche Bank eventually updated its country risk rating system in 2015 and it now categorises approximately 100 countries, including Russia, as high risk.

4.63. During the Relevant Period, Deutsche Bank's AML customer risk rating methodology used a scoring system based on a number of factors: jurisdiction, industry, domicile of UBOs, presence of PEPs, bearer shares, negative press, company structure, and use of intermediaries. The scoring system assigned one of three risk scores: a score of 1 was low risk and required a KYC review every five years; a score of 2 was medium risk and required a KYC review every three years; and a score of 3 was high risk, which required escalation to the AML team for further consideration and, if the customer was onboarded, annual KYC reviews.

4.64. The AML customer risk rating methodology was inadequate. The methodology failed to consistently take into account the type of legal entity that was being considered for onboarding and it did not consider the different risks associated with the different delivery channels for providing customer services. In particular, the risk rating methodology did not consider the risks associated with the lack of face-to-face contact between Deutsche Bank and the mirror trading customers.

4.65. Because of the inappropriate country risk ratings and the deficient AML customer risk rating methodology, none of the mirror trading customers were considered to be high risk and therefore were not subject to review by the AML team during the onboarding process. Similarly, almost 50% of the low risk files and 30% of the higher risk files that were reviewed during the SAMLP had been assigned inappropriate risk ratings that underestimated the level of risk associated with those customers.

4.66. Deutsche Bank identified the deficiencies in its AML customer risk rating methodology in 2013 and intended to address them as part of the global KYC review programme, but the methodology was not changed until after the commencement of the internal investigation into the mirror trades in 2015. However, even if high risk customers had been appropriately classified and subjected to review by the AML team, Deutsche Bank's AML team was unlikely to have had the capacity to review the increased number of high risk customers because of a lack of resources.

KYC POLICIES AND PROCEDURES

4.67. During the Relevant Period, Deutsche Bank operated a policy and procedure hierarchy on four levels. Level 1 policies were the global operating fundamentals and code of conduct that applied to all aspects of Deutsche Bank's business. The Level 2 requirements were high-level global minimum standards, which required each business division to develop its own AML policies and procedures. Deutsche Bank, therefore, had a decentralised AML policy framework. The Level 2 requirements were used by each division to formulate local and divisional policies (Level 3) and key operating procedures (Level 4). The Level 3 and 4 KYC policies and procedures in the CB&S business, however, were not sufficiently prescriptive and failed to provide sufficient guidance on key aspects of the onboarding process as set out in the following paragraphs.

4.68. Deutsche Bank's policies did not provide guidance on how to evidence or establish the legitimacy of a customer's sources of wealth and funds. Information regarding sources of wealth and funds was almost entirely inadequate in the files reviewed during the SAMLP. The same deficiencies were observed in the files for the customers involved in the mirror trading and one-sided trades.

4.69. The onboarding policies and procedures did not require the gathering of information about expected account activity, which meant that Deutsche Bank could not monitor whether a customer's behaviour was consistent with its profile. All of the customer files reviewed by the Authority contained negligible information about the purpose and intended nature of the business relationship.

4.70. The policies and procedures for UBOs were incomplete. As noted in Chapter 3 of the Financial Crime Guide, it is poor practice to not consider all individuals who exercise control over the management of a corporate customer when identifying and verifying a customer's UBOs. Although Deutsche Bank's policies and procedures covered individuals who own or control 25% or more of a business, they did not include those individuals who otherwise exercise control over a business, except in respect of legal representatives. Deutsche Bank's failure to consider both types of individuals meant that it could not ensure that it identified the beneficial owners of its customers.

4.71. Deutsche Bank failed to ensure that CDD was conducted on the underlying clients of customers that acted as intermediaries. Consequently, CDD was not conducted on the underlying clients of the mirror trading customers. The Level 3 and 4 KYC policies and procedures required CDD to be conducted on the underlying clients of

a customer unless the customer was regulated. For regulated customers, the Level 3 KYC policy indicated that reliance could be placed on the presumed CDD conducted by the customer. The policy, however, did not clarify the caveat in Regulation 17 of the 2007 Regulations that, for a non-EEA customer, such reliance is only permitted when the customer is subject to AML requirements that are equivalent to the Third Money Laundering Directive. As Russia is not presumed equivalent for these purposes, reliance should not have been placed on the regulatory status of the Moscow Side customers when those customers were onboarded. The failure of the policy to clarify this point contributed to the lack of CDD in relation to the underlying clients of the mirror trading customers.

4.72. Deutsche Bank's policies did not require the London Front Office to supervise the onboarding of customers in the UK by offices in other jurisdictions. Therefore Deutsche Bank relied on front office businesses in other jurisdictions to ensure that the UK was not exposed to the risk of financial crime. For example, Moscow Front Office initiated and facilitated the onboarding of all of the mirror trading customers to Deutsche Bank without the knowledge or involvement of London Front Office.

