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:	**Sonali Bank (UK) Limited**
Firm Reference Number:	**207518**
Address:	**29-33 Osborn Street, London E1 6TD**
Date:	**12 October 2016**

1. ACTION

1.1. For the reasons given in this notice, the Authority hereby imposes on Sonali Bank (UK) Limited ("SBUK"):

(1) a financial penalty of £3,250,600; and

(2) a restriction in terms that for a period of 168 days from the date of this Final Notice, in respect of its regulated activities only, SBUK shall not accept deposits from customers who do not hold a deposit account with SBUK at the date of this Final Notice.

1.2. SBUK agreed to settle at an early stage of the Authority's investigation. SBUK 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 on SBUK:

(1) a financial penalty of £4,643,800; and

(2) a restriction in the terms outlined at paragraph 1.1(2) above of 240 days.

2. SUMMARY OF REASONS

2.1. Financial services firms are at risk of being abused by those seeking to launder the proceeds of crime or to finance terrorism. This undermines the integrity of the UK financial services sector. Firms are obliged to take appropriate and proportionate steps to manage such risks effectively in order to reduce the risk of financial crime. The Authority has the operational objective of protecting and enhancing the integrity of the UK financial system (the integrity objective). The integrity of the UK financial system is endangered by weaknesses which risk allowing the system to be used for a purpose connected with financial crime.

2.2. In order to manage such risks, the Authority expects firms to demonstrate a culture that supports effective regulation and expects senior management to lead from the top in this regard. Firms should ensure that robust AML controls are embedded at all levels of the business and that the importance of complying with AML requirements is impressed on all members of staff.

2.3. During the period from 20 August 2010 to 21 July 2014 ("the Primary Relevant Period"), SBUK failed to take such steps in relation to its AML governance and control systems. The weaknesses in these controls were serious and systemic, and affected almost all levels of its business and governance structure, including its senior management team, MLRO function, oversight of its branches, and policies and procedures in relation to AML. By failing to take reasonable care to manage its AML risks, SBUK breached Principle 3 during the Primary Relevant Period. Subsequently while under investigation for the above breach, SBUK breached Principle 11 by failing to notify the Authority for at least seven weeks that it had become aware of a potentially significant fraud which had occurred at SBUK.

2.4. In 2010, as part of thematic work considering financial crime controls at smaller firms, the Authority visited SBUK to assess its AML systems and controls. Following the 2010 Visit, the Authority notified SBUK of a number of serious concerns. As a result, SBUK should have been aware of the importance of ensuring that its AML controls were robust and effective.

2.5. However, although SBUK put in place a Remediation Plan, it failed to test adequately its implementation and whether the steps taken were effective. A follow-up visit by the Authority in 2014 again identified a number of serious concerns with its AML systems. The Authority requested SBUK to take a series of measures to address the immediate and ongoing risks.

2.6. At the top of the business, despite warnings from board members and from the Internal Auditors, the board and senior management failed to embed a culture of compliance throughout the firm and failed to provide adequate oversight to the MLRO department which was under-resourced.

2.7. SBUK's reporting lines to its branches were unclear and insufficient management attention was paid to compliance with AML processes. AML policy and procedure documentation was high level and failed to provide staff with meaningful practical guidance.

2.8. As a result of the above, there were serious deficiencies in the processes by which SBUK front-line staff sought to comply with their AML responsibilities and SBUK's monitoring systems failed to identify these deficiencies. These included failures to conduct adequate CDD and EDD, monitoring of transactions and customer relationships and the making of suspicious activity reports.

2.9. For example, having identified one customer as a PEP with an income of £20,000 per annum, SBUK failed to question whether significant cash and cheque deposits made by this customer were commensurate with his income and, as a result, failed to consider the AML risks involved. In another case, SBUK failed to identify publicly available information in respect of one of its customers which should have informed its AML risk assessment.

2.10. SBUK's failures are particularly serious because they left the firm open to the risk that it might be used to further financial crime.

2.11. Subsequently, in March 2015, SBUK was informed of an allegation by a customer that a significant sum of money was missing from his account. Despite being aware by no later than 27 March 2015 that the circumstances may have involved a potential fraud, SBUK failed to notify the Authority until 15 May 2015. The Authority would expect to be notified immediately of any significant fraud occurring at a firm. This is particularly important when, as was the case with SBUK, it was under investigation for its AML systems and controls at the time.

2.12. The Authority therefore imposes on SBUK:

(1) pursuant to section 206 of the Act, a financial penalty in the amount of £3,250,600; and

(2) pursuant to section 206A of the Act, a restriction for a period of 168 days, that, in respect of its regulated activities only, it shall not accept deposits

from customers who do not hold a deposit account with SBUK at the date of this Final Notice.

2.13. The Authority believes that imposing a restriction, in addition to a financial penalty, will be a more effective and persuasive deterrent than a financial penalty alone. The imposition of a restriction is appropriate because it will demonstrate to firms that fail to address deficiencies in their AML systems and controls that the Authority will take disciplinary action to suspend and/or restrict the firm's regulated activities.

2.14. The Authority acknowledges:

(1) SBUK has invested in improving its AML systems and controls. It has appointed an independent non-executive director who has specific AML skills. In addition, it has retained the services of external consultants to assist it in its review of AML systems and controls, updated the AML Staff Handbook and other AML policies and procedures, and revised the risk assessments for the on-boarding of its retail customers, PEPs and high risk accounts. The MLRO has conducted reviews of SBUK's branches, staff have undertaken refresher AML training which is more relevant to the operations of the firm and it has retained an external contractor to conduct a past business review of its client on-boarding files;

(2) SBUK and its senior management have co-operated and engaged with the Authority's investigation;

(3) SBUK has made a strategic decision to streamline its retail banking operations by closing all but two of its branches by the end of 2016.

