12 Endeavour Square
London
E20 1JN

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

FINAL NOTICE

To: **Santander UK Plc**

Reference Number: **106054**

Address: **2 Triton Square**
Regent's Place
London
NW1 3AN

Date: **8 December 2022**

1. ACTION

1.1 For the reasons given in this Final Notice, the Authority hereby imposes on Santander UK Plc ("Santander UK") a financial penalty of £107,793,300 pursuant to section 206 of the Act.

1.2 Santander UK agreed to resolve this matter and 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 £153,990,400 on Santander UK.

2. SUMMARY OF REASONS

2.1 The Authority has the operational objective of protecting and enhancing the integrity of the UK financial system. The laundering of money through UK financial institutions undermines the integrity of the UK financial system. The nature of their business means that banks are particularly susceptible to the risk of being used by their customers to facilitate the laundering of money. To mitigate this risk, a bank must take reasonable care to organise and control its affairs responsibly and effectively and to establish and maintain an effective risk-based anti-money laundering ("AML") control framework.

2.2 In particular, this involves ensuring that the bank has established the identity of its customers and, in respect of business customers, the nature of the customer's business and how it will use the bank's services. By establishing this accurately at the start of the relationship, the bank can assess the money laundering risks presented by the customer. Thereafter, the bank must monitor the activities of the customer, including monitoring transactions, to ensure that they remain consistent with the bank's understanding of its business and the associated money laundering risks. The extent and frequency of the monitoring in respect of each customer will depend on the particular risks presented by that customer. Where a bank identifies that a customer's activities are not consistent with the bank's understanding of its business, or that it may be engaged in suspicious activity, it must take prompt action to manage any money laundering risks this creates.

2.3 Maintaining an effective AML framework involves ensuring that the design of systems is informed by an assessment of the risks presented by particular operations or products, that the systems are robustly operated by appropriately resourced and trained staff and that the systems are capable of being overseen and monitored by senior managers, with clear lines of responsibility and accountability.

2.4 Santander UK is a large retail and commercial bank, providing a range of financial services. At the end of the Relevant Period, it had over 14 million customers, of which approximately 566,000 were in the Business Banking portfolio. "Business Banking customers" were business customers with an anticipated turnover of less than £250,000.

2.5 Having become aware in December 2012, at the start of the Relevant Period, of significant issues with its AML framework, Santander UK made various changes to

its AML operating model and processes for Business Banking during the Relevant Period. However, while these changes resulted in some improvements, continued weaknesses in its AML framework meant that Santander UK failed to manage adequately the money laundering risks presented by its Business Banking customers.

2.6 The failure to address these weaknesses in a sufficiently comprehensive and timely manner led to significant shortcomings in the operational AML controls applied to Business Banking customers and, in turn, to an unacceptable risk of money laundering by its Business Banking customers going undetected and unaddressed. As a result, throughout the Relevant Period, Santander UK failed to manage effectively the money laundering risks associated with its Business Banking portfolio.

2.7 At the start of the Relevant Period, Santander UK's processes did not provide for the effective ownership of the money laundering risk presented by its Business Banking portfolio. Various AML functions were divided between different teams, which operated in siloes and did not share information sufficiently, and some functions operated a centralised operational model which prioritised the completion of processes above qualitative assessments. As a result, its governance processes failed to ensure that its systems managed AML risks within Business Banking appropriately.

2.8 At an operational level, there were significant weaknesses in Santander UK's assessment and monitoring of its Business Banking customers. In particular, when establishing new customer relationships and opening bank accounts, Santander UK's processes failed to ensure that it obtained sufficient information to understand the nature of a customer's business. This had the effect that, where Santander UK did not obtain sufficient information, it was unable to assess accurately the money laundering risks presented by those Business Banking customers. Unless customers identified, and staff recorded, the business as one which Santander UK assessed as high risk, no verification was conducted to ensure that the customer in fact carried on that business. Santander UK subsequently identified many customers whose business had not been accurately recorded, meaning that Santander UK could not assess accurately the money laundering risks presented by those customers.

2.9 These weaknesses at onboarding were exacerbated by the absence of an effective framework within Business Banking for ongoing customer monitoring. From the

start of the Relevant Period to April 2015, customer risk assessments were not recorded on systems generally used by staff, meaning that they could not readily be taken into account by staff dealing with the customer nor updated where appropriate. This also impacted Santander UK's ability to produce accurate management information ("MI") on the risks within its Business Banking portfolio.

2.10 At the start of the Relevant Period, Business Banking customers were not subject to any periodic reviews, nor any other effective review process, to ensure that Santander UK's understanding of their businesses and money laundering risks remained up to date. While periodic reviews were introduced in 2016 for customers assessed to be high risk, those assessed to be standard or low risk continued to be exempted. Given the weaknesses in the original risk assessment process, this was a significant shortcoming since it meant that Santander UK had no assurance that the activities of its customers were consistent with its understanding of their businesses.

2.11 Santander UK's automated transaction monitoring system lacked sophistication and failed to take into account important information such as the anticipated turnover of a Business Banking customer and a planned upgrade, by integrating it with other systems, could not be achieved during the Relevant Period.

2.12 Transaction monitoring alerts were investigated by Santander UK's Suspicious Activity Reporting Unit ("SAR Unit"). All Business Banking alerts were treated as medium risk alerts, which meant that they were subject to a review to determine whether an internal report of suspicious activity should be raised. During the Relevant Period, the SAR Unit prioritised alerts categorised as high risk and was subject to significant resourcing pressure. Together, this meant that, while steps were taken by Santander UK to address this issue, there were, at times during the Relevant Period, significant delays in investigating medium risk alerts.

2.13 While SAR Unit investigators were able to record inconsistencies identified in customer information, and there were processes in place for the purposes of considering whether, in light of their investigation, a SAR should be submitted and an account should be referred for closure, until 2016, Santander UK's processes did not provide for the information the SAR Unit identified to be used in the ongoing monitoring of the customer, or a reassessment of the customer's risk rating.

2.14 Notwithstanding the various steps Santander UK took to improve its processes for implementing account closures during the Relevant Period, where Santander UK

decided that, as a result of the risks presented by a Business Banking customer, its accounts should be closed, its processes for implementing the closure were unclear and divided between a number of teams resulting, in some instances, in significant delays, during which time the accounts continued to be operational.

2.15 These failures resulted in Santander UK being unable adequately to identify, assess, monitor and manage its money laundering risk relating to its Business Banking customers. Although its processes improved throughout the Relevant Period, it did not adequately implement policies and procedures within Business Banking to comply with its obligation to counter the risk that the firm might be used to further financial crime.

2.16 The weaknesses in Santander UK's systems were exemplified by its treatment of Customer A, a Business Banking customer which operated a money service business ("MSB"), receiving and making payments on behalf of its own customers. MSBs may present enhanced money laundering risks to banks which require careful management. Santander UK was aware of these risks but as at 2013, senior managers believed that it provided services to only one MSB, which was incorrect, and had no appetite to take on any more. Any proposed account in respect of an MSB had to be referred to senior financial crime staff for approval.

2.17 Customer A opened an account with Santander UK in May 2013. It did so on the basis that it provided translation services with an estimated monthly account turnover of £5,000. Despite indications from the information obtained when opening the account that Customer A was involved in financial intermediation, Santander UK failed to verify the nature of its business and opened the account on the basis that it was a standard risk customer. As a result, no referral or enhanced checks were made and it was not subject to any periodic reviews.

2.18 From October 2013, large payments began to be made into and out of Customer A's account. A transaction monitoring alert was triggered in November 2013 because transactions on the account exceeded £1.5 million per month. This was not investigated until 3 March 2014, by which time approximately £26 million had passed through the account. On investigation, the SAR Unit identified that Customer A had misrepresented the true nature of its business and appeared to be operating an MSB. The SAR Unit suspected that funds had derived from criminal activity and recommended closure of the account. However, this recommendation was not actioned and the account continued to operate. A further investigation in September 2014, by which time over £86 million had passed through the account,

reached the same conclusion but no further action was taken to progress the closure and no steps were taken to enhance the monitoring of Customer A.

2.19 Another investigation in February 2015, as a result of an internal report of suspicious transactions, concluded that, while Customer A may have misrepresented the nature of its business, it may have done so to ensure that Santander UK opened the account and that the transactions were consistent with those of a legitimate MSB. No enhanced controls or monitoring were imposed but a recommendation to close the account was made because MSBs were outside Santander UK's risk appetite.

2.20 A decision to close Customer A's account was made in April 2015. However, as a result of confusion between the various teams involved, and despite a further internal report of suspicious activity and two transaction monitoring alerts, the closure was not actioned until September 2015. At that point, at the request of a law enforcement agency, Santander UK appropriately decided to keep the account open. However, despite, by that time, being aware of the risks associated with Customer A, Santander UK failed to ensure that it regularly reviewed the need to keep the account open, including following receipt in June 2016 of information that should have prompted it to confirm with the law enforcement agency the need to do so. After the Authority wrote to Santander UK about its treatment of Customer A in December 2016, it took steps to close the account. By the time it was closed, approximately £269 million had passed through it.