IT INFRASTRUCTURE

4.73. Deutsche Bank lacked a single authoritative repository of KYC information because it used multiple IT systems. The KYC review programme identified this as a risk, but the absence of an appropriate system was not remediated during the Relevant Period.

4.74. The absence of a single repository of KYC information had a number of consequences, including a lack of reconciliation between the trading and customer onboarding systems, which Internal Audit identified as a critical issue in 2014. The lack of reconciliation between the different systems was partly due to the absence of unique identifiers for each of Deutsche Bank's customers. Customers could be assigned different identifiers in each of the systems where their data was recorded. As a result, Deutsche Bank was unable to connect trading activity with underlying KYC information.

4.75. The lack of reconciliation between the different systems impacted Deutsche Bank's ability to monitor the trading activity of its customers; interfered with attempts by London Front Office to retrieve KYC information about its customers; and hampered Deutsche Bank's process for remediating the large number of orphan accounts.

Lack of adequate transaction and payment monitoring and oversight

4.76. As set out in Regulation 8 of the 2007 Regulations, a relevant person must conduct ongoing monitoring of the business relationship with its customers to ensure that customer transactions are consistent with the relevant person's knowledge of the customer including, where necessary, the customer's source of funds.

4.77. Although Deutsche Bank's global AML policy required the implementation of systems to monitor customer accounts for unusual or suspicious transactions, Deutsche Bank did not implement any Level 3 or 4 policies and procedures in the UK for transaction monitoring or the escalation of suspicious activity to the AML team.

4.78. A firm's transaction monitoring should be adequate to handle the volume of transactions undertaken by the firm. Paragraph 18.92 of Part II of the JMLSG Guidance notes that a firm operating in the wholesale markets is likely to engage in very high volumes of transactions executed by large numbers of customers. Because the CB&S business lacked an automated AML system for the detection of suspicious securities trades, it could not effectively monitor the high volumes of securities transactions that it executed on behalf of its customers.

4.79. The CB&S business also failed to implement an effective system for monitoring the money flows associated with transactions. The alerts generated by the payments monitoring system were reviewed in accordance with strictly defined criteria that did not allow for a risk-based review of individual alerts. This process-driven approach limited the effectiveness of the system. In addition, Deutsche Bank failed to recalibrate the system between 2011 and 2014, which meant it was significantly out-of-date during the Relevant Period.

4.80. Both the Moscow and London Sides of the mirror trades were visible in the trading systems used by Deutsche Bank. These systems, however, were not used for the monitoring of money laundering risks.

4.81. Deutsche Bank did not have adequate controls for addressing the risk of inappropriate trading behaviour being booked in the UK. The London Side of the mirror trades was booked into the UK by Moscow Front Office. Although London Front Office was responsible for the trading book, it was concerned with aggregate and open risk positions rather than individual trades, and therefore was not aware of the identities of the customers that were entering trades into the book.

4.82. London Front Office considered DB Moscow to be responsible for monitoring the remotely booked trades. Deutsche Bank's reliance on DB Moscow in this regard was misplaced, partly because the relevant parts of DB Moscow that were responsible for trade monitoring did not have access to a system that could provide data about the trades booked in the UK by DB Moscow. Furthermore, even if DB Moscow had had visibility of those trades, it was unable to introduce an effective automated trade surveillance system because of a lack of resources.

5. FAILINGS

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

5.2. Principle 3 required Deutsche Bank to take reasonable care to organise its affairs responsibly and effectively, with adequate risk management systems.

5.3. Furthermore, SYSC rules 6.1.1 R and 6.3.1 R required Deutsche Bank, broadly, to ensure that its AML control framework was comprehensive and proportionate to the nature, scale, and complexity of its activities and that it was able to identify, assess, monitor, and manage its money laundering risk.

5.4. Deutsche Bank breached Principle 3 and SYSC rules 6.1.1 R and 6.3.1 R in that, during the Relevant Period, in its CB&S business:

(1) its CDD and EDD was inadequate in that it failed to obtain sufficient information about its customers to inform the risk assessment process and to provide a basis for transaction monitoring;

(2) its culture failed to instil a sense of responsibility in the front office business for the identification and management of non-financial risks, particularly in the London Front Office, which failed to appreciate that it was ultimately responsible for Deutsche Bank's KYC obligations (in accordance with London Front Office's role as the first line of defence);

(3) it used flawed AML customer and country risk rating methodologies which meant that customers were assigned inappropriate risk ratings;

(4) its AML policies and procedures were deficient;

(5) its AML IT infrastructure was inadequate and failed to provide a single authoritative repository of KYC information;

(6) it lacked automated AML systems for detecting suspicious trades and lacked an effective system for monitoring money flows associated with transactions; and

(7) it failed to provide adequate oversight of trades booked in the UK by Moscow Front Office as well as other non-UK locations.