3. DEFINITIONS

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

"the 2010 Visit" means the visit by the Authority to SBUK on 26 and 27 July 2010;

"the 2014 Visit" means the visit by the Authority to SBUK in January 2014;

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

"AML" means anti-money laundering;

"the AML Staff Handbook" means the "Anti-money laundering and countering terrorist financing Handbook for Management and Staff", the document used by SBUK to outline its AML processes and provided to its staff;

"APG" means the Asia/Pacific Group on Money Laundering, an international organisation designed to assist members in the effective implementation and enforcement of internationally accepted AML standards;

"the Audit Committee" means the committee of SBUK's board responsible for monitoring operational controls;

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

"CDD" means customer due diligence measures, the measures a firm must take to identify its customer and to obtain information on the purpose and intended nature of the business relationship, as outlined in regulation 5 of the ML Regulations;

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

"EDD" means enhanced due diligence, the measures a firm must take in certain situations, as outlined in regulation 14 of the ML Regulations;

"FATF" means the Financial Action Task Force, an inter-governmental body designed to promote a co-ordinated international response to money laundering;

"the Handbook" means the Authority's Handbook of rules and guidance;

"the Internal Auditors" means the firm appointed by SBUK to conduct audits of its systems and controls during the Primary Relevant Period;

"JMLSG" means the Joint Money Laundering Steering Group, a group made up of the leading UK trade associations in the financial services industry with the aim of promulgating good practice in countering money laundering;

"the ML Regulations" means the Money Laundering Regulations 2007;

"MLRO" means the money laundering reporting officer;

"PEP" means politically exposed person, as defined in regulation 14(5) of the ML Regulations;

"Principle" means one of the Authority's Principles for Businesses;

"the Primary Relevant Period" means 20 August 2010 to 21 July 2014;

"the Remediation Plan" means the series of measures designed by SBUK to remediate the issues identified by the Authority during the 2010 Visit;

"SAR" means suspicious activity report, a report of suspected money laundering to be made by any employee to the MLRO, as required by Part 7 of the Proceeds of Crime Act 2002;

"SBUK" means Sonali Bank (UK) Ltd;

"the Secondary Relevant Period" means 27 March 2015 to 15 May 2015;

"the Skilled Person" means the skilled person appointed pursuant to section 166 of the Act to assess and report upon SBUK's AML processes;

"SUP" means the part of the Handbook entitled "Supervision"; and

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

4. FACTS AND MATTERS

Background

4.1. SBUK is the UK subsidiary of Sonali Bank Limited, which is based in Bangladesh, and is ultimately owned by the Bangladesh government. SBUK has been authorised since 6 December 2001 and provides banking services to the Bangladeshi community in the UK. During both the Primary and Secondary Relevant Periods, SBUK operated six branches in the UK and the services it offered included personal and corporate accounts, money remittance services to Bangladesh (conducted face-to-face and by telephone) and trade finance.

4.2. In 2014, SBUK had 2,457 live customer accounts and 85,625 registered remitters, of which 11,268 had been active in the preceding 12 month period. Its turnover was £10,113,368.

AML legal and regulatory obligations

4.3. Fighting financial crime is an issue of great international significance and has been a top political priority of the UK and the EU for a number of years. Authorised firms play a key role in the UK's fight against financial crime and must

have in place effective, proportionate and risk-based systems and controls to ensure that their businesses cannot be used for financial crime. The importance of firms' systems and controls in preventing financial crime was identified as one of the Authority's seven forward-looking areas of focus in its 2015/16 Business Plan.

4.4. Activities involving the international transfer of funds, the remittance of cash and non-face-to-face business each pose significant AML risks. Moreover, Bangladesh is regarded as a higher risk jurisdiction for AML risks. In July 2009, a Mutual Evaluation Report of the APG assessed that Bangladesh "*faces significant risks of money laundering (ML) and some risks of terrorism financing (TF). The authorities readily acknowledge the prevalence of corruption, narcotics trafficking and human trafficking*." In October 2010, the FATF identified strategic deficiencies in Bangladesh's AML regime, resulting in it monitoring the country's on-going AML compliance process. In February 2014, the FATF reported that Bangladesh is no longer subject to this monitoring process. However, the country and relevant government bodies continue to work with the APG to address the full range of AML issues identified in the July 2009 Mutual Evaluation Report.

4.5. Authorised firms are required by the ML Regulations and by the Authority's rules to put in place policies and procedures to prevent and detect money laundering. These include systems and controls to identify, assess and monitor money laundering risk as well as conducting CDD, EDD and ongoing monitoring of both business relationships and transactions to manage the risks identified. Firms must determine the extent of monitoring on a risk-sensitive basis depending on the type of customer, business relationship and product or transaction.

4.6. Firms have access to considerable guidance on how to comply with their duties. Since 2011, the Authority has published guidance on the steps that firms can take to reduce their financial crime risk and examples of good and bad practice.

4.7. Further, since 1990, the JMLSG has published detailed written guidance on AML controls. This provides guidance on compliance with the legal requirements of the ML Regulations, regulatory requirements in the Handbook and evolving best practice within the financial services industry.

4.8. Firms that do not put in place robust and effective AML systems may be perceived to have an unfair competitive advantage over firms that are compliant, both because they save the costs involved in implementing such systems and because they may attract customers who do not wish to undergo appropriate CDD and EDD checks.

Assessments of SBUK's AML systems and controls

The 2010 Visit

4.9. On 26 and 27 July 2010, as part of thematic work considering financial crime controls at smaller firms, the Authority visited SBUK to assess its AML systems and controls. Subsequently, on 20 August 2010, the Authority notified SBUK of a number of serious concerns.

4.10. These findings should have alerted SBUK to the need to ensure that there was a sufficient focus on AML measures throughout its business and to ensure that compliance with legal and regulatory requirements was prioritised.

4.11. As a result of the Authority's concerns, SBUK put in place the Remediation Plan and took a number of steps to rectify the issues identified. This included redrafting the AML Staff Handbook and upgrading its AML processes. SBUK's senior management committed to ensuring that financial crime issues were given closer attention in the future.

The 2014 Visit

4.12. In January 2014, the Authority visited SBUK as part of follow-up thematic work to assess AML controls in small banks. Notwithstanding the measures taken as a result of the 2010 Visit, the Authority identified serious AML failings.

4.13. The Authority requested that SBUK take a number of immediate actions to address the risks posed by its AML weaknesses. These included lowering the remittance threshold for obtaining source of funds information, screening its customers to identify PEPs, conducting EDD on all PEPs and high risk customers and carrying out visits to its branches to assess their AML systems.

The Skilled Person

4.14. As a result of concerns arising from the 2014 Visit, a Skilled Person was appointed to assess and report upon SBUK's AML systems and controls. On 21 July 2014, the Skilled Person reported its findings. It concluded that there were "*systemic*" AML failings arising from "*a lack of understanding and implementation of systems and controls throughout the Bank*".

4.15. Following the Skilled Person's report, the decision was made to refer SBUK for investigation. The Authority appointed investigators on 30 September 2014.

SBUK's AML systems and controls

4.16. During the Primary Relevant Period, SBUK failed to maintain adequate systems and controls to manage the risk of money laundering and financial crime. These failures were systemic, and affected almost all levels of its business and governance structure. Failings were noted in the following areas in particular:

(1) SBUK's board of directors;

(2) SBUK's senior management team;

(3) SBUK's MLRO function;

(4) SBUK's oversight of its branches;

(5) SBUK's AML policies and procedures; and

(6) SBUK's AML control systems.

4.17. These failings are set out below. For the sake of clarity, any criticisms of the board, senior management, MLRO department, Audit Committee, or any other body referred to using a collective term (including any variation of any of the preceding collective terms) are not criticisms of all, nor even necessarily any particular, individuals who may have been a part of any of these bodies during the Primary Relevant Period or the Secondary Relevant Period.