2.21 Santander UK has identified multiple customers who, at the time of onboarding, were not identified by the Bank as operating MSBs, but were identified as such during the course of the customer relationship. The Authority examined the cases of six such customers (Customers A to F) and identified failings in Santander UK's treatment of them for AML purposes. The combined funds which passed through these accounts during the Relevant Period amounted to approximately £298 million. Approximately £269 million of this was attributable to Customer A's account.

2.22 As a result of the Authority's request to review its treatment of Customer A, Santander UK identified end-to-end weaknesses in the AML control systems for Business Banking customers. The Authority's investigation of the underlying causes for the control failings in respect of Customers A to F confirms that during the Relevant Period there were significant and persistent gaps and deficiencies across Santander UK's AML control framework for Business Banking including in respect

of onboarding, monitoring, governance, closure of customer accounts, and provision of information to senior management to enable effective oversight. This created a significant risk that financial crime would be facilitated, occasioned or otherwise occur in relation to Business Banking customers.

2.23 As a result, the Authority considers that, in respect of its AML controls for Business Banking during the Relevant Period, Santander UK failed to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. In so doing, it breached Principle 3.

2.24 In mid-2017, Santander UK concluded that the changes and improvements to its AML systems made during the Relevant Period did not adequately address the underlying weaknesses and decided that more significant changes were needed, involving a wholesale restructuring of its processes and systems. Santander UK continues to undertake remedial and enhancement action and has committed very significant resources to improving its AML control framework. The Authority acknowledges the significant work undertaken to date and senior management's commitment to ensuring an effective and sustainable AML control framework is achieved.

2.25 The Authority therefore imposes on Santander UK a financial penalty of £107,793,300 pursuant to section 206 of the Act.

2.26 For the avoidance of doubt, no criticism is made of anyone except Santander UK in this Notice.

2.27 Santander UK has cooperated fully with the Authority throughout the course of its investigation.

3. DEFINITIONS

3.1 The definitions below are used in this Notice:

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

"AML" means anti-money laundering;

"the AML Governance Forum" (subsequently named the Financial Crime Governance Forum and later the Financial Crime Risk Control Forum) means the senior AML decision-making forum at Santander UK;

"the Authority" means the Financial Conduct Authority;

"BMLRO" means business money laundering reporting officer;

"Business Banking" means the portfolio of business customers, generally those with an anticipated turnover of £250,000 per annum or less, serviced by the Retail and Business Banking Division;

"CDD" means customer due diligence, the measures a firm must take to establish and verify the identity of its customers and the purpose and intended nature of the business relationship;

"Central AML Policy" means Santander UK's central AML policy;

"Central AML Standards" means Santander UK's central AML standards;

"Central UK Operations" means the separate subsidiary of the Santander Group to which Santander UK outsourced certain AML activities, as described in paragraph 4.26 below;

"the CET" means the Customer Escalation Team, a Santander UK department created in 2014 with the purpose of receiving referrals from the CRA System and reviewing customer accounts;

"the Court Order Unit" means the department at Santander UK responsible for receiving and actioning court orders and requests for information from authorities;

"the CRA System" means the customer risk assessment system used by Santander UK from April 2015;

"DEPP" means the Decision Procedure and Penalties Manual, part of the Handbook;

"DMLRO" means divisional money laundering reporting officer;

"EDD" means enhanced customer due diligence, the measures a firm must apply in certain circumstances, including where the customer presents a higher risk of money laundering;

"the FI Unit" means the Financial Intelligence Unit, a Santander UK department responsible for coordinating the closure of accounts;

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

"the JMLSG" means the Joint Money Laundering Steering Group, a private sector body made up of the leading UK trade associations in the financial services industry which provides guidance on the application of AML requirements;

"the JMLSG MSB Guidance" means the guidance for banks on the risks presented by MSBs, provided by the JMLSG in November 2013;

"LBM" means local business manager, Santander UK employees generally responsible for onboarding Business Banking customers;

"MI" means management information;

"the MLRs" means the Money Laundering Regulations 2007 and, as of 26 June 2017, the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017;

"MLRO" means money laundering reporting officer;

"MSB" means money service business, a business which exchanges currency, transmits money or cashes cheques for customers;

"the NCA" means the National Crime Agency;

"the OBE" means the Onboarding and Exits Forum, a Santander UK forum introduced in January 2015 to consider and decide upon the provision of services to high risk customers;

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

"the QRT" means the Quality Review Team, a department within Central UK Operations that reviewed onboarding documentation;

"the Relevant Period" means 31 December 2012 to 18 October 2017;

"the Retail and Business Banking Division" means the division of Santander UK which provided services to retail customers and to businesses with an anticipated turnover of less than £250,000 per annum;

"Santander UK" means Santander UK Plc (FRN 106054);

"the Santander Group" means the major, multi-national financial services group of companies, of which Santander UK is part;

"SAR" means suspicious activity report, a report which a firm is obliged to make to the NCA when it suspects that a person has engaged in money laundering;

"the SAR Unit" means the Suspicious Activity Reporting Unit, the department at Santander UK responsible for considering and dealing with internal reports of suspicious activity and transaction monitoring alerts;

"SIC" means standard industry code, a means of specifying the nature of a company's business by reference to a four digit code;

"SMEs" means small and medium-sized enterprises, a term widely-used to describe smaller businesses;

"SYSC" means the section of the Handbook entitled "Senior Management Arrangements, Systems and Controls"; and

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

4. FACTS AND MATTERS

Background

4.1 Santander UK is the UK operating subsidiary of a major, multi-national financial services group ("the Santander Group"). It is authorised to carry on a range of regulated activities, including deposit-taking. It began direct commercial activity in the UK in 2004 with the acquisition of Abbey National. It continued to grow through acquisitions, including of Bradford & Bingley and Alliance & Leicester in 2008 and 2009 respectively. These were combined and began trading as Santander UK in 2010.

4.2 As of December 2012, Santander UK had approximately 1,312 branches and employed over 25,000 staff. It provided a range of financial services, including mortgages, savings, bank accounts, credit cards, loans, investments and insurance, to over 20 million customers.

4.3 Santander UK's operations were conducted by separate divisions. Its provision of services to business customers depended on their turnover. Businesses with an anticipated turnover of over £250,000 per annum were serviced by Santander UK's Corporate Banking Division and assigned a relationship manager. Businesses with an anticipated turnover of under £250,000 per annum (sometimes referred to as small and medium-sized enterprises or "SMEs") were serviced by Santander UK's

Retail and Business Banking Division. This portfolio was generally referred to within Santander UK as "Business Banking".

4.4 During the Relevant Period, Santander UK's strategy was to increase its market share of SME banking. As a result, the Business Banking portfolio grew significantly over the Relevant Period. At the end of the Relevant Period, it numbered approximately 566,000 SME businesses. While Santander UK was unable to provide precise numbers for the start of the Relevant Period, information suggests that the portfolio grew by approximately 18% between 2012 and 2017. The net revenue generated to Santander UK from the portfolio increased from approximately £90 million in 2012 to £234 million in 2017.

Obligations of banks

4.5 All authorised firms are required by the Authority's rules to maintain adequate policies and procedures sufficient for countering the risk that the firm might be used to further financial crime, including money laundering. These must include systems and controls that enable it to identify, assess, monitor and manage money laundering risk and which are comprehensive and proportionate to the nature, scale and complexity of the firm's activities. A firm must allocate to a director or senior manager (who may also be the money laundering reporting officer ("MLRO")) overall responsibility within the firm for the establishment and maintenance of effective AML systems and controls. A firm must also appoint an MLRO who should act as the focal point for all activity within the firm relating to AML.

4.6 The nature of its business means that a bank is particularly susceptible to being used by its customers for the purposes of money laundering. As a result, the controls a bank puts in place to manage money laundering risk must be effectively designed, informed by assessments of the risks presented by particular business areas or products, robustly operated, with clear lines of responsibility, and subject to regular review. Senior managers should ensure that they have appropriate oversight of the effectiveness of the controls, including the provision of clear and useful MI which enables them to ensure that controls are working effectively and that risks are being mitigated appropriately. In addition, the MLRs impose specific AML obligations on all banks.

4.7 Best practice will usually involve a 'three lines of defence' model, with operational business areas forming the first line, by taking responsibility for managing and mitigating money laundering risk in their own areas; a risk or compliance oversight

function forming the second line by monitoring the compliance of business areas with policies and requirements; and a risk assurance function, frequently performed by an internal audit department, forming the third line by providing assurance of the effectiveness of controls.