5.5. Because of the inadequacies in Deutsche Bank's AML control framework, it was unable to identify, assess, monitor, or manage its money laundering risk. As a result, Deutsche Bank engaged in suspicious transactions that enabled its customers to transfer approximately USD10 billion from Russia, via Deutsche Bank's UK trading books, to overseas bank accounts including in Cyprus, Estonia and Latvia without detection.

5.6. Deutsche Bank did not know the customers responsible for the suspicious trading or the money laundering risk that was associated with them. It was unable to verify the source of the USD10 billion, or determine the purpose of the transactions, and it did not have adequate systems for monitoring the trading by those customers.

5.7. Deutsche Bank's complex management structure, in which roles and responsibilities were not clearly defined, and its insufficient allocation of resources to Deutsche Bank's AML control framework contributed to Deutsche Bank's breaches of Principle 3 and the SYSC rules.

5.8. For the sake of clarity, any criticisms of a collective term in this Notice (such as, but not limited to, Moscow Front Office, London Front Office, Deutsche Bank AML team, the Management Board, or GEC) are not criticisms of all, or even necessarily any particular, individuals who fitted that description during the Relevant Period.

6. SANCTION

6.1. The Authority 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 Authority's policy for imposing a financial penalty is set out in Chapter 6 of DEPP. In respect of conduct occurring on or after 6 March 2010, the Authority applies a five-step framework to determine the appropriate level of financial

penalty. DEPP 6.5A sets out the details of the five-step framework that applies in respect of financial penalties imposed on firms.

Step 1: disgorgement

6.3. Pursuant to DEPP 6.5A.1G, at Step 1 the Authority seeks to deprive a firm of the financial benefit derived directly from the breach where it is practicable to quantify this.

6.4. Deutsche Bank made an estimated EUR11.05 million in commission payments from the mirror and one-sided trading. These were substantially credited to DB Moscow by Deutsche Bank pursuant to the brokerage arrangements between Moscow and London.

6.5. Step 1 is therefore £9,076,224.

Step 2: the seriousness of the breach

6.6. Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breach. Where the amount of revenue generated by a firm from a particular product line or business area is indicative of the harm or potential harm that its breach may cause, that figure will be based on a percentage of the firm's revenue from the relevant products or business area.

6.7. The Authority considers that the revenue generated by Deutsche Bank is indicative of the harm or potential harm caused by its breach. The Authority has therefore determined a figure based on a percentage of Deutsche Bank's relevant revenue during the period of the breach.

6.8. Deutsche Bank's relevant revenue is the revenue derived by Deutsche Bank's CB&S division in the UK as it relates to the breaches identified in this Notice. The period of Deutsche Bank's breach was from January 2012 to December 2015. The Authority considers Deutsche Bank's relevant revenue for this period to be £11,577,000,000.

6.9. In deciding on the percentage of the relevant revenue that forms the basis of the step 2 figure, the Authority considers the seriousness of the breach and chooses a percentage between 0% and 20%. This range is divided into five fixed levels which represent, on a sliding scale, the seriousness of the breach; the more serious the breach, the higher the level. For penalties imposed on firms there are the following five levels:

Level 1 – 0%

Level 2 – 5%

Level 3 – 10%

Level 4 – 15%

Level 5 – 20%

6.10. In assessing the seriousness level, the Authority takes into account various factors which reflect the impact and nature of the breach, and whether it was committed deliberately or recklessly. DEPP 6.5A.2G(11) lists factors likely to be considered 'level 4 or 5 factors'. Of these, the Authority considers the following factors to be relevant:

(1) the breach revealed serious and systemic weaknesses in Deutsche Bank's procedures and AML control framework in its CB&S division in the UK;

(2) the breach created a significant risk that financial crime would be facilitated, occasioned or otherwise occur, as evidenced by the suspicious trading allowed to occur repeatedly, on a large scale and over a lengthy period without proper AML controls being applied.

6.11. The Authority also considers that the following factors are relevant:

(1) The deficiencies in Deutsche Bank's AML control framework meant that Deutsche Bank employees in the UK were not aware or involved in the suspicious trading identified in this Notice.

(2) The AML failings were committed negligently, rather than deliberately or recklessly. There is no evidence that senior management at Deutsche Bank were aware of the existence of the suspicious trading, including the mirror trades.

6.12. Taking all of these factors into account, the Authority considers the seriousness of the breach to be level 4 and so the Step 2 figure is 15% of £11,577,000,000.