Board of directors

4.18. SBUK's board of directors met quarterly during the Primary Relevant Period. The board was responsible for ensuring that resources were adequate for effective compliance with AML requirements and for ensuring that adequate systems were in place for recognising, deterring and preventing all criminal activity including money laundering.

4.19. The board delegated to the Audit Committee responsibility for reviewing operational control matters and overseeing the internal audit programme, including assessing compliance coverage of all risks relating to financial crime.

4.20. The board failed to act cohesively and effectively during the Primary Relevant Period. There was a lack of experience and expertise in relation to regulatory and compliance matters and manifest differences in opinion and approach to complying with regulatory requirements which affected the board's ability to operate effectively as a collective unit.

4.21. The board relied in part upon the knowledge of independent non-executive directors yet failed to ensure that all their recommendations were effected. For example, in September 2010, the board's attention was drawn to "*a cultural mind-set which needed to change*" in relation to AML issues. Despite this, and similar expressions of concern made to the board during the Primary Relevant Period, the board took insufficient steps to ensure that the importance of AML compliance was ingrained throughout the business.

4.22. Although the board initially monitored the progress of the Remediation Plan, it made insufficient enquiry into the effectiveness of the measures taken and, by March 2011, the Remediation Plan did not feature on the board agenda. This meant that the board was not able to satisfy itself that the implemented measures were operating effectively. The board failed to consider, assess, document and mitigate adequately the risks to which SBUK was exposed, including that of AML compliance. In 2012, the Internal Auditors drew attention to a lack of evidence to demonstrate that SBUK had identified and considered the conduct risks to which it was exposed, that SBUK's risk register was not reflective of the risks faced and that there was a lack of any demonstrable link to the tasks listed in SBUK's compliance monitoring plan. They recommended that the board approve a conduct risk appetite statement and that SBUK review its compliance monitoring plan.

4.23. Despite this, in 2013, the Internal Auditors reported that no conduct risk appetite had been documented, that the risk register had not been updated and that the compliance monitoring plan remained insufficiently focussed on high-risk areas. As a result, SBUK's board failed to ensure that it was sufficiently sighted of the risks to which it was exposed, including the risk of being used for money laundering or other financial crime.

4.24. Further, the board failed to provide effective oversight of senior management responsible for ensuring systems and controls were robust and routinely accepted without challenge management assurances on the effectiveness of AML controls. For example, despite identifying from a report of the Internal Auditors in June 2012 that it was "*clear that the management have failed in some areas*", the Audit Committee accepted the recommendations of senior management and failed to take steps to ensure that failures were remediated adequately.

4.25. Although the board received regular financial crime reports, it raised insufficient challenge to the conclusions reached and failed to enquire adequately into the oversight of the implemented systems.

4.26. Accordingly, during the Primary Relevant Period, SBUK's board:

(1) failed to act cohesively and effectively;

(2) failed to take adequate steps to address the warnings of independent non-executive directors of a weak AML compliance regime;

(3) failed to take appropriate steps to satisfy itself that the Remediation Plan had been effectively implemented;

(4) failed to ensure it was sufficiently sighted of the risks to which SBUK was exposed; and

(5) failed effectively to oversee senior management or to challenge the effectiveness of AML systems.

Senior management team

4.27. It was the responsibility of SBUK's senior management to ensure that sufficient focus was given to AML issues at all levels of the business, to ensure that all staff members were capable and adequately resourced and to ensure that AML systems and controls were robust and effective.

4.28. Following the 2010 Visit, SBUK's senior management oversaw the Remediation Plan. The Remediation Plan was accepted as complete in December 2011 without sufficient testing of its implementation to determine whether the required steps had been taken or how effective the systems introduced as a result were operating.

4.29. At no time during the Primary Relevant Period did SBUK's senior management put in place a coherent strategy for addressing AML risk. As identified above at paragraph 4.23, SBUK's senior management failed to act on the recommendations of the Internal Auditors to ensure that all risks were identified, assessed and recorded within a risk register.

4.30. As part of the Remediation Plan, SBUK's senior management received monthly Compliance and Financial Crime reports from the MLRO department. However, these were formulaic, provided insufficient analysis on the effectiveness of systems and controls, failed to highlight particular risks or issues for the immediate attention of management and were subject to insufficient challenge by the senior management team.

4.31. The senior management team failed to take responsibility for ensuring that AML issues were sufficiently prioritised throughout the business. Overall, senior management was willing to accept assurances that compliant AML systems were in place without conducting any adequate enquiry as to the effectiveness of these systems and despite adverse reports from the Internal Auditors.

4.32. In 2010, as part of the Remediation Plan, SBUK informed the Authority that it had appointed an external firm to carry out its internal audit functions and that it will "*pay close attention to whether the* [AML] *procedures are being correctly followed*".

4.33. On the basis of their work, the Internal Auditors produced regular reports, relevantly in each of the years 2011 to 2013. The reports identified significant weaknesses in SBUK's control systems, some of which related to AML issues. Several of these are outlined in this Notice.

4.34. Overall, in 2011 the Internal Auditors graded the risks and controls associated with SBUK's governance and regulation activities as '3', indicating 'actual/potential significant implications for SBUK as a whole or as a business area (say a department)'.

4.35. In both 2012 and 2013, the grading was '4' – the highest grade available, indicating 'actual/potential very serious implications for SBUK'.

4.36. In respect of several failings, the Internal Auditors noted that they persisted in subsequent years despite the assurances of senior management that they would be remediated.

4.37. Despite these indicators, between 2011 and 2013, the number of days allocated by the Internal Auditors to consideration of governance and regulation matters was reduced from 18 days in 2011 to 8 days by 2013.

4.38. The failure of SBUK's senior management to react appropriately to the adverse findings of its own independent Internal Auditors and to improve adequately the control framework is a clear indicator that senior management was insufficiently focussed on compliance in general and AML systems in particular.

4.39. As a result, senior management failed to ensure that SBUK fostered a culture which valued robust adherence to its regulatory responsibilities and allowed a culture of minimal, or non-compliance to persist throughout the firm.

4.40. Accordingly, during the Primary Relevant Period, SBUK's senior management:

(1) failed to test adequately the implementation of the Remediation Plan;

(2) failed to put in place a coherent strategy for addressing AML risk;

(3) failed to challenge sufficiently the MLRO on the contents of monthly reports;

(4) failed to exercise effective management oversight of the MLRO department;

(5) failed to enquire adequately into the effectiveness of AML systems;

(6) failed to take appropriate heed of the warnings of the Internal Auditors and to remediate adequately the issues identified; and

(7) allowed a culture of minimal or non-compliance throughout the firm to persist.