Santander UK's AML Framework

4.8 Santander UK's Central AML Policy ("Central AML Policy") set the mandatory minimum AML requirements for the Bank and assigned responsibilities. Further detail to these requirements was contained in Santander UK's Central AML Standards ("Central AML Standards"). The Central AML Policy gave responsibility for managing money laundering risks and approving appropriately designed AML controls to members of the executive committee and their direct reports. The Central AML Standards provided that senior management of each business area was responsible for systems and controls within that business area, and that the MLRO was accountable to senior management for oversight of AML compliance across Santander UK. The Central AML Standards cross-referred to the AML Governance and Framework documents for further details of roles and responsibilities.

4.9 Each business division was responsible for managing its own AML risk and for formulating local processes and procedures to comply with the Central AML Policy. Each business division was assigned a Divisional MLRO ("DMLRO") and several more junior Business MLROs ("BMLRO") to provide AML support.

4.10 Santander UK maintained a central AML team headed by its MLRO within its Compliance Division. This was responsible for providing guidance on AML policy and assessing the robustness of controls in individual divisions. It also had ownership of certain key AML operations, such as the SAR Unit, which was responsible for considering internal reports of suspicious activity and transaction monitoring alerts, and the Court Order Unit, which was responsible for receiving and actioning court orders and liaising with authorities.

4.11 The most senior dedicated AML forum was the AML Governance Forum (subsequently the Financial Crime Governance Forum from August 2013 until October 2016 and then the Financial Crime Risk Control Forum until the end of the Relevant Period), formed of senior financial crime staff from across Santander UK, which met monthly. Until 2015, it was also involved in ratifying decisions made by

the Divisional Financial Crime Officer (formerly the DMLRO) to onboard and exit certain customers deemed to present high money laundering risks.

Issues with the Bank's AML framework

4.12 From at least 31 December 2012, when Santander UK's internal audit department issued a report on its AML governance and operating framework, Santander UK was aware that its AML control framework was insufficient and that significant improvements were required throughout, including with respect to its governance, setting of policies, risk assessments, customer data quality, the management of automated alerts and suspicious transactions.

4.13 A review conducted in August 2012 by senior financial crime staff, and provided to senior management in February 2013, found that: the central AML team lacked structure, resource and experience at a management level; there had been a lack of profile and engagement at a senior level, meaning that there had been limited reporting of AML risks at senior management forums; reporting lines within the central AML function were mixed between first and second lines, meaning that it had failed to provide appropriate second line oversight; and systems were complex and reliant on manual processes.

4.14 In April 2013, an external consultancy commissioned by Santander UK prepared an AML maturity and gap analysis report which found that, whilst some enhancements to the AML framework had been made, including evidence of greater escalation of AML issues to senior management, it was immature compared to peers in many areas. The report detailed gaps and identified, in particular, that the risk rating attributed to a customer at the time of onboarding did not determine the level of ongoing monitoring and that periodic reviews of customers were not conducted in all business areas.

4.15 Shortly thereafter, the Authority conducted a review of Santander UK's AML controls. Although a feedback letter of 30 September 2013 recognised that Santander UK had begun work to improve the effectiveness of its AML framework, it highlighted significant weaknesses, including: until May 2012, a lack of appropriate engagement by senior management on AML issues as well as failure to escalate certain issues; a high turnover of MLROs which contributed to a failure to take ownership for mitigating identified weaknesses until a review was conducted by the MLRO in late 2012; a historical lack of investment in IT systems; and a lack of a formal training strategy. The letter identified that Santander UK's risk

assessment of its standard and higher risk retail customers (which included its Business Banking customers) was significantly inadequate, was failing to consider multiple AML risk indicators at the onboarding stage and that Santander UK was consequently failing adequately to identify its higher risk customers, exposing it to unknown money laundering risk. The Authority expressed its expectation that a substantial programme of change was required, that senior management were expected to demonstrate that they were exerting strong influence to drive forward mitigation steps and that measures to ensure customers were properly risk assessed should be implemented with high priority.

4.16 Santander UK recognised and accepted the Authority's findings which were reflected in a two year Financial Crime Transformation Programme which Santander UK had commenced following its initial work with the external consultancy in April 2013. Between 2014 and 2016, Santander UK invested a significant amount into the Financial Crime Transformation Programme. This delivered certain changes and improvements to its financial crime systems and controls, including revised policies, delivering a target operating model for financial crime, prioritising business requirements and informing a major project to implement enhanced IT systems. Santander UK also prioritised tactical responses with the objective of addressing some of the Authority's immediate concerns and enhancing Santander UK's financial crime control environment.

4.17 However, although Santander UK invested substantial time, resource and expenditure to improve its AML systems, significant deficiencies continued to exist in Santander UK's AML control framework for Business Banking during the Relevant Period, which affected Santander UK's ability to mitigate the money laundering risks associated with its Business Banking portfolio.

Governance

Lack of first line ownership of risk

4.18 In an effective system, as the first line of defence, the operational business should take responsibility for managing and mitigating money laundering risk. At the beginning of the Relevant Period, Santander UK's systems did not provide for Business Banking adequately to accept this responsibility in relation to the money laundering risks associated with its Business Banking portfolio.

4.19 From the start of the Relevant Period until 2014, although the central AML team carried out an annual risk assessment, this was high-level and lacked

sophistication. No money laundering risk assessments were carried out by (among other areas) Business Banking, which should have been best placed to assess the particular risks of its operations.

4.20 In 2014, Santander UK engaged external consultants to assist with the preparation of risk assessments, after this had been identified by Santander UK as an issue in an Internal Audit report prepared in December 2012. From 2014, Business Banking was required to perform an annual risk assessment to identify key risks and document the effectiveness of key controls. The Business Banking risk assessment, completed in November 2014, identified that Business Banking senior managers:

4.20.1. were not receiving specific bespoke AML training;

4.20.2. had no AML responsibilities within their role descriptions or through relevant committees;

4.20.3. were not actively involved in developing or approving AML risk appetite;

4.20.4. had no involvement in the approval of AML policies and procedures;

4.20.5. did not receive AML related MI that was sufficiently informative or effective to enable them to make decisions; and

4.20.6. did not have effective involvement in managing AML risk.

4.21 Because they did not always assess money laundering risk in a systematic way, in some instances the Business Banking Division gave inadequate consideration to the particular risks presented by its operations and how they would best be mitigated.

4.22 Given the relative immaturity and lack of subject matter expertise in the first line function, some of the new teams created as part of the Financial Crime Transformation Programme were designed, built out and initially operated in the second line, moving across to the first line only in 2016. Santander UK adopted this approach in order to leverage the greater AML expertise of the second line staff in the formative stages of the new model. However, this impacted on their ability to perform their usual functions.

Structure and information flow

4.23 As described in more detail below, responsibility for Santander UK's AML controls was divided between a number of different teams, most with specific and limited responsibilities and with different reporting lines. In the earlier part of the Relevant

Period, these teams tended to work in siloes, each concentrating on the fulfilment of its own function, but with limited understanding of how this impacted on the wider picture.

4.24 Limitations in the information flow between teams meant that teams risked making decisions in the absence of important information and that managers had difficulty in assessing the overall position. On occasion, information presented to senior managers did not include all of the information necessary to give them the full picture.

4.25 At the beginning of the Relevant Period, divisional senior managers were not sufficiently involved in committees at which AML risks and issues were discussed and the information and MI being escalated were not adequate to give them sufficient visibility on money laundering risks.

4.26 Allied to this was the outsourcing of some financial crime functions to an operations company ("Central UK Operations") which was a separate subsidiary of the Santander Group. Santander UK was responsible for instructing and overseeing the activities it outsourced to this entity which included the Quality Review Team ("QRT"), responsible for quality reviewing the onboarding documentation for Retail and Business Banking customers and some customer and payment screening functions. It provided services pursuant to a contract with specified service level agreements including processing deadlines. This led to a centralised operational model, focussed more on meeting these deadlines than on qualitative assessments. Reporting to Santander UK senior managers was similarly focussed, meaning that senior managers were not sufficiently able to assess the effectiveness of the function in mitigating risk.

Improvements in governance

4.27 Santander UK made a series of changes to its AML control systems during the Relevant Period including the introduction of a target operating model across all three lines of defence that entailed new teams, processes and training, clarified roles and responsibilities, efforts by financial crime senior management to bring teams together, initiatives to improve the quality of MI available to management in relation to financial crime risks and the adoption of greater responsibility for managing money laundering risk in the first line business areas. These changes included the establishment of a centralised function for receiving information about customers, reviewing customer accounts and proposing recommendations on

retaining or exiting customers. However, effective change took time to implement and the target operating model was not fully embedded by the end of the Relevant Period.

4.28 In the meantime, as described below, weaknesses in AML systems led to significant failures at an operational level to identify and manage money laundering risk within Business Banking. These included failures to assess the money laundering risks associated with customers, to monitor customers appropriately and to take prompt action to mitigate risks once identified.