6.13. Step 2 is therefore £1,736,550,000.

6.14. DEPP6.5.3(3)G provides that the Authority may decrease the level of penalty arrived at after applying Step 2 of the framework if it considers that the penalty is disproportionately high for the breach concerned. The Authority considers that the level of penalty is disproportionate, taking into account the non-deliberate nature

of the breach and the lack of any significant financial benefit to Deutsche Bank arising from the suspicious trading.

6.15. In order to achieve a penalty that (at Step 2) is proportionate to the breach, and having taken into account previous cases, the Step 2 figure is therefore reduced to £200,000,000.

Step 3: mitigating and aggravating factors

6.16. Pursuant to DEPP 6.5A.3G, at Step 3 the Authority may increase or decrease the amount of the financial penalty arrived at after Step 2, but not including any amount to be disgorged as set out in Step 1, to take into account factors which aggravate or mitigate the breach.

6.17. The Authority considers that the following factors aggravate the breach:

(1) the Authority and the JMLSG have published a number of documents highlighting money laundering risks and the standards expected of firms when dealing with those risks. The most significant publications include the JMLSG Guidance and Financial Crime Guide (including the thematic reviews that are referred to therein), which set out good practice examples to assist firms, for example in managing and mitigating money laundering risk by (amongst other things) conducting appropriate customer due diligence, monitoring of customers' activity and guidance of dealing with higher-risk situations. Given the number and detailed nature of such publications, and past enforcement action taken by the Authority in respect of similar failings by other firms, Deutsche Bank should have been aware of the importance of appropriately assessing, managing and monitoring the money laundering risk associated with its CB&S division in the UK.

(2) Deutsche Bank's previous disciplinary history:

(a) 10 April 2006: £6.4 million penalty for breaches of Principles 2 and 5 in respect of trading misconduct;

(b) 21 August 2014: £4.7 million penalty for breaches of the Supervision Manual rules in respect of DBL's inaccurate reporting of CFD equity swaps;

(c) 23 April 2015: £226.8 million penalty for breaches of Principles 3, 5 and 11 for LIBOR-related misconduct.

(3) Deutsche Bank missed several warning signs and opportunities to identify or investigate the mirror trades before October 2014, as described in this Notice.

6.18. The Authority considers that the following factors mitigate the breach:

(1) The Authority expects regulated firms and individuals to work with the Authority in an open and co-operative manner at all times. The Authority considers that Deutsche Bank's co-operation was exceptional throughout the Authority's investigation by ensuring that senior management was engaged from the outset, conducting extensive and wide-ranging internal investigations and reporting the conclusions of those investigations to the Authority in a fully transparent manner.

(2) After its discovery of the mirror trading and the associated issues, Deutsche Bank promptly notified the Authority and commenced a large scale remediation programme across its business to correct the deficiencies in its AML control framework and customer files. The Authority has also had regard to Deutsche Bank entering into an undertaking not to take on new high risk customers in the UK until it has remediated the deficiencies in its AML controls to the Authority's satisfaction.

6.19. Having taken into account these aggravating and mitigating factors, the Authority considers that the Step 2 figure should be increased by 10%.

6.20. Step 3 is therefore £220,000,000.

Step 4: adjustment for deterrence

6.21. Pursuant to DEPP 6.5A.4G, if the Authority considers the figure arrived at after Step 3 is insufficient to deter the firm who committed the breach, or others, from committing further or similar breaches, then the Authority may increase the penalty.

6.22. The Authority considers that the Step 3 figure of £220,000,000 represents a sufficient deterrent to Deutsche Bank and others, and so has not increased the penalty at Step 4.

6.23. Step 4 is therefore £220,000,000.

Step 5: settlement discount

6.24. Pursuant to DEPP 6.5A.5G, if the Authority and the firm on whom a penalty is to be imposed agree the amount of the financial penalty and other terms, DEPP 6.7 provides that the amount of the financial penalty which might otherwise have been payable will be reduced to reflect the stage at which the Authority and the firm reached agreement. The settlement discount does not apply to the disgorgement of any benefit calculated at Step 1.

6.25. The Authority and Deutsche Bank reached agreement at Stage 1 and so a 30% discount applies to the Step 4 figure. The Step 5 figure after settlement discount is therefore £154,000,000.

6.26. The total financial penalty including the Step 1 disgorgement figure is £163,076,224.

Financial penalty

6.27. The Authority therefore hereby imposes a total financial penalty of £163,076,224 on Deutsche Bank for breaching Principle 3 (management and control) and Senior Management Arrangements, Systems and Controls (SYSC) rules 6.1.1 R and 6.3.1 R.