MLRO function

4.41. The MLRO function was responsible for monitoring and ensuring SBUK's compliance with its AML responsibilities. It was therefore important that the MLRO function was properly equipped with staff who had adequate skills and experience, and systems which enabled effective monitoring.

4.42. In addition to his role overseeing the AML systems and controls, until 2014, SBUK required its MLRO:

(1) to act as compliance officer;

(2) to act as line manager to staff;

(3) to undertake responsibilities for appropriate training; and

(4) to undertake some company secretarial work, including taking, and subsequently typing up, minutes at board and Audit Committee meetings.

4.43. Having identified in March 2013 that the MLRO function required further staffing, although steps were taken from the summer of 2013 onwards, SBUK did not recruit another staff member until January 2014. The lack of adequate resource during this period adversely affected the monitoring carried out by the MLRO function: for example, in August 2013, the Internal Auditors noted that only 17

reviews of trade finance files had been carried out, rather than the 75 mandated by SBUK's procedures.

4.44. In addition to staffing, SBUK failed to provide the MLRO department with adequate resources. Despite the MLRO recommending membership of a commercial crime information service in each of the MLRO reports for 2011 to 2013, SBUK failed to purchase the suggested service or an alternative.

4.45. The MLRO also recommended software enhancements in each of the MLRO reports for 2011 to 2014 in relation to SWIFT message sanctions screening, which was implemented in 2015. In 2012 the MLRO recommended that upgrades to remittance software were required to ensure that transactions were automatically screened against sanctions lists and this was implemented in the second half of 2014. SBUK failed to implement the necessary upgrades in a timely manner.

4.46. In 2011 SBUK started a project to replace its IT system which would have provided enhanced AML functionality. SBUK is still working on implementation of this new system.

4.47. The Authority acknowledges that external factors have been involved in the delay in implementing the new system. Nevertheless, senior management's lack of sufficient focus on AML systems meant that they have not responded adequately to the delay. Therefore senior management failed to ensure that SBUK was equipped properly to carry out its functions effectively.

4.48. During much of the Primary Relevant Period the MLRO department did not have adequate resources and was overstretched which hampered its ability to carry out its functions. In particular:

(1) the MLRO was required to perform significant work in excess of what should have been his primary function;

(2) it took ten months to recruit a staff member after SBUK had identified the need for more staff in the MLRO department; and

(3) SBUK failed to provide IT upgrades and software in a timely manner which would have assisted the MLRO function in conducting its duties more effectively.

Oversight of branches

4.49. SBUK's head office was based in London. It operated five additional branches, providing retail banking and money remittance services to Bangladeshi communities outside central London.

4.50. Reporting lines from the branches to SBUK's head office were unclear. While some visits to branches were made by senior management during the Primary Relevant Period, these were focused on the administrative operations of the branches and did not consider compliance with AML processes.

4.51. As a result, AML compliance was not embedded in the reporting lines of branch staff or management and insufficient ongoing management attention was focused upon the effectiveness of AML systems within the branches, although half yearly conferences were conducted for branch managers at which AML issues were discussed.

4.52. The MLRO reports of 2012, 2013 and 2014 each outlined a recommendation for a regular program of visits to be conducted by the MLRO to the branches. As a result of a lack of resources in the MLRO department, these visits did not take place until after the Authority's feedback from the 2014 Visit. Despite being alerted by the MLRO reports for three successive years to the need for branch visits, SBUK's senior management took no steps to ensure that they took place.

4.53. Instead, AML oversight of the branches was conducted by the (already under-resourced) MLRO department's transaction monitoring and by dealing with ad hoc queries posed by branch staff. This led to a culture amongst branch staff of reliance on the MLRO department to ensure that AML monitoring and reviews were satisfactorily completed.

4.54. When members of the senior management carried out branch visits in April 2014, SBUK identified a lack of adequate understanding of AML issues among some branch managers and staff, including unsatisfactory knowledge of CDD, EDD, customer risk assessments and the circumstances in which a SAR was necessary.

4.55. In summary, there was insufficient contact between SBUK's head office and its branches to ensure that branches were operating in compliance with regulatory requirements. There was an over-reliance on the MLRO function and a failure to identify a lack of adequate understanding of AML issues among some branch managers and staff.

AML policies and procedures

4.56. SBUK maintained the AML Staff Handbook which contained its AML policy and procedures. It was redrafted following the 2010 Visit with the assistance of external consultants and subsequently approved by the board on an annual basis. The AML Staff Handbook was a high level manual that provided insufficient practical guidance to staff to assist them with carrying out their functions effectively. Staff were provided with the AML Staff Handbook but were given limited further documentary guidance on how to follow the AML processes. This meant that staff were not provided with adequate guidance on how to comply with SBUK's AML processes.

4.57. For example, staff were instructed that prior to establishing a relationship or opening an account, they were required to obtain "*sufficient due diligence*" but the guidance did not specify what would be considered as "*sufficient*".

4.58. Members of staff were required to obtain evidence of source of funds for cash remittances of £9,000 and above (reduced to £2,000 and above in January 2014) but no guidance was provided on what form this evidence should take. This was despite cash remittances being a key risk area for the business. The lack of specific guidance in this area led to staff processing very large cash remittance transactions with little evidence of source of funds. For example, a cash remittance transaction of £10,000 (a significant sum compared to the income of the remitter) was processed where the only documented evidence of source of funds obtained consisted of a withdrawal slip. It does not appear that adequate consideration was given as to whether this was sufficient in such circumstances, or whether further information, such as evidence of the activity that generated the funds, was necessary.

4.59. The AML Staff Handbook was at times contradicted by the MLRO Reports. For example, from January 2012, the AML Staff Handbook provided for SBUK to treat all new customers as high risk for the first six months. However, the 2012 and 2013 MLRO Reports stated that SBUK's policy was "*not to conduct relationships with any individual or organisation which it considers to be high risk or engages in high risk activities, except for correspondent banking relationships*".

4.60. Moreover, the MLRO Reports provided that all account applications for high risk customers and subsequent reviews were required to be signed off by senior management. However this provision was not set out in the AML Staff Handbook and consequently was not communicated to staff. It remained unclear for the

duration of the Primary Relevant Period how these policies coincided with the classification of all new customers as high risk. In practice, the requirement in the MLRO Reports was not followed: while senior management did sign off some categories of customer, they did not sign off all high risk customers.

4.61. The first time a customer underwent a considered risk assessment was after the initial six months when the customer was assessed as low, medium or high risk. This review was largely limited to a manual paper exercise involving a paper diary system because, until mid-2013, SBUK databases did not have the capability to record review dates. This meant that the review after the initial six months was not always conducted on time.