4.29 Many of these failures were exemplified by the case of Customer A, an MSB which was a Business Banking customer between May 2013 and March 2017. As described in more detail below, Santander UK failed to identify at the time of onboarding that Customer A operated an MSB and was consequently both a high risk customer and operating a business outside of Santander UK's risk appetite. Santander UK failed to monitor Customer A's activities appropriately and, despite having been alerted to suspicious transactional activity in November 2013, and having formed the suspicion that Customer A may have been laundering money in March 2014, Santander UK failed to take prompt and appropriate action to mitigate the risks involved in continuing to provide Customer A with banking services. The Authority has also identified failings in respect of five other customers which, during the course of its customer relationships, Santander UK subsequently identified as operating MSBs (described in this notice as Customers B to F).

4.30 After the Authority requested a review of Santander UK's treatment of Customer A in April 2017, Santander UK staff identified and alerted its senior management to "*end to end control weaknesses*" in its Business Banking AML controls. However, there was a lack of clarity within Santander UK at the time as to the extent to which the weaknesses had been addressed by then as part of steps taken by Santander UK to remediate its Business Banking controls.

Ongoing remedial steps taken by Santander UK

4.31 In mid-2017, Santander UK's Board and senior management determined that a wholesale restructuring of Santander UK's processes, technology and financial crime architecture was required. In particular, this involved ending the outsourcing of financial crime operations to Central UK Operations, creating a specific centralised function dedicated to financial crime and investing in training and in technology to address fragmented and aging systems. Santander UK launched a

project, the Realigned Financial Crime Transformation and Remediation Programme, with the support of external consultants, in August/September 2017.

4.32 The Authority recognises the scale and complexity of the transformation and remediation programme that Santander UK has undertaken, which has spanned multiple years and involved the commitment of substantial resources, including a material increase in financial crime headcount and expertise. This programme is designed to increase the effectiveness of Santander UK's financial crime control framework and significantly reduce Santander UK's overall exposure to financial crime. Santander UK continues to invest in its ongoing transformation and remediation programme.

Operational failures

Treatment of customers

4.33 A bank's treatment for AML purposes of each of its customers should depend upon an assessment of the money laundering risks the particular customer presents. When taking on a customer, a bank must establish the identity of the customer and the intended purpose of the business relationship, based on information obtained from the customer, and independently verified where appropriate (customer due diligence or "CDD"). In relation to a business customer, this includes ascertaining the nature of the customer's business and establishing how it will use the bank's services. Establishing this at the start of the relationship means that the bank can assess what money laundering risks may be presented by the customer and the extent of the necessary CDD and ongoing monitoring.

4.34 Where the bank assesses the relationship as presenting a higher risk of money laundering, it must apply, on a risk-sensitive basis, enhanced customer due diligence ("EDD") and enhanced ongoing monitoring.

4.35 Where a bank ascertains that a customer has misled the bank about the nature of its business, or identifies that the transactions conducted by the customer are not consistent with the bank's understanding of the customer's business, the bank should take prompt action to mitigate any resulting risks. This may involve refreshing its CDD (which the bank is required to do when it doubts the veracity of information provided as part of CDD or suspects money laundering), conducting EDD, or, if the bank considers that the risks cannot otherwise be appropriately mitigated, terminating the relationship. When a bank suspects that a customer may

be engaged in money laundering, it must submit a suspicious activity report ("SAR") to the National Crime Agency ("NCA").

Treatment of MSBs

4.36 Some customers may present significant money laundering risks to a bank. These are likely to include a firm which transmits money on behalf of its own clients, defined in the MLRs as a money service business or MSB. Because a bank will not generally have access to the MSB's client list, or the reasons for the underlying transactions, the bank is dependent on the MSB complying with its own financial crime obligations. A bank providing services to an MSB should ensure that it has assessed the money laundering risks involved, that it has taken steps to assure itself that the MSB maintains appropriate controls to manage its own money laundering risks and that it monitors the relationship sufficiently to ensure that its own understanding of the conduct of the MSB's business remains up to date.

4.37 In November 2013, the Joint Money Laundering Steering Group ("JMLSG") published detailed guidance for banks on the risks MSBs present as customers (the "JMLSG MSB Guidance"). The JMLSG MSB Guidance warned that features of the MSB sector make it an attractive vehicle for criminals to launder funds and that MSBs are vulnerable to use by criminals where the MSB unwittingly performs transactions for them or where they are owned by, or complicit with, a criminal organisation. It noted that if banks are to detect such cases, they must effectively apply CDD measures and monitor customers. Several possible red flags were set out. These included: the turnover of the MSB exceeding to a large extent the cash flows of other comparable businesses; suspicious connections of the MSB owner; and false information provided during the customer identification procedure.

4.38 Santander UK was aware of the enhanced risks presented by MSBs. The Central AML Standards assessed MSBs to present higher risks. In line with its risk appetite, Santander UK's policy was that it offered limited services to the MSB sector and did not enter into new MSB business. Where a business area within Santander UK decided to enter into a business relationship with an MSB as an exception, it was required to be referred to a BMLRO and further endorsed by the DMLRO. In July 2013, a discussion between senior managers revealed that they believed Santander UK had only one UK relationship with an MSB customer and had no appetite to take on any more due to the risks to Santander UK.

4.39 However, Santander UK had failed to identify that it was, in fact, providing services to multiple MSBs, including Customers A to F. This became apparent during the Relevant Period: emails in April 2014 show senior financial crime staff circulating a list of approximately 450 customers of Santander UK with active accounts as at October 2008 which had been inherited from the Alliance & Leicester book and which were suspected of operating as MSBs or MSB agents. This list was accompanied by a request to identify which of these accounts still remained active. Any live customers identified as MSBs or MSB agents underwent investigation and in total 85 were assessed by an internal forum as to whether Santander UK should continue to provide services to them. By January 2017, based on the application of broad search criteria, Santander UK had conducted a review which identified some 2,549 Business Banking customers as potential MSBs. A sample review of this customer population completed in November 2016 determined that the significant majority of customers within the sample population were not MSBs. However, these reviews suggest that even late in the Relevant Period, Santander UK was unable readily to identify its MSB customer population and therefore manage the money laundering risks associated with customers who were MSBs.

Risk Rating and CDD at Onboarding

4.40 Santander UK's Business Banking customers could open accounts through face-to-face meetings at local branches, by telephone or by internet. Where accounts were opened in branches, they were generally dealt with by a Local Business Manager ("LBM").

4.41 Although LBMs received annual on-line 'Fighting Financial Crime' training, this training was not specific to their role and did not train them to consider the plausibility of a business application at the point of onboarding. In September 2013, the Authority expressed concerns about the lack of targeted role-specific training, in particular to front-line staff. From mid-2014, Santander UK began to implement a strategy to move towards more role-specific training on AML-related issues for front-line staff, which included training on identifying and verifying a customer's nature of business (including external sources available for these purposes, such as Companies House checks). More formal role-specific training was introduced in 2017.

4.42 To open a business account, the customer had to fill in an application form and would generally meet with the LBM in person at the branch or deal with Santander UK's Business Banking Direct Telephony team. Among other details, the application

form requested the customer to state the nature of its business. Other requested details included whether the firm conducted MSB business, the anticipated turnover of the business over the next 12 months and the amount it anticipated paying into the account per month.

4.43 From the information provided by the customer, the LBM would complete an AML checklist. The LBM was required to enter certain details to ascertain the risk rating for the business. This included 'Business Location', 'Location of Individuals' and 'Transactional Location' (in which countries the business transacted). The responses to each of these generated a risk rating - either 'Standard', 'High' or 'Refer', the latter meaning that the LBM was required to refer the application to a BMLRO who would then seek authorisation from the DMLRO to proceed to onboard the customer. In addition, the LBM was required to enter '*full description of nature of business*' and to select from a list provided to the LBM by Santander UK a four digit code which most accurately described the business. This code was referred to as a Standard Industry Code ("SIC"). The list related each SIC to a risk rating, again either 'Standard', 'High' or 'Refer'.

4.44 Beyond selecting the appropriate SIC for the nature of the business, LBMs undertook no qualitative assessment of the money laundering risks that may be associated with the business of a particular customer and, unless the list assigned either a 'High' or 'Refer' risk rating to the SIC, the LBM was not directed to conduct any further verification of the nature of the customer's business.

4.45 In 2014, the AML checklist was replaced by a CDD checklist. This automatically applied the requisite risk rating to the SIC entered by the LBM. However, it continued to rely on the LBM entering the appropriate SIC and, unless the list assigned either a 'High' or 'Refer' risk rating to the SIC, it did not require the LBM to verify the nature of the customer's business.

4.46 Santander UK's processes provided for LBMs to obtain documentation from Companies House and from commercial corporate information providers in order to verify the ownership, trading address and, in respect of a 'High' or 'Refer' risk Business Banking customer, the nature of its business. Both Companies House and commercial providers generally listed a SIC for each company. The SICs used by Santander UK did not align with those used by Companies House or commercial providers, and therefore LBMs did not compare the SIC relating to the nature of business as provided by the customer with that listed at Companies House or by the commercial provider to ensure consistency. In September 2016, Santander UK

commenced a project to upgrade its structural systems to enable capture of 'UK SIC 2007' information for all customers in order to assist with aligning SICs applied by Santander UK with SICs held for customers on Companies House.