7. PROCEDURAL MATTERS

Decision maker

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 Deutsche Bank to the Authority by no later than 13 February 2017, 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 14 February 2017, the Authority may recover the outstanding amount as a debt owed by Deutsche Bank and due to the Authority.

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 these provisions, the Authority must publish such information about the matter to which this notice relates as the Authority considers appropriate. The information may be published in such manner as the Authority considers appropriate. However, the Authority may not publish information if such publication would, in the opinion of the Authority, be unfair to you or prejudicial to the interests of consumers or detrimental to the stability of the UK financial system.

Authority contacts

7.6. For more information concerning this matter generally, contact Jeremy Parkinson (direct line: 020 7066 0224) or David Malone (direct line: 020 7066 0870) of the Enforcement and Market Oversight Division of the Authority.

Mark Francis

Project Sponsor

Financial Conduct Authority, Enforcement and Market Oversight Division

ANNEX

RELEVANT STATUTORY PROVISIONS, REGULATORY REQUIREMENTS AND GUIDANCE

1. RELEVANT STATUTORY PROVISIONS

1.1. The Authority's operational objectives established in section 1B of the Act include the strategic objective to ensure that the relevant markets function well and the operational objective to protect and enhance the integrity of the UK financial system.

1.2. Pursuant to section 206 of the Act, if the Authority considers that an authorised person has contravened a requirement imposed on it by or under the Act, it may impose on that person a penalty in respect of the contravention of such amount as it considers appropriate.

2. RELEVANT REGULATORY PROVISIONS

2.1. In exercising its powers to impose a financial penalty and to impose a restriction in relation to the carrying on of a regulated activity, the Authority has had regard to the relevant regulatory provisions published in the Authority's Handbook. The main provisions that the Authority considers relevant are set out below.

Principles for Businesses (PRIN)

2.2. The Principles are a general statement of the fundamental obligations of firms under the regulatory system and are set out in the Authority's Handbook. They derive their authority from the Authority's rule-making powers as set out in the Act and reflect the Authority's statutory objectives.

2.3. Principle 3 provides:

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

Senior Management Arrangements, Systems and Controls (SYSC)

2.4. One of the purposes of SYSC is to increase certainty by amplifying Principle 3, under which a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

2.5. SYSC 6.1.1 R provides:

"*A firm must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable, tied agents) with its obligations*

under the regulatory system and for countering the risk that the firm might be used to further financial crime."

2.6. SYSC 6.3.1 R provides:

"*A 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."

Decision Procedure and Penalties Manual (DEPP)

2.7. Chapter 6 of DEPP, which forms part of the Authority's Handbook, sets out the Authority's statement of policy with respect to the imposition and amount of financial penalties under the Act. In particular, DEPP 6.5A sets out the five steps for penalties imposed on firms.

RELEVANT REGULATORY GUIDANCE

The Enforcement Guide

2.8. The Enforcement Guide sets out the Authority's approach to exercising its main enforcement powers under the Act.

2.9. Chapter 7 of the Enforcement Guide sets out the Authority's approach to exercising its power to impose a financial penalty.

The Financial Crime Guide

2.10. The Financial Crime Guide consolidates the Authority's guidance on financial crime and although it is not binding on firms, it refers to examples of good and poor practice in managing the risks of financial crime which firms should have regard to.

Part I, Chapter 3, Money laundering and terrorist financing

2.11. Box 3.3, which relates to risk assessment, provides the following as an example of good practice:

"*Consideration of money laundering risk associated with individual business relationships takes account of factors such as:*

- *company structures;*
- *political connections;*
- *country risk;*
- *the customer's or beneficial owner's reputation;*
- *source of wealth;*
- *source of funds;*
- *expected account activity;*
- *sector risk; and*

- *involvement in public contracts."*

2.12. Box 3.4, which relates to CDD, provides the following as an example of poor practice:

"*The firm fails to consider both:*

- *any individuals who ultimately control more that 25% of shares or voting rights of; and*

- *any individuals who exercise control over the management over a corporate customer when identifying and verifying the customer's beneficial owners. This breaches the ML Regulations."*

2.13. In April 2015, the Authority updated its guidance to include Box 3.5A, which relates to source of wealth and source of funds:

"*Establishing the source of funds and the source of wealth can be useful for ongoing monitoring and due diligence purposes because it can help firms ascertain whether the level and type of transaction is consistent with the firm's knowledge of the customer. It is a requirement where the customer is a PEP.*

'Source of wealth' describes how a customer or beneficial owner acquired their total wealth.

'Source of funds' refers to the origin of the funds involved in the business relationship or occasional transaction. It refers to the activity that generated the funds, for example salary payments or sale proceeds, as well as the means through which the customer's or beneficial owner's funds were transferred.