4.62. The AML Staff Handbook listed a number of factors to be used in making a risk assessment of an individual customer but provided insufficient guidance on how these factors interrelated or how staff should use them in an individual case. Although the AML Staff Handbook required ongoing periodic reviews, it did not provide details of what information these reviews should consider.

4.63. The AML Staff Handbook set out SBUK's policy and procedural requirements for carrying out EDD, but it did not explain adequately what EDD was, and did not provide staff with guidance on how to carry out EDD.

AML control systems

Customer Due Diligence

4.64. Following the 2010 Visit, the Authority had alerted SBUK to deficiencies in its CDD processes.

4.65. Despite this, when the Authority examined 16 files during the 2014 Visit, it found a failure to carry out adequate CDD, including a lack of documented evidence of the purpose and intended nature of the business relationship and information relating to the expected turnover or transactional activity. As a consequence, these files lacked suitable information to assess whether account activity was consistent with the anticipated activity.

4.66. The Skilled Person found a systemic failure to carry out sufficient CDD. Failings included scanned documentation which was unclear, out of date identification documentation, incomplete account opening forms and insufficient information about expected account activity.

4.67. Following the Skilled Person's Report, SBUK identified 2,457 live customer accounts. Each file suffered from a lack of appropriate documentation.

Enhanced Due Diligence

4.68. The ML Regulations require firms to carry out EDD in any situation which can present a higher risk of money laundering. SBUK's policies required it to carry out EDD in respect of all high risk customers. The AML Staff Handbook reflected this requirement. The classification of all new customers as high risk therefore required SBUK to conduct EDD on all of these customers. In fact, SBUK routinely failed to carry out EDD in respect of its new customers, on the basis that they were not in fact high risk for these purposes.

4.69. The result of this was that SBUK failed to follow its own policies and failed to give any meaningful consideration to whether the risks of a particular customer merited carrying out EDD.

Ongoing monitoring

4.70. The MLRO department did not review live customer accounts at all until a review in 2011. This review found that in most cases the customer information was not up to date resulting in SBUK writing to 300 customers and requesting information. These included customers whose account activity involved large cash transactions or transactions which did not appear consistent with their customer profile. SBUK did not undertake any subsequent periodic reviews of its customer files and in 2014 approximately 20% of live customer files were still found to be deficient, demonstrating CDD was still not being carried out properly.

4.71. A sample review of customer files by the Skilled Person found that the reviews undertaken by the MLRO department after the initial six months was flawed. For example, the reasons for classifying a customer as high, medium or low risk were not always documented adequately.

4.72. After the initial six month review, SBUK failed to carry out ongoing monitoring of customer relationships beyond the monitoring of certain transactions. This meant that, after the initial six month review, insufficient consideration was given to the AML risks posed by a particular customer unless he or she completed an individual transaction which was subject to monitoring. This meant that there was a risk that customers were not classified appropriately which would have impacted on the level of due diligence undertaken on customers and the frequency of monitoring determined. The decision whether to monitor a particular transaction

was generally made by reference to the transaction itself rather than by any consideration of the risks posed by the customer.

4.73. For example, one customer who was identified by SBUK as a PEP and whose income had been noted in 2007 as £20,000 per annum, had made a number of significant cash and cheque deposits. SBUK had failed to consider whether these deposits were commensurate with his earnings and, accordingly, whether the account activity posed increased AML risks.

4.74. Until February 2011, SBUK conducted no documented monitoring of transactions. From February 2011, the MLRO department monitored transactions by reviewing a series of daily reports which flagged transactions that fell outside pre-set criteria. Of these, the MLRO department investigated transactions on a sample basis. The rationale for selecting the sample was unclear and the number of transactions investigated depended on the resource available.

4.75. SBUK operated two separate systems for money remittances throughout the Primary Relevant Period. However, the MLRO department was unaware that it only received daily reports in respect of one of these systems. As a result, a significant number of transactions were not subject to monitoring.

4.76. In 2012, the Internal Auditors recommended that the parameters for the daily reports be reviewed and that all transactions on the reports should be investigated. However, SBUK did not follow this recommendation.

4.77. SBUK's systems were unable to detect linked transactions or transactions from a number of remitters to a single beneficiary. Moreover, individual branches could not access the remittance history of a customer from other branches and the MLRO department could not access remittance histories from branches other than the Head Office.

4.78. This meant that SBUK failed to assess the overall risks posed by particular customers. For example, the Skilled Person examined a remittance transaction of £10,000. When assessing the risk of the transaction and of the customer, SBUK did not document any considerations regarding the fact that the customer's stated income was £28,000 and that, in less than 18 months, he or she had remitted over £25,000. As a result, the transaction was not considered by SBUK to be suspicious and no documented assessment of the risk posed by the customer was made.

Monitoring of PEPs and EDD

4.79. Until 2014, SBUK did not conduct routine screening of its customer list to identify PEPs. Although checks were carried out in respect of new customers, SBUK failed to identify some customers who should have been assessed as PEPs. On other occasions, information which suggested customers were PEPs was discounted without any documented reasoning. This meant that SBUK risked failing to appropriately identify PEPs.

4.80. Even when SBUK identified a customer as a PEP, it did not always carry out adequate EDD. In particular, it failed to establish adequately the source of particular funds or the source of the customer's wealth. Even when areas of concern or adverse information were identified, these were not always sufficiently considered and the associated risks identified and considered. There was a failure to document adequately the rationale for the steps taken.

4.81. In one case, SBUK failed to identify that several PEPs sat on the board of one of its customers and failed to consider publicly available information concerning corruption investigations involving this customer. As a result, SBUK's risk assessment of this customer was seriously deficient.

Suspicious Activity Reporting

4.82. It was the responsibility of SBUK staff members to refer any suspicious activity to the MLRO department by completing a SAR. Throughout the Primary Relevant Period, SBUK staff made very low levels of SAR submissions. In each of the annual MLRO reports between 2011 and 2014, the MLRO Report described the lack of SARs referred by staff, particularly in the trade finance part of the business, as "*surprising*". Each report stated that this "*may well be attributable to the fact that the vast majority of counterparties to the LCs* [letters of credit] *are familiar to the trade Finance staff*".

4.83. Despite this potential indicator that staff were not reporting suspicious activity appropriately, no adequate investigation of the reasons for the low levels of submissions was made and SBUK accepted the explanation given as sufficient without any challenge.

4.84. Following the report of the Skilled Person, SBUK reviewed its customer files and a sample of its remittance transactions. As a result, an additional 141 SARs were submitted to the MLRO department in respect of account holders and 102 SARs in

respect of remittance transactions. This is a clear indicator that staff had previously failed to report suspicious activity appropriately.