4.47 In 2017, in connection with the issues identified in respect of Customer A, Santander UK reviewed the accuracy of its SICs. Using a sample of 51,600 business customers, it found that, in respect of 38%, there was a mismatch between the SICs applied by Santander UK and those listed on Companies House. In response, certain specific actions were taken, including the contracting of a third party analytics company to assist with SIC remediation and upgrades.

4.48 Although the identification obtained for the controllers of the account was subject to a "four eye check" by another Santander UK employee within the branch, this was limited to ensuring that the identification documents had been appropriately seen and verified, rather than a holistic check of the application.

4.49 LBMs sent the completed application forms, CDD checklists and supporting documentation to the QRT, part of Central UK Operations, which checked the application for AML compliance. Santander UK's policy stated that 100% of Business Banking applications in branches would be subject to quality checking by QRT. However, in practice, this had been reduced to 25% by the start of the Relevant Period.

4.50 Reviewers in the QRT checked that the LBM had completed the AML checklist correctly, rather than assessing the quality and veracity of the information provided or conducting any independent verification. The QRT team received limited role-specific AML training during the Relevant Period, including guidance on the process that checkers were expected to follow to verify the business entity. Any issues that were identified with an application were raised manually by email with the LBM, with a warning that the account may be blocked in the absence of a response within a specified period. Save where a customer was assessed to be 'High' or 'Refer' risk, QRT reviewers were not trained to verify the nature of the applicant's business, nor to ensure that the LBM dealing with the application had done so.

4.51 The effect of the above was that, if a Business Banking customer seeking to open an account claimed to conduct business that, by reference to the applicable SIC, was given a 'Standard' risk rating, no verification that the customer in fact conducted that business was carried out and (unless the other categories on the

checklist assigned a higher risk rating) the customer was assessed as 'Standard' risk.

Impact of the onboarding issues

Customer A

4.52 Santander UK's treatment of Customer A illustrates many of the weaknesses that affected its Business Banking AML controls, including at the point of onboarding. Customer A operated a payments business which fell within the definition of an MSB. Customer A opened a business current account at a regional branch of Santander UK on 17 May 2013. The branch was in a town approximately 40 miles from the trading address of Customer A and the home address of its sole director, both of which were in a large city. The application form described the nature of its business as 'Translation service', its estimated annual turnover as £100,000 and its expected monthly deposits to its Santander UK account as £5,000. The part of the application form which asked if Customer A undertook MSB activity was crossed out.

4.53 The LBM who considered the application completed an AML checklist. They entered the Santander UK SIC for translation service which was 7485. This assigned the customer a 'Standard' risk rating. No verification of the nature of Customer A's business was sought or evidenced. No evidence was provided of any questions asked, or answers received, as to why Customer A should have wished to open an account at a branch 40 miles away from its business address.

4.54 The LBM obtained documentation from Companies House and from a commercial information provider. Both listed a SIC in relation to Customer A of 64999, defined (on Companies House) as "Financial intermediation not elsewhere classified" and (on the commercial provider) as "Other financial service activities except insurance and pension funding (not including security dealing on own account and factoring)". Customer A's website address was listed in the materials obtained: this incorporated the term "FX" (which commonly refers to trading in, or transmitting, foreign currencies), whilst an insurance document obtained as part of the onboarding material provided the nature of business as "Travel Agency". As Santander UK subsequently ascertained, Customer A's website made the nature of its business clear.

4.55 These discrepancies were either not identified or were left unchallenged by the LBM and the QRT reviewer. QRT marked the application as "compliant first time", despite the review form including an option to record "KYB Information missing/incorrect".

4.56 As a consequence of failing to identify these discrepancies or otherwise to verify the true nature of its business, Customer A was incorrectly onboarded as a standard risk customer, without any of the controls that should have applied to a higher risk business or an MSB.

4.57 In a subsequent 2017 review of its treatment of Customer A, Santander UK identified a lack of adequate training, a lack of understanding of the importance of the information provided and a lack of curiosity to understand the customer and the business as causes for it opening an account for Customer A without identifying the discrepancies in the application. Since the end of the Relevant Period Santander UK has enhanced its training and onboarding processes to require LBMs to identify and verify a customer's nature of business.

Other customers

4.58 Failures at onboarding were identified with Customer B, Customer C and Customer D, each of which was subsequently identified by Santander UK as operating an MSB. Each opened bank accounts with Santander UK in the middle of 2013. In each case there were discrepancies within the onboarding material that ought to have caused Santander UK to enquire further into the customer's stated nature of the business and either carry out further CDD/EDD or refuse to onboard the customer. As with Customer A, there were inconsistencies between SICs, the stated nature of the business and indications of MSB activity. In the case of Customer C, its expected annual turnover exceeded the threshold for Business Banking customers. However, there is no evidence to suggest that the inconsistencies were identified and followed up with the customer. Each was assigned a standard risk rating and the accounts opened without challenge.

Ongoing monitoring

4.59 Having established a business relationship with a customer, a bank must continue to monitor the customer's activities to ensure that they remain consistent with the bank's understanding of the nature of the customer's business and its use of the bank's services. This includes ensuring that the information obtained from the customer at onboarding, and the bank's consequent understanding of the activities of its customer, remain up to date. The appropriate intensity and frequency of the

monitoring of a particular customer will depend on the money laundering risks associated with the customer. Since these risks are inevitably informed by the bank's own assessment, it is important that the customer risk assessment process is robust.

4.60 Santander UK's policy required it to keep customer information up to date under a trigger event strategy or by periodic file reviews. However, trigger events were limited to requests by the customer for additional products or notifications by the customer of updated information and, at the start of the Relevant Period, the frequency of periodic reviews was not mandated.

4.61 Although each Business Banking customer was assigned to a particular LBM, whom it could contact when seeking a new product or service, given the large number of Business Banking customers, the LBM was not directed, nor necessarily expected, to maintain contact with the customer, nor to oversee its activities.

4.62 Santander UK managed its Business Banking customers using a computer system and front-line staff dealing with a customer would access its details using this system. This system did not display an obvious record of the customer's risk rating, meaning that it was not immediately visible to all staff dealing with the customer.

4.63 From the start of the Relevant Period to April 2015, Santander UK did not have a centralised database that held details of its customers' risk ratings. This meant that, during that period, while Santander UK could manually produce some information about the risk profile of its Business Banking customer base, its ability to produce MI was limited. Nor did it have a centralised customer escalation team with specific financial crime expertise to carry out qualitative reviews of customers' risk ratings following referrals.

4.64 In addition, at the start of the Relevant Period, Santander UK operated no process for conducting periodic reviews of Business Banking customers and no other process for ensuring that the risk rating assessed when the customer was onboarded remained appropriate. As a result, Business Banking customers were not subject to any systematic review process to ensure that Santander UK's understanding of their businesses, and of the associated money laundering risks, remained up to date.

4.65 Further, while trigger events may have led to Santander UK obtaining updated documentation (for example in relation to a change of address), they did not cause the customer risk assessment to be reviewed or refreshed. The risk assessment

was also not reviewed if Santander UK identified specific adverse information about the customer.

4.66 In September 2013, the Authority notified Santander UK of its findings that Santander UK's risk assessments of some standard and higher risk retail customers were significantly inadequate and that Santander UK was not adequately identifying its higher risk retail customers. Santander UK recognised and accepted the Authority's findings, many of which had already been identified by Santander UK.

4.67 To provide for on-going risk assessments of its customers, Santander UK introduced an automated customer risk assessment system ("the CRA System"). The CRA System carried out an automated assessment of the money laundering risk presented by a customer based on defined risk factors and scheduled a review of the customer, to be carried out by Santander UK staff, at prescribed intervals. In January 2015, Santander UK updated its central AML Standards to provide for periodic reviews of customers to be carried out on the basis of minimum frequencies of: High risk – every 12 months; Medium (standard) risk – every 36 months; and Low risk – no later than 60 months. Santander UK's highest risk customers were to be reviewed at earlier intervals or subject to enhanced monitoring.

4.68 A new function, the Customer Escalation Team ("CET") was created in 2014 and substantially embedded by Q4 2015, with the purpose of receiving referrals from the CRA System and business areas, to review customer accounts, to build and review EDD files, to propose recommendations on retaining or exiting customers and to refer those recommendations to another newly created function, the Onboarding and Exit Forum ("OBE") which considered whether higher risk customer relationships should be commenced and terminated.