The JMLSG's guidance provides that, in situations where the risk of money laundering/terrorist financing is very low and subject to certain conditions, firms may assume that a payment drawn on an account in the customer's name with a UK, EU or equivalent regulated credit institution satisfied the standard CDD requirements. This is sometimes referred to as 'source of funds as evidence' and is distinct from 'source of funds' in the context of Regulation 8 and Regulation 14 of the Money Laundering Regulations 2007 and of this Guide. Nothing in this Guide prevents the use of 'source of funds as evidence' in situations where this is appropriate."

Part I, Annex 1, Common terms

2.14. Between 2012 and 2014, Annex 1 of the Financial Crime guide provided:

"*As part of their customer due diligence and monitoring obligations, firms should establish that the source of wealth and source of funds involved in a business relationship or occasional transaction is legitimate. They are required to do so when the customer is a PEP. 'Source of wealth' describes how a customer acquired their total wealth, while 'source of funds' refers to the origin of the funds involved in the business relationship or occasional transaction."*

2.15. In April 2015, this section of Annex 1 was updated and now provides:

"'*Source of wealth' describes how a customer or beneficial owner acquired their total wealth.*

'Source of funds' refers to the origin of the funds involved in the business relationship or occasional transaction. It refers to the activity that generated the

funds, for example salary payments or sale proceeds, as well as the means through which the customer's or beneficial owner's funds were transferred."

The JMLSG Guidance

2.16. The JMLSG Guidance outlines the legal and regulatory framework for anti-money laundering/countering terrorist financing requirements and systems across the financial services sector. It provides interpretation on the requirements of the relevant law and legislation and indicates good industry practice through a proportionate, risk-based approach. It is comprised of three parts.

Relevant Extracts from the JMLSG Guidance

Part I, Chapter 5.3, Application of CDD measures

2.17. Paragraph 5.3.1 provides:

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

2.18. Paragraph 5.3.2 provides:

"*The firm identifies the customer by obtaining a range of information about him. The verification of the identity consists of the firm verifying some of this information against documents, data or information obtained from a reliable and independent source."*

2.19. Paragraph 5.3.20 (2014) provides:

"*A firm must understand the purpose and intended nature of the business relationship or transaction to assess whether the proposed business relationship is in line with the firm's expectation and to provide the firm with a meaningful basis for ongoing monitoring. In some instances this will be self-evident, but in many cases the firm may have to obtain information in this regard. Whether, and to what extent, the customer has contact or business relationships with other parts of the firm, its business or wider group can also be relevant, especially for higher risk customers. The customer may have different risk profiles in different parts of the business or group."*

2.20. The guidance in Paragraph 5.3.20 (2014) was previously set out in Paragraph 5.3.21 (2011 and 2013), which provided:

"*A firm must understand the purpose and intended nature of the business relationship or transaction to assess whether the proposed business relationship is in line with the firm's expectation and to provide the firm with a meaningful basis for ongoing monitoring. In some instances this will be self-evident, but in many cases the firm may have to obtain information in this regard."*

Part I, Chapter 5.5, Enhanced due diligence

2.21. Paragraph 5.5.1 provides:

"*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 information it has collected as part of the customer due diligence process (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, the customer's beneficial owner, where applicable, and the purpose and intended nature of the business relationship."

2.22. Paragraph 5.5.2 provides:

"*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:*

(1) to inform its risk assessment process, and thus manage its money laundering/terrorist financing risks effectively; and

(2) 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."

2.23. Paragraph 5.5.6 (2013 and 2014) provides:

"*When someone becomes a new customer, or applies for a new product or service, or where there are indications that the risk associated with an existing business relationship might have increased, the firm should, depending on the nature of the product or service for which they are applying, request information as to the customer's residential status, employment and salary details, and other sources of income or wealth (e.g., inheritance, divorce settlement, property sale), in order to decide whether to accept the application or continue with the relationship. The firm should consider whether, in some circumstances, evidence of source of wealth or income should be required (for example, if from an inheritance, see a copy of the will). The firm should also consider whether or not there is a need to enhance its activity monitoring in respect of the relationship. A firm should have a clear policy regarding the escalation of decisions to senior management concerning the acceptance or continuation of high-risk business relationships.*"

2.24. The guidance in paragraph 5.5.6 was updated in 2013, the earlier guidance that was issued in 2011 provided:

"*When someone becomes a new customer, or applies for a new product or service, or where there are indications that the risk associated with an existing business relationship might have increased, the firm should, depending on the nature of the product or service for which they are applying, request information as to the customer's residential status, employment details, income, and other sources of income, in order to decide whether to accept the application or continue with the relationship. The firm should also consider whether or not there is a need to enhance its activity monitoring in respect of the relationship. A firm should have a clear policy regarding the escalation of decisions to senior management concerning the acceptance or continuation of high-risk business relationships.*"

Part I, Chapter 5.6, Multipartite relationships, including reliance on third parties

2.25. Paragraph 5.6.4 provides:

"*The ML Regulations expressly permit a firm to rely on another person to apply any or all of the CDD measures, provided that the other person is listed in Regulation 17(2), and that consent to being relied on has been given (see paragraph 5.6.8). The relying firm, however, retains responsibility for any failure*

to comply with a requirement of the Regulations, as this responsibility cannot be delegated."