Correspondent Banks

4.85. SBUK was notified following the 2010 Visit that its correspondent banking files contained very poor records. In October 2012, the MLRO identified that the files were "*in a mess*". Despite this, a full review of correspondent banking relationships was not carried out until December 2013 at which point four relationships with correspondent banks were suspended as a result of AML issues.

4.86. Even when SBUK identified adverse information about its correspondent banks, it did not always act upon this in a timely fashion or at all. On occasions, it relied upon assurances from the correspondent bank that the information was baseless or failed to provide documented reasons for reaching conclusions on the risks posed.

4.87. Even when SBUK identified that directors or shareholders of correspondent banks were PEPs, it failed to record this status on its PEP register.

Trade Finance

4.88. Monitoring of trade finance transactions was undertaken by the MLRO department. While some investigations were carried out, SBUK could not demonstrate that effective CDD measures were undertaken adequately. Transactions were approved by the MLRO department with insufficient evidence of any analysis and reasoning was not always documented.

4.89. In 2013, the Internal Auditors identified that the level of monitoring of trade finance files was not taking place to the extent provided by SBUK's internal procedures. This was as a result of a lack of resourcing in the MLRO department.

4.90. The Internal Auditors considered a sample of 35 trade finance files. They identified an error rate of 83%, including insufficient CDD and a failure to gain approval from the MLRO in respect of high risk transactions. It was noted that "*high risk*" was not defined and a recommendation was made to update the trade finance manual. SBUK did not follow this recommendation.

Money Service Bureaux

4.91. In October 2013, SBUK agreed to provide banking services for seven money service bureaux, each of which provided money remittance services. SBUK

provided these services despite identifying various deficiencies in the AML processes of some of the money service bureaux. These included outdated process documentation, registration forms which lacked full information or were not completed, staff with inadequate knowledge and incomplete training records.

4.92. SBUK later terminated the relationships with six of the seven money service bureaux. It retained the relationship with one on the basis that SBUK was satisfied that appropriate AML systems and controls were in place.

4.93. Accordingly, there were serious deficiencies in SBUK's AML control systems, including:

(1) a systemic failure to carry out adequate CDD;

(2) a system of customer risk assessments which failed to consider adequately the individual risks posed by each individual customer and instead initially deemed each as high risk;

(3) a systemic failure to carry out EDD on new customers, despite deeming them all high risk;

(4) a failure to conduct adequate ongoing monitoring of customer relationships, including weaknesses in transaction monitoring systems;

(5) a failure to identify PEPs and to carry out adequate EDD on those customers identified as PEPs;

(6) a failure by staff members to submit SARs when appropriate;

(7) a failure to maintain adequate correspondent banking files;

(8) a failure to maintain adequate controls over trade finance transactions; and

(9) the provision of banking services to money service bureaux offering money remittance services, even when SBUK identified that their AML systems were deficient.

Notification of fraud

4.94. On 18 March 2015, SBUK received a complaint from a branch customer that a significant sum of money (some £23,000) was missing from his account. This money had been removed from the account the previous year. SBUK's senior

management was made aware of the complaint on 19 March 2015. They instructed the branch to investigate the matter and to keep senior management updated on its findings.

4.95. By no later than 27 March 2015, SBUK had been informed that the customer alleged that the missing money had been misappropriated by a senior employee of SBUK and that withdrawal documentation was missing.

4.96. SBUK was aware of the requirement within SUP 15.3.17 of the Authority's rules to notify the Authority immediately if an employee may have committed fraud against one of its customers and the event was significant. Moreover, at the time of learning of the potential fraud, SBUK was under investigation by the Authority for failings in its AML and financial crime systems and controls. Accordingly, it should have been aware that the Authority would expect to be notified.

4.97. However, SBUK did not notify the Authority until 15 May 2015, at least seven weeks after it first became aware of the potential fraud. SBUK acknowledged in its notification of the incident to the Authority that it considered the matter significant for disclosure purposes in view of the amount of the fraud and the potential reputational risk and loss to SBUK.

5. FAILINGS

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

5.2. Principle 3 requires that a firm take reasonable steps to ensure that it has organised its affairs responsibly and effectively, with adequate risk management systems.

5.3. SBUK breached this requirement in that, during the Primary Relevant Period:

(1) it failed to take adequate steps to ensure that the importance of AML compliance was ingrained throughout the business, despite receiving clear warnings of a culture of non-compliance;

(2) it did not ensure that the ongoing effectiveness of the measures introduced by the Remediation Plan was monitored and assessed effectively;

(3) it failed to ensure that its board and senior management were provided with sufficiently clear information to ensure that they were adequately sighted of the AML risks faced by the business and able to assess how they were being addressed;

(4) it ignored warnings from the Internal Auditors of weaknesses in its governance systems and controls;

(5) it failed to ensure that the MLRO department was adequately resourced;

(6) it failed to implement adequate oversight of the MLRO department;

(7) managerial oversight of its branches was confused and did not sufficiently consider AML compliance;

(8) its policies on AML compliance failed to provide adequate practical guidance to staff;

(9) its policy on the risk assessment of customers was unclear and contradictory;

(10) it failed to carry out adequate CDD when establishing a business relationship and its systems failed to identify that CDD measures were inadequate;

(11) it failed to carry out EDD in higher risk situations and its systems failed to identify that EDD measures were inadequate;

(12) it failed to conduct on-going monitoring of some customer relationships;

(13) its transaction monitoring was conducted on a sample basis, the rationale for which was unclear, omitted to consider some transactions, was insufficiently documented and failed to consider all relevant information;

(14) it failed to take adequate measures to identify PEPs and to apply adequate EDD measures to those identified as PEPs; and

(15) its staff failed to identify and report suspicious activity in appropriate circumstances. SBUK received warnings that the number of SARs was surprisingly low but failed to take any adequate steps to ascertain the reasons for this and consequently failed to identify that staff were not submitting SARs in appropriate circumstances.

5.4. Principle 11 requires that a firm deal with the Authority in an open and cooperative way, and disclose to it appropriately anything relating to the firm of which the Authority would reasonably expect notice.

5.5. SBUK breached this requirement during the Secondary Relevant Period by failing to notify the Authority of a suspected fraud committed by one of its employees against one of its customers in a timely manner.

6. SANCTION

Financial Penalty – Breach of Principle 3

6.1. 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

6.2. 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.

6.3. The Authority has not identified any financial benefit that SBUK derived directly from its breach.

6.4. Step 1 is therefore £0.

Step 2: the seriousness of the breach

6.5. 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.

6.6. The Authority considers that the revenue generated by SBUK is indicative of the harm or potential harm caused by its breach. The Authority has therefore determined a figure based on a percentage of SBUK's relevant revenue. SBUK's relevant revenue is the revenue derived by SBUK during the Primary Relevant Period. The Authority considers SBUK's relevant revenue for this period to be £24,688,000.