4.69 The CRA System was initially due to begin operating in the first half of 2013. However, its introduction was delayed, and it did not begin operating until April 2015. It was first applied to new customers and extended, between May and July 2015, to existing Business Banking customers who had, at onboarding, been risk rated either 'Refer' or 'High risk'. The first periodic reviews of customers commenced in August 2016. Until that time, despite being aware that it was contrary to its own policies and its obligations under the MLRs, Santander UK conducted no periodic customer reviews, nor any other effective review process, even of its higher risk customers.

4.70 Moreover, despite being aware of the weaknesses in its systems for assessing the appropriate risks of Business Banking customers, in January 2015, and shortly before the introduction of the CRA System, Santander UK decided to exempt from the need to conduct periodic reviews all customers within the Retail and Business Banking Division which were risk rated 'Medium' or 'Low' risk.

4.71 The exemption has been described by Santander UK as a "*policy-level carve out*". It appears to have been driven by the fact that Santander UK did not have the resources (either manual or automated) to carry out the reviews at the time, as opposed to the view that its other monitoring controls were sufficiently robust to dispense with them. An internal document explained that the risk assessment of Santander UK's existing customer base had been "*de scoped due to the costs involved and the fact that over the next few years it is likely that most customers will have made a change to their profile, and therefore risk assessed by* [the CRA System]." The exemption remained in place at the end of the Relevant Period.

4.72 The exemption was subject to the proviso that at appropriate trigger events the risk rating and customer information for existing medium and low risk customers would be reviewed for accuracy. However, the non-exhaustive list of trigger events that would prompt the CRA System to re-score an existing customer's risk rating included events such as the customer changing an aspect of their profile or requesting additional products but did not include changes in customer turnover, transaction monitoring alerts or, necessarily, the identification of adverse information about the customer.

4.73 In August 2016, Santander UK identified that only 36% of its customers had been risk rated by the CRA System and determined that more proactive steps should be taken to run all existing customers through a simulated version of the CRA System to identify previously undetected high-risk customers. This exercise identified a further 1,149 non-personal customers in the Retail and Business Banking Division who were assessed to be high-risk. A rectification exercise was undertaken to remediate these customers, namely to build EDD files and make recommendations on exit where appropriate. The rectification exercise was largely completed in mid-2017.

4.74 A further project, designed to identify potential MSBs or other customers presenting higher financial crime risks, was implemented in 2017. The initial triage identified 141 potential customers in the Business Banking portfolio with characteristics that could be consistent with higher financial crime risks.

4.75 By the time investigations were complete, 39 of these accounts had already been closed or were in the process of being closed and referrals were made to consider ending the relationship in respect of 48 further customers. Even where no financial crime risks were, in the event, identified, staff reported that their enquiries were hindered by a lack of available documentation on the customers. Santander UK established that 78% of these customers had been onboarded in the period 2013 to 2017, demonstrating that weaknesses with the onboarding process continued throughout this time.

4.76 In August 2017, Santander UK recognised that it still did not hold accurate information concerning its Business Banking customers' nature of business and part of the Realigned Financial Crime Transformation and Remediation Programme subsequently involved a full back-book remediation of all customer files.

Transaction monitoring

4.77 In addition to ensuring that its understanding of its customers remains up to date, a bank must maintain systems which allow it to scrutinise transactions and identify potentially suspicious transactions. In the absence of any effective process for conducting ongoing reviews of customers, it was all the more important that Santander UK's process for monitoring transactions, and identifying potentially suspicious activity, was effective.

4.78 A monitoring system may be manual or automated but for firms where there are significant issues of volume, a more sophisticated automated system may be necessary. The greater the volume of transactions, the less easy it will be for a firm to monitor them without the aid of some form of automation.

4.79 Santander UK operated an automated system which primarily assessed transactions against specified "rules", a breach of which automatically triggered an alert on the basis that it may have constituted unusual activity which, in turn, might have denoted suspicious activity.

4.80 At the start of the Relevant Period, Santander UK's automated transaction monitoring system lacked sophistication. The system operated on fixed rules, although it also contained some scenarios. Key customer data relating to expected turnover, occupation and nature of business that should have fed into the system, did not. As a result, although the system utilised scenarios to assess whether activity on the account was unusual for a Business Banking customer, it was not

designed to take account of a particular customer's anticipated turnover as provided at the time of onboarding.

4.81 Santander UK appreciated that the effectiveness of the system depended on the parameters of the scenarios which generated the alerts and the ability of staff to assess the alerts and act as appropriate. Early in the Relevant Period, there was a lack of clarity in Santander UK's policy documents regarding responsibility for oversight and sign off of the parameters and as of late 2014, the parameters had not been reviewed for over 12 months. From late 2014, regular reviews were performed of the rules and scenarios used by the system. Although certain checks were performed in respect of alerts, in the early part of the Relevant Period, there was no risk-based sample testing of the system and Santander UK was unable to identify any holistic review of the system having taken place between 2012 and 2017.

4.82 Santander UK planned to upgrade the transaction monitoring system by integrating it with the CRA System. However, this proved technologically complex and integration was not achievable. As a result, Santander UK continued to use the old system throughout the Relevant Period, relying on temporary incremental fixes.

4.83 Until 2016, the system automatically categorised alerts as either medium risk or high risk. The categorisation of an alert as either medium risk or high risk determined the timescales within which it was to be reviewed. Alerts categorised as high risk were those of a type which had previously demonstrated high conversion rates to the submission of a SAR. As alerts relating to Business Banking customers did not fall into this category, they were automatically categorised as medium risk. Neither the nature of the customer's business, nor the risk rating assigned to the customer at the time of account opening, affected the categorisation of the transaction monitoring alert.

The SAR Unit

4.84 Where a transaction triggered a transaction monitoring alert, an automated message was sent to the SAR Unit, part of the central AML team, that investigated internal reports of suspicious activity and transaction monitoring alerts and determined the appropriate course of action. Generally, this involved determining whether the activity provided grounds to suspect money laundering or terrorist financing and therefore whether a SAR needed to be submitted to the NCA. SAR

Unit investigators worked to a service level agreement which required them to investigate and determine internal reports of suspicious activity within 30 days.

4.85 High risk transaction monitoring alerts were considered and investigated in the same way as internal reports of suspicious activity, without prior investigation by a transaction monitoring alert specialist. In contrast, medium risk transaction alerts were subject to an initial review to assess the activity that had triggered the alert. Following this initial review, a decision would be taken either to close the alert or to treat it in the same way as a report of suspicious activity. Since all alerts in respect of Business Banking customers were categorised as medium risk, this process applied to all transaction monitoring alerts in respect of Business Banking customers.

4.86 At the start of the Relevant Period, the SAR Unit was subject to significant resourcing pressure and, as a result, prioritised transaction monitoring alerts deemed to be high risk: in December 2012, there was a backlog of 6,464 medium risk alerts, the oldest of which was 161 days, meaning that activity identified as being unusual had not been considered for over five months.

4.87 The heavy workload in the SAR Unit and the pressure of keeping within the service level agreement created a risk that investigations would be rushed and lack sufficient detail, although quality control checks involving sampling and feedback were in place to seek to guard against this risk.

4.88 Further resource was allocated to the SAR Unit and the backlog of transaction monitoring alerts was resolved by August 2014, including through recruitment, training and monitoring of the backlog by management. However, resourcing remained an issue for parts of the Relevant Period. In or around 2016, two teams that were dedicated to considering transaction monitoring alerts were established, staffed by increased numbers of investigators. However, in July 2017, transaction monitoring alerts and internal reports of suspicious activity were still on occasions not being reviewed within the agreed time period under the service level agreement and the function remained under-resourced.

4.89 SAR Unit staff received training on investigating and submitting SARs. The majority of SAR Unit staff had qualifications in AML awarded by a recognised external provider, which included coverage of the MLRs. However, they did not receive role-specific training in relation to Santander UK's duties under the MLRs. Santander UK's processes did not provide for investigators to contribute to the ongoing

monitoring of the customer by, for example, considering whether, in light of the information they ascertained, the customer's risk rating should be amended. Although routes of escalation were available, until February 2016, there was no embedded process for the SAR Unit to refer a customer for an event driven review of the customer's CDD. Prior to the implementation of the CRA System, the risk rating assigned to a customer during onboarding was not consistently considered as part of an investigation by the SAR Unit.

4.90 This exacerbated the weaknesses in Santander UK's assessment of a Business Banking customer's risk at onboarding since it meant that, where Santander UK became aware of information which should have led to a reassessment of the original risk rating, and thus the arrangements for ongoing monitoring of the customer, there was no process for ensuring that such reassessment took place.

4.91 Certain senior managers within Santander UK's financial crime functions acknowledged that this was symptomatic of financial crime teams working in silos, with inadequate communication and sharing of information. As noted above, changes were made during the Relevant Period with a view to addressing this issue, including the creation of the CET and the OBE, as well as changes being made to the SAR Unit processes.

The SAR Unit's approach to MSBs

4.92 Despite the JMLSG MSB Guidance referred to above, prior to December 2015, the only written guidance provided to SAR Unit investigators on the risks associated with MSBs was a guidance note dating back to 2010 which focused on Hawala money transfers.