Part I, Chapter 5.7, Monitoring customer activity

2.26. Paragraph 5.7.1 provides:

"Firms must conduct ongoing monitoring of the business relationship with their customers. Ongoing monitoring of a business relationship includes:

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 firm's knowledge of the customer, his business and risk profile;

b) Ensuring that the documents, data or information held by the firm are kept up to date."

2.27. Paragraph 5.7.2 provides:

"*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.*"

2.28. Paragraph 5.7.10 provides:

"Effective monitoring is likely to be based on a considered identification of transaction characteristics, such as:

a) the unusual nature of a transaction: e.g., abnormal size or frequency for that customer or peer group; the early surrender of an insurance policy;

b) the nature of a series of transactions: for example, a number of cash credits;

c) the geographic destination or origin of a payment: for example, to or from a high-risk country; and

d) the parties concerned: for example, a request to make a payment to or from a person on a sanctions list."

Part II, Chapter 18, Wholesale markets

2.29. Paragraph 18.16, which relates to the assessment of generic risk elements, provides:

"*The main factors to consider when assessing the risk when undertaking business in the wholesale markets are: the nature of the customer (including their source of funds), the market participants, the products involved; and, whether the products are exchange traded or OTC.*"

2.30. Paragraph 18.92, which relates to monitoring, provides:

"*Monitoring in wholesale firms will be affected by the fact that firms may only have access to a part of the overall picture of their customer's trading activities.*

The fact that many customers spread their activities over a number of financial firms will mean that many firms will have a limited view of a customer's trading activities and it may be difficult to assess the commercial rationale of certain transactions. Extreme market conditions may also impact on a customer's trading strategy. There are, however, specific characteristics of the wholesale market sector which will impact a firm involved in the wholesale markets monitoring activity. These include:

- *Scale of activity*

  The wholesale markets involve very high volumes of transactions being executed by large numbers of customers. The monitoring activity undertaken should therefore be adequate to handle the volumes undertaken by the firm.

- *Use of multiple brokers*

  Customers may choose to split execution and clearing services between different firms and many customers may use more than one execution broker on the same market. The customer's reasons for this include ensuring that they obtain best execution, competitive rates, or to gain access to a particular specialism within one firm. This will restrict a firm's ability to monitor a customer, as they may not be aware of all activity or even contingent activity associated with the transactions they are undertaking.

- *Electronic execution*

  There is an increasing use of electronic order routing where customers access markets directly and there is little or no personal contact between the firm and the customer in the day to day execution of the customer's business. This means that the rationale for particular transactions may not be known by the firm."

3. RELEVANT EXTRACTS FROM THE MONEY LAUNDERING REGULATIONS 2007

3.1. The 2007 Regulations provide a series of measures for the purposes of preventing the use of the financial system for the purpose of money laundering. In particular, they impose a set of requirements which all firms operating in the financial system are obliged to follow.

Meaning of customer due diligence measures

3.2. Regulation 5 provides:

"*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."

Meaning of beneficial owner

3.3. Regulation 6 provides:

"*(1) In the case of a body corporate, "beneficial owner" means any individual who—*

a) as respects any body other than a company whose securities are listed on a regulated market, ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25% of the shares or voting rights in the body; or

b) as respects any body corporate, otherwise exercises control over the management of the body.

(2) In the case of a partnership (other than a limited liability partnership), "beneficial owner" means any individual who—

a) ultimately is entitled to or controls (whether the entitlement or control is direct or indirect) more than a 25% share of the capital or profits of the partnership or more than 25% of the voting rights in the partnership; or

b) otherwise exercises control over the management of the partnership.

(3) In the case of a trust, "beneficial owner" means—

a) any individual who is entitled to a specified interest in at least 25% of the capital of the trust property;

b) as respects any trust other than one which is set up or operates entirely for the benefit of individuals falling within sub-paragraph (a), the class of persons in whose main interest the trust is set up or operates;

c) any individual who has control over the trust.

(4) In paragraph (3)—

"specified interest" means a vested interest which is—

a) in possession or in remainder or reversion (or, in Scotland, in fee); and

b) defeasible or indefeasible;

"control" means a power (whether exercisable alone, jointly with another person or with the consent of another person) under the trust instrument or by law to—

a) dispose of, advance, lend, invest, pay or apply trust property;

b) vary the trust;

c) add or remove a person as a beneficiary or to or from a class of beneficiaries;

d) appoint or remove trustees;

e) direct, withhold consent to or veto the exercise of a power such as is mentioned in sub-paragraph (a), (b), (c) or (d).