6.7. 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%

6.8. 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 systemic weaknesses in the firm's AML procedures, management systems and internal controls. These systems and controls related to all of SBUK's business; and

(2) the breach created a significant risk that financial crime would be facilitated, occasioned or otherwise occur.

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

(1) the financial crime and AML systems and controls failings are systemic and significantly affect all business lines and all levels of management, from the board to branch management. In addition, during the course of the investigation, five separate instances of potential fraud were discovered in relation to one of SBUK's branches. Whilst the frauds were not directly a result of the AML systems and controls breach they did indicate poor systems and controls relating to the prevention of financial crime and are indicative of the culture of SBUK.

6.10. Taking all of these factors into account, the Authority considers the seriousness of the breach to be level 4 and the Step 2 figure is therefore 15% of total revenue, being £3,703,200.

Step 3: mitigating and aggravating factors

6.11. 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.

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

(1) following the 2010 Visit, the Authority notified SBUK of serious weaknesses in its AML systems and controls. SBUK was accordingly aware of the importance of implementing and maintaining robust AML systems and controls; and

(2) SBUK had access to considerable guidance on how to comply with regulatory requirements. The Authority has published guidance on the steps firms can take to reduce their financial crime risk and provided examples of good and bad practice since 2011. The Authority has also published a number of Final Notices against firms for AML weaknesses, including Habib Bank AG Zurich on 4 May 2012, Turkish Bank (UK) Limited on 26 July 2012 and EFG Private Bank Ltd on 28 March 2013. Since 1990, the JMLSG has published detailed written guidance on AML controls. During the Primary Relevant Period, the JMLSG provided guidance on compliance with the legal requirements of the ML Regulations, regulatory requirements in the Handbook and evolving practice within the financial services industry.

6.13. Having taken into account these aggravating and mitigating factors, the Authority considers that the Step 2 figure should be increased by 20%.

6.14. The Step 3 figure is therefore £4,443,840.

Step 4: adjustment for deterrence

6.15. Pursuant to DEPP 6.5A.4G, if the FCA 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.

6.16. The Authority considers that the Step 3 figure of £4,443,840 represents a sufficient deterrent to SBUK and others, and so has not increased the penalty at Step 4.

6.17. Step 4 is therefore £4,443,840.

Step 5: settlement discount

6.18. 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.

6.19. The Authority and SBUK reached agreement at stage 1 and so a 30% discount applies to the Step 4 figure.

6.20. The figure at Step 5 is therefore £3,110,688 which has been rounded down to £3,110,600.

Financial Penalty – Breach of Principle 11

6.21. The same five-step framework applies to determining the appropriate level of financial penalty for SBUK's breach of Principle 11.

Step 1: disgorgement

6.22. The Authority has not identified any financial benefit that SBUK derived directly from its Principle 11 breach.

6.23. Step 1 is therefore £0.

Step 2: the seriousness of the breach

6.24. In considering the approach to take regarding Principle 11, the Authority does not consider that revenue is an appropriate metric to provide an indication of the harm or potential harm caused by the breach. The Authority has not identified an alternative indicator of harm or potential harm appropriate to the breach and so, pursuant to DEPP 6.5A.2G(13), has determined the appropriate Step 2 amount by taking into account those factors which are relevant to an assessment of the level of seriousness of the breach.

6.25. The breach of Principle 11 (the Secondary Relevant Period) lasted from 27 March 2015 to 14 May 2015.

6.26. In assessing the seriousness level, the Authority takes into account the factors outlined at DEPP 6.5A.2G. DEPP 6.5A.2G (12) lists factors likely to be considered 'level 1, 2 or 3 factors'. Of these, the Authority considers the following factors to be relevant:

(1) little, or no profits were made or losses avoided as a result of the breach, either directly or indirectly; and

(2) the breach was committed negligently or inadvertently.

6.27. Taking these factors into account, the Authority considers the seriousness of the Principle 11 breach to be level 2 and the Step 2 figure to be £200,000.

Step 3: mitigating and aggravating factors

6.28. The Authority does not consider that any factors aggravate or mitigate the breach and, consequently, the Authority considers that the Step 2 figure should not be increased or decreased.

6.29. The Step 3 figure is therefore £200,000.

Step 4: adjustment for deterrence

6.30. The Authority considers that the Step 3 figure of £200,000 represents a sufficient deterrent to SBUK and others, and so has not increased the penalty at Step 4.

6.31. Step 4 is therefore £200,000.

Step 5: settlement discount

6.32. The Authority and SBUK reached agreement at stage 1 and so a 30% discount applies to the Step 4 figure.

6.33. The figure at Step 5 is therefore £140,000.

Restriction

6.34. The Authority's policy for imposing a suspension or restriction is set out in Chapter 6A of DEPP.

6.35. When determining whether a restriction is appropriate, the Authority is required to consider the full circumstances of the case. The Authority will impose a restriction where it believes that such action will be a more effective and persuasive deterrent than the imposition of a financial penalty alone. This is likely

to be the case where the Authority considers that direct and visible action in relation to a particular breach is necessary. DEPP 6A.2.3G specifies examples of circumstances where the Authority may consider it appropriate to impose a restriction.

6.36. The Authority considers the following factors are relevant:

(1) the Authority has previously taken action in respect of firms' failures to put in place adequate AML and financial crime systems and controls. Despite this, the Authority considers that industry standards require improvement, especially within smaller banks; and

(2) the misconduct appears to have been widespread across a number of individuals across a number of business areas, including SBUK's deposit taking business.

6.37. The Authority considers it appropriate to impose a restriction in relation to SBUK's regulated deposit taking activities. To ensure that the restriction does not impact upon current deposit account holders, the Authority considers it appropriate to restrict SBUK's activities by preventing it from accepting deposits from new customers only. Thus, SBUK will be restricted from accepting deposits from customers who do not hold a deposit account with SBUK on the date of a Final Notice.

6.38. Prior to the imposition of the restriction, SBUK had voluntarily decided not to accept deposits from new retail customers. Notwithstanding this decision, the Authority considers it appropriate to impose a restriction for the reasons outlined above.

6.39. When determining the length of the restriction that is appropriate for the breach concerned, and also the deterrent effect, the Authority will consider all the relevant circumstances of the case. DEPP 6A.3.2G sets out factors that may be relevant in determining the appropriate length of the restriction. The Authority considers that the following factors are particularly relevant in this case.

Deterrence (DEPP 6A.3.2G(1))

6.40. When determining the appropriate length of the restriction, the Authority has regard to the principal purpose for which it imposes sanctions, namely to promote high standards of regulatory and/or market conduct by deterring persons who have committed breaches from committing further breaches and helping to deter

other persons from committing similar breaches, as well as demonstrating generally the benefits of compliant business.