4.93 This led to a lack of clarity on how SAR Unit investigators should treat customers identified as operating an MSB, particularly where the customer held appropriate regulatory permissions. Despite the Central AML Policy stating that the regulatory status of an MSB should not be used as an indication of the money laundering risks associated with it, in October 2015, SAR Unit managers identified that investigators may recently have been closing cases on the basis that, as the customer held regulatory permissions, there were not necessarily suspicions of money laundering. To address this, in December 2015, the SAR Unit managers distributed a note among SAR Unit staff, providing guidance on suspicious activity indicators in respect of MSBs.

4.94 By February 2016, the SAR Unit embedded a process to refer customers to the CET if they fell within one of four specified categories (including those suspected of operating an MSB) but the SAR Unit was not instructed to consider risks more generally when determining whether to refer a customer to the CET. In May 2017, further guidance, including an expansion of the circumstances in which SAR Unit investigators should refer customers was provided. In conjunction with this, enhanced training was also provided to the transaction monitoring team regarding MSB indicators.

4.95 Procedures did exist for SAR Unit investigators to recommend the closure of accounts, including where customers were believed to fall into a "Prohibited" category, where customers were deemed to be "repeat offenders" or where there were grounds to know or suspect that the customer was under investigation for money laundering. "Repeat offenders" were deemed to be those in respect of whom three SARs had been submitted in respect of similar activity during a period of three months or more. The process did, however, provide for a recommendation to be made in other circumstances based on the judgement of the investigator. From October 2015, the Account Closure Process expressly provided for an account closure recommendation to be based on a single reportable SAR.

4.96 Once an investigator decided to make a recommendation to close an account, the processes for effecting the closure were reliant upon emails being sent between the investigator, their manager, senior financial crime staff and a separate team that actioned the closure. There was no formal feedback process or system to ensure that recommendations to close accounts were sent to the relevant team or actioned thereafter.

4.97 This manual process exposed Santander UK to the risk that the recommendation would not be made, or progressed to a decision, due to human error. This risk was compounded by the resourcing challenges faced by the SAR Unit team. Whilst system capabilities to track account closures were utilised from 2015 onwards, a fully automated tracking process for account closures was not implemented within the Relevant Period.

Impact of the monitoring issues on specific customers

Customer A

Ineffective ongoing monitoring processes

4.98 Santander UK's monitoring of Customer A illustrates the weaknesses in its ongoing monitoring processes. Following Customer A's onboarding in May 2013, its account operated as expected for approximately five months, with relatively small transactions being made. However, from mid-October 2013, large payments into the account began to be made, frequently followed by large payments out.

4.99 Because Customer A had been onboarded as a 'Standard' risk customer, it was not subject to periodic review and, notwithstanding the matters outlined below, it had still not been risk assessed by the CRA System by December 2016.

4.100 In November 2013, a transaction monitoring alert was triggered in respect of Customer A following transactions on the account exceeding £1.5 million in a month. As this alert was a Business Banking alert, it was categorised as medium risk. Due to the backlog that existed at the time, it was not investigated by the SAR Unit until almost four months later in March 2014. The SAR Unit investigator considered the alert which, as they were expected to do, included manually accessing information regarding anticipated turnover. From their investigation, the SAR Unit investigator identified that:

4.100.1. turnover on the account vastly exceeded the expected turnover;

4.100.2. over £10 million had been credited to the account in 2013 and over £18 million in 2014;

4.100.3. most of the credits originated from a large cash management company;

4.100.4. funds were rapidly transferred out of the account, typically to companies involved in the financial sector, including foreign exchanges;

4.100.5. while Customer A had claimed its business to be translation services, its website clearly stated that it specialised in foreign currencies;

4.100.6. a website listing company information showed Customer A to be involved in financial intermediation;

4.100.7. media suggested that a person associated with Customer A had been involved in a money laundering investigation; and

4.100.8. the investigator suspected that funds had derived from criminal activity.

4.101 The investigator decided to recommend closure of Customer A's account. However, Santander UK has identified no evidence that this recommendation was progressed, and has also not identified any documented rationale for this. The Authority considers that this was overlooked due to human error and the lack of any formal process to ensure that account closure recommendations were completed. As a result, the closure was not actioned.

4.102 Further, because there was no embedded process to do so at the time, Customer A's account was not referred for a review of the operation of the account, the information provided to Santander UK at the time of onboarding, or of Customer A's risk rating.

4.103 As a result, Customer A continued to be assessed as a standard risk relationship with no further controls or monitoring applied. Thereafter, although transactions on Customer A's account exceeded £1.5 million in each of the intervening months, no transaction monitoring alerts were triggered until September 2014. In respect of December 2013, this was likely to have been the result of a rule designed to prevent multiple alerts being triggered on an account by the same rule or scenario within a given time period. However, this rule should not have prevented a further alert from being triggered under the same rule after 1 January 2014. It is unclear to Santander UK why transaction monitoring alerts were not triggered in the months January to August 2014.

4.104 In September 2014, a second transaction monitoring alert was triggered on Customer A's account. Despite the information ascertained from the previous alert, this was automatically categorised as a medium risk alert. A SAR Unit investigator considered the alert a month later. The investigator noted the findings of the first SAR Unit investigation, identified that over £76 million had been credited to the account in 2014, mostly from the same large cash management company, and recorded that it was believed that Customer A was a foreign currency provider which had deliberately concealed the true nature of its business. The investigator noted their suspicion that funds were being laundered through the account.

4.105 Although seven months had passed since the first investigation, no checks were made by the SAR Unit to determine whether the account closure recommendation

resulting from the previous investigation had been progressed. It was incorrectly assumed that the account closure process was underway. Therefore, no further account closure recommendation was made, the account was not referred for any further review within Santander UK and no additional controls were applied to it.

4.106 Four months later, on 18 February 2015, an internal report of suspicious activity was submitted to the SAR Unit in respect of Customer A, requesting consent to make three large transfers out of the account following a credit to the account from the same large cash management company to the value of £396,740. The report noted that the nature of the customer's business was secretarial and translation activities, showing that Santander UK had failed to update its customer records despite the two previous SAR Unit investigations.

4.107 Despite being aware of the two previous occasions on which the SAR Unit had determined that there were grounds for suspecting money laundering, on this occasion, the SAR Unit decided to permit the transfers to be made on the basis that the activity on the account was consistent with Customer A offering legitimate foreign exchange and money transmission services. The investigator noted that Customer A was authorised by the Authority to provide payment services. Although the investigator appreciated that Customer A had provided false information as to the nature of its business at the time of onboarding, they "*suspected*" that this was done not with the intention of using the account illegitimately but to ensure that the account was opened, since Santander UK did not accept business of that type.

4.108 The adverse media previously identified in November 2013 was discounted due to the fact that it dated back to 2006 and that the money laundering investigation could have been in respect of one of Customer A's clients, rather than the MSB itself. However, due to certain security settings, the document, which was freely available on the internet and set out the full nature of the adverse media, could not be accessed by the particular investigator. The Authority considers that this was not an isolated incident and impacted other investigators, although it notes that it was open to the investigators to request a change to their security settings.

4.109 A member of another financial crime team later accessed the full adverse media document, drawing the SAR Unit's attention to its contents and querying the findings. Further, the team noted that Customer A's "*activities…seem to be very high in terms of volume of transactions, particularly as the business doesn't seem to have any widely available online presence*" and noted that "*organised crime*

usually requires moving large amounts of money (which a money transmission company can allow)".

4.110 However, although these questions were raised, they did not lead to any reappraisal of Customer A at that point and the transactions were deemed not to be suspicious. Despite this finding, on the basis that Customer A was apparently operating an MSB, which was outside Santander UK's risk appetite, the SAR Unit decided to refer Customer A with a view to closure of its account.

Other customers

4.111 Certain issues also affected Santander UK's ongoing monitoring of other customers subsequently identified as MSBs.

4.112 Customer B opened an account in June 2013 on the basis that it was a translations business with estimated monthly deposits of £15,000. However, actual volumes passing through the account were, on occasions, significantly more than estimated. In October 2013 alone, £145,000 was deposited, approximately ten times the expected amount. The majority of the deposits were in cash and there were numerous transactions to other MSBs, including Customer A. However, no transaction monitoring alerts triggered on the account over the four and a half years it was open.

4.113 In November 2015, Santander UK received information that a company with a similar name to Customer B was suspected of operating an MSB and of being involved in money laundering. A review of the account identified that activity on the account was inconsistent with the stated business and that Customer B's website advertised MSB services. Santander UK identified reasonable grounds for suspecting money laundering. Despite these concerns, there is no evidence that Customer B was referred for an event driven review, EDD, enhanced monitoring or closure.