(5) For the purposes of paragraph (3)—

a) where an individual is the beneficial owner of a body corporate which is entitled to a specified interest in the capital of the trust property or which has control over the trust, the individual is to be regarded as entitled to the interest or having control over the trust; and

b) an individual does not have control solely as a result of—

(i) his consent being required in accordance with section 32(1)(c) of the Trustee Act 1925(1) (power of advancement);

(ii) any discretion delegated to him under section 34 of the Pensions Act 1995(2) (power of investment and delegation);

(iii) the power to give a direction conferred on him by section 19(2) of the Trusts of Land and Appointment of Trustees Act 1996(3) (appointment and retirement of trustee at instance of beneficiaries); or

(iv) the power exercisable collectively at common law to vary or extinguish a trust where the beneficiaries under the trust are of full age and capacity and (taken together) absolutely entitled to the property subject to the trust (or, in Scotland, have a full and unqualified right to the fee).

(6) In the case of a legal entity or legal arrangement which does not fall within paragraph (1), (2) or (3), "beneficial owner" means—

a) where the individuals who benefit from the entity or arrangement have been determined, any individual who benefits from at least 25% of the property of the entity or arrangement;

b) where the individuals who benefit from the entity or arrangement have yet to be determined, the class of persons in whose main interest the entity or arrangement is set up or operates;

c) any individual who exercises control over at least 25% of the property of the entity or arrangement.

(7) For the purposes of paragraph (6), where an individual is the beneficial owner of a body corporate which benefits from or exercises control over the property of the entity or arrangement, the individual is to be regarded as benefiting from or exercising control over the property of the entity or arrangement.

(8) In the case of an estate of a deceased person in the course of administration, "beneficial owner" means—

a) in England and Wales and Northern Ireland, the executor, original or by representation, or administrator for the time being of a deceased person;

b) in Scotland, the executor for the purposes of the Executors (Scotland) Act 1900(4).

(9) In any other case, "beneficial owner" means the individual who ultimately owns or controls the customer or on whose behalf a transaction is being conducted.

(10) In this regulation—

"arrangement", "entity" and "trust" means an arrangement, entity or trust which administers and distributes funds;
"limited liability partnership" has the meaning given by the Limited Liability Partnerships Act 2000(5)."

Application of customer due diligence measures

3.4. Regulation 7 provides:

"*(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

3.5. Regulation 8 provides:

"*(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

3.6. Regulation 14 provides:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(i) a state other than the United Kingdom;

(ii) a Community institution; or

(iii) an international body,

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

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

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

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

Reliance

3.7. Regulation 17 provides:

"*(1) A relevant person may rely on a person who falls within paragraph (2) (or who the relevant person has reasonable grounds to believe falls within paragraph (2)) to apply any customer due diligence measures provided that—*

a) the other person consents to being relied on; and

b) notwithstanding the relevant person's reliance on the other person, the relevant person remains liable for any failure to apply such measures.

2) The persons are—

a) a credit or financial institution which is an authorised person;

b) a relevant person who is—

(i) an auditor, insolvency practitioner, external accountant, tax adviser or independent legal professional; and

(ii) supervised for the purposes of these Regulations by one of the bodies listed in Part 1 of Schedule 3;

c) a person who carries on business in another EEA state who is—

(i) a credit or financial institution, auditor, insolvency practitioner, external accountant, tax adviser or independent legal professional;

(ii) subject to mandatory professional registration recognised by law; and

(iii) supervised for compliance with the requirements laid down in the money laundering directive in accordance with section 2 of Chapter V of that directive; or

d) a person who carries on business in a non-EEA state who is—

(i) a credit or financial institution (or equivalent institution), auditor, insolvency practitioner, external accountant, tax adviser or independent legal professional;

(ii) subject to mandatory professional registration recognised by law;

(iii) subject to requirements equivalent to those laid down in the money laundering directive; and

(iv)supervised for compliance with those requirements in a manner equivalent to section 2 of Chapter V of the money laundering directive.

(3) In paragraph (2)(c)(i) and (d)(i), "auditor" and "insolvency practitioner" includes a person situated in another EEA state or a non-EEA state who provides services equivalent to the services provided by an auditor or insolvency practitioner.

(4) Nothing in this regulation prevents a relevant person applying customer due diligence measures by means of an outsourcing service provider or agent provided that the relevant person remains liable for any failure to apply such measures.

(5) In this regulation, "financial institution" excludes money service businesses."