6.41. The Authority considers that the length of the restriction it proposes will deter other firms from committing similar breaches and demonstrate the benefits of compliant business.

The seriousness of the breach (DEPP 6A.3.2G(2))

6.42. When assessing the seriousness of the breach, the Authority takes into account various factors (which may include those listed in DEPP 6.5A.2G(6) to (9)) which reflect the impact and nature of the breach, and whether it was committed deliberately or recklessly.

6.43. When considering the seriousness of the breach, the Authority has taken into account the factors listed at paragraphs 6.8 and 6.9 above.

Aggravating and mitigating factors (DEPP 6A.3.2G(3))

6.44. The Authority will have regard to various factors (which may include those listed in DEPP 6.5A.3G(2)) which may aggravate or mitigate a breach.

6.45. The Authority considers that the factors outlined at paragraph 6.12 above aggravate the breach.

Impact of restriction on SBUK (DEPP 6A.3.2G(4))

6.46. When assessing the impact of the restriction on SBUK, the Authority has taken into account the following:

(1) any financial impact on SBUK from not being able to carry out the restricted activity;

(2) potential economic costs, for example, the payment of salaries to employees who will not work or will have reduced work during the period of restriction; and

(3) the effect on other areas of SBUK's business.

Impact of restriction on persons other than SBUK (DEPP 6A.3.2G(5))

6.47. When assessing the impact of the restriction on persons other than SBUK, the Authority considers the following to be relevant: the impact on new, potential

depositors who will not be able to use SBUK's deposit taking services for the period of the restriction.

6.48. Having taken the above into account, the Authority considers the appropriate length of the period of the restriction to be 240 days.

6.49. Having taken into account all the circumstances of the case, including the considerations set out at DEPP 6A.3.3G, the Authority does not consider it appropriate to delay the commencement of the period of restriction.

Settlement discount

6.50. SBUK agreed to settle at an early stage of the Authority's investigation. SBUK therefore qualified for a 30% (stage 1) discount to the length of the restriction under the Authority's executive settlement procedures, reducing the length of the restriction to 168 days.

Total penalty

6.51. The Authority has therefore imposes a total financial penalty of £3,250,600 on SBUK for breaching Principles 3 and 11.

6.52. The Authority also imposes a restriction in that, for a period of 168 days from the date of this Final Notice, in respect of its regulated activities only, SBUK shall not accept deposits from customers who do not hold a deposit account with SBUK at the date of this Final Notice.

7. PROCEDURAL MATTERS

Decision maker

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

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

Manner of and time for payment

7.4 The financial penalty must be paid in full by SBUK to the Authority by no later than 26 October 2016, 14 days from the date of this Final Notice.

If the financial penalty is not paid

7.5 If all or any of the financial penalty is outstanding on 27 October 2016, the Authority may recover the outstanding amount as a debt owed by SBUK and due to the Authority.

Publicity

7.6 Sections 391(4), 391(6) and 391(7) of the Act apply to the publication of information about the matter to which this notice relates. Under those provisions, the 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 SBUK or prejudicial to the interests of consumers or detrimental to the stability of the UK financial system.

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

Authority contacts

7.8 For more information concerning this matter generally, contact Kerralie Wallbridge (direct line: 020 7066 6548) of the Enforcement and Market Oversight Division of the Authority.

Anthony Monaghan

Project Sponsor

Financial Conduct Authority, Enforcement and Market Oversight Division

ANNEX A

RELEVANT STATUTORY AND REGULATORY PROVISIONS

1. RELEVANT STATUTORY PROVISIONS

1.1 Pursuant to sections 1B and 1D of the Act, one of the Authority's operational objectives is protecting and enhancing 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.

1.3 Pursuant to section 206A 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, for such period as it considers appropriate (not exceeding 12 months), such limitations or other restrictions in relation to the carrying on of a regulated activity by that person 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 Business ("Principles")

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.

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*."

2.4 Principle 11 provides:

"*A firm must deal with its regulators in an open and cooperative way, and must disclose to the appropriate regulator appropriately anything relating to the firm of which that regulator would reasonably expect notice.*"

2.5 During the Primary Relevant Period and the Secondary Relevant Period, the following rules applied:

Senior Management Arrangements, Systems and Controls ("SYSC")

2.6 SYSC 6.1.1R 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*."

2.7 SYSC 6.3.1R provides:

"*A firm must ensure the policies and procedures established under SYSC 6.1.1R 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*."

Supervision ("SUP")

2.8 SUP 15.3.17R provides:

"*A firm must notify the appropriate regulator immediately if one of the following events arises and the event is significant:*

(1) it becomes aware that an employee may have committed a fraud against one of its customers; or

(2) it becomes aware that a person, whether or not employed by it, may have committed a fraud against it; or

(3) it considers that any person, whether or not employed by it, is acting with intent to commit a fraud against it; or

(4) it identifies irregularities in its accounting or other records, whether or not there is evidence of fraud; or

(5) *it suspects that one of its employees may be guilty of serious misconduct concerning his honesty or integrity and which is connected with the firm's regulated activities or ancillary activities*."

2.9 SUP 15.3.18G provides:

"*In determining whether a matter is significant, a firm should have regard to:*

(1) the size of any monetary loss or potential monetary loss to itself or its customers (either in terms of a single incident or group of similar or related incidents);

(2) the risk of reputational loss to the firm; and

(3) whether the incident or a pattern of incidents reflects weaknesses in the firm's internal controls."

Decision Procedure and Penalties Manual ("DEPP")

2.10 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.

2.11 Chapter 6A of DEPP sets out the Authority's statement of policy with respect to the imposition of suspensions or restrictions, and the period for which those suspensions or restrictions are to have effect.

Enforcement Guide

2.12 The Enforcement Guide sets out the Authority's approach to taking disciplinary action. The Authority's approach to financial penalties and suspensions (including restrictions) is set out in Chapter 7 of the Enforcement Guide.

3. RELEVANT PROVISIONS OF THE MONEY LAUNDERING REGULATIONS 2007

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

3.2 Regulation 5 (Meaning of customer due diligence measures) of the ML Regulations defines "*customer due diligence measures*" as:

(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.

3.3 Regulation 7(1) to (3) (Application of customer due diligence measures) of the ML Regulations 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…

3.4 Regulation 8 (Ongoing monitoring) of the ML Regulations 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.

3.5 Regulation 14 (enhanced customer due diligence and ongoing monitoring) of the ML Regulations 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…

(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) an EU 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.

3.6 Regulation 20(1) and (2) (Policies and procedures) of the ML Regulations provides:

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

(a) customer due diligence measures and ongoing monitoring;

(b) reporting;

(c) record-keeping;

(d) internal control;

(e) risk assessment and management;

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

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

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

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

(i) complex or unusually large transactions;

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

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

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

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

(d) under which—

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

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

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