4.114 Changes in Customer B's details caused its risk rating to be automatically assessed by the CRA System in both February 2016 and February 2017. On both occasions, it was assessed to be "medium" risk, despite Santander UK having established by that time that Customer B appeared to be operating an MSB (and should thus, according to Santander UK's policies, have been deemed to be a high risk customer) and having formed suspicions that it was engaged in money laundering.

4.115 Santander UK received further information suggesting that Customer B may have been involved in criminality in March 2016 and August 2016. However, it continued to allow its account to be operated until April 2017 and it was not until July 2017 that the SAR Unit decided to recommend closure of the account.

4.116 Customer C opened an account in May 2013 on the basis that it was a property lettings business. In September 2013, the account opener was suspended due to concerns about their conduct when opening certain accounts. By February 2014, Santander UK had concluded that misconduct had occurred, including in relation to the onboarding of Customer C, which had been identified as an MSB. Despite this, there is no evidence that Customer C's account was subjected to an event driven review, CDD refresh, EDD, enhanced monitoring or a referral for closure.

4.117 Despite unusual transactional activity on the account, which included third party deposits from multiple individuals and other MSBs, numbering over 1,100 in 2014 and over 2,500 in 2015, and deposits exceeding those disclosed at account opening, the first of three automated transaction monitoring alerts did not trigger for over a year, until 27 June 2014.

4.118 Despite having identified by that time that Customer C was an MSB, the first evidence of any steps taken to review or close the account was in August 2015.

4.119 Customer D was onboarded in July 2013 as a software publishing business, with estimated annual deposits of £250,000. By the end of 2013, turnover was in excess of £1 million. In 2014 it exceeded £4 million. Although a manual payment alert was triggered in June 2015, the transaction monitoring system did not trigger automated alerts until October 2015. Nor is there evidence of the account being subjected to an event driven review, CDD refresh, EDD or enhanced monitoring.

4.120 In June 2015, Santander UK identified that Customer D was registered as a Small Payments Institution and in July 2015, Santander UK made the decision to close Customer D's account. However, in October 2015, an automated transaction monitoring alert triggered after faster payments out of the account exceeded £250,000 in a month, illustrating that three months later the account remained open with high volumes of funds continuing to flow through it.

4.121 Customer E was onboarded in September 2012 on the basis that it conducted management activities for holding companies, with estimated annual turnover of £250,000. In the remaining 3 months of 2012, the account showed a credit turnover of £1.4 million, almost 6 times expected turnover for the year. There was

credit turnover of £4.9 million in 2013, £4 million in 2014 and £4.5 million in 2015. However, no transaction monitoring alerts triggered on the account over the 3 years it was open.

4.122 In November 2013, the account opener was dismissed due to concerns about their conduct when opening certain accounts. However, until August 2015, there is no evidence that, as a result, the account was subjected to an event driven review, CDD refresh, EDD, enhanced monitoring or a referral for closure. Customer E's standard AML risk rating does not appear to have been reviewed until the introduction of the CRA System. This re-scored the customer as "low" risk in July 2015 and "medium" risk in September 2015.

4.123 In August 2015, Santander UK reviewed Customer E's account and suspected that it was functioning as an unauthorised MSB run from the account owner's home. In September 2015, discussions took place regarding potential account closure and in October 2015, Santander UK decided to close Customer E's account.

4.124 Customer F had been onboarded in February 2011 as a cargo handling company with estimated annual deposits of £45,000. Over the 4-year period the account was open, it received a credit turnover of over £428,000, including multiple third-party cash deposits. However, no transaction monitoring alerts triggered on the account and, despite identifying in March 2012 that Customer F's website offered money transfer services and shipping to a country that would have been designated as high risk under the Central AML Policy, Santander UK does not appear to have reviewed Customer F's standard AML risk rating, with Customer F having been exited prior to the introduction of the CRA System.

Account closure processes

4.125 At the start of the Relevant Period, Santander UK's AML Governance Forum was the senior decision-making forum required to ratify any decision to approve (as an exception) or decline a high-risk customer relationship. In practice, however, decisions about taking on or exiting certain high-risk customers were being taken by DMLROs because discussions at the AML Governance Forum had become too lengthy.

4.126 In June 2014, there was confusion among Santander UK staff as to who could close customer accounts. It was not clear to staff to whom authority had been delegated for the purpose of agreeing the closure of accounts. Any central MI required on account closures at this point in time would have to be compiled manually by

reviewing individual customer records, although certain teams within Santander UK began to operate their own trackers from January 2015.

4.127 As of July 2014, discussions remained ongoing as to the process for account closures. By 2014, senior financial crime staff had recognised that there needed to be development of the governance structure and exit committee, and work was already ongoing at that point to put this structure in place. In the meantime, closure recommendations from various teams within Santander UK were building up. Prior to 2015, there was no workflow management tool to assist with tracking closures.

4.128 In January 2015, the OBE was introduced. It replaced the AML Governance Forum's decision-making function on whether to onboard and exit high risk customer relationships taking account of the customer's profile, including its financial crime risk.

4.129 Where the OBE decided to close an account, the closure and exit process was to be carried out by Central UK Operations and coordinated by a newly created Financial Intelligence Unit ("FI Unit"). The FI Unit's responsibilities included:

4.129.1. communicating the OBE decision to the relevant central financial crime function and business area;

4.129.2. ensuring that the operational steps necessary to effect a closure / exit were taken in a timely manner (to commence within five working days of the decision);

4.129.3. tracking the progress of closures and maintaining appropriate exit MI; and

4.129.4. retaining comprehensive records regarding account closures and exits for financial crime reasons.

4.130 The FI Unit was also responsible for considering whether information received from law enforcement agencies should be distributed to the SAR Unit, and for taking ownership of higher risk customers where there was liaison with law enforcement.

4.131 Although Santander UK's policies allocated responsibility for certain actions to the FI Unit as of January 2015, in fact the team was being built out at that time, meaning that other teams had to carry out its actions.

4.132 In March 2015, Santander UK decided that exit decisions based on financial crime concerns could, where reasonable, be taken by the SAR Unit. Any complex or particularly high risk cases could, however, still be referred to the OBE. Before the FI Unit was set up in 2016, where a closure recommendation was made by a SAR Unit investigator, they were expected to liaise with Central UK Operations, who would process the closure, and to track the closure to completion.

4.133 A review by Santander UK in August 2015 concluded that the OBE was not at the time functioning effectively in managing the take on and ongoing management of high risk customer relationships. In particular:

4.133.1. its structure, membership and accountabilities were not clearly defined;

4.133.2. because its minutes were not being approved in a timely manner, delays were caused to business areas completing necessary actions;

4.133.3. some actions being requested were not being carried out, usually because business areas were not aware of how to action the OBE's requirements; and

4.133.4. no mechanism was in place for the OBE to track requested actions to conclusion.

4.134 In October 2015, a review of cases brought to the OBE between April and August 2015 identified 24 instances of accounts which the OBE had decided should be closed but which had not been actioned appropriately and which remained open. This included six customers which were suspected of operating MSBs (including Customer A, as to which see below) and which had misrepresented the nature of their business. In respect of three customers, the OBE had determined that there were financial crime concerns and that consent was required from the NCA before funds were returned to the customers.

4.135 Santander UK subsequently identified that the OBE was experiencing some operational issues which included capacity and resourcing constraints. Improvements to the OBE's processes were made, by 2017, including through amendments to the March 2017 AML Standards and the introduction of a workflow tool. However, there remained some problems: the efficiency of meetings was poor, sometimes lasting 3 to 4 hours; reading packs would be sent out late with insufficient time for participants to consider them and often contained basic mistakes and poor narratives. Decisions would therefore frequently be deferred

pending the gathering of further information. For example, if 20 cases were tabled for decision, only 5 might be considered in the meeting, and an exit decision made only on one of these. An internal review of the OBE conducted by Santander UK in January 2017 noted that whilst, the OBE itself provided an effective means of assessing high risk customers, the documentation of decisions and supporting procedures should be improved.

4.136 Despite the FI Unit's responsibility to maintain records of account closures, it appears that no central record was ever created during the Relevant Period. Whilst some of the prescribed information was retrievable from other systems, obtaining it was a manual and resource intensive exercise. During 2015, the OBE and SAR Unit began to operate their own account closure trackers.

Impact of the account closure process issues on specific customers

Customer A

4.137 On 19 February 2015, the SAR Unit decided to refer Customer A for consideration of closure. However, although the CET had been created by July 2014, it was still being developed and built out, was not fully resourced or embedded, and there existed no clear process for the SAR Unit to make the referral to it. As the CET was not yet fully operational, the referral was made by the SAR Unit to the Retail Financial Crime Team, which provided advisory services to the Retail and Business Banking Division but whose role did not generally encompass this responsibility and for which no guidance existed.

4.138 Upon receipt of the referral, the Retail Financial Crime Team did not consider it part of their remit to review the customer nor to apply EDD, but sought to escalate the matter to the OBE for decision. It did not articulate or present any findings and recommendations in respect of the customer. The SAR Unit's referral was made on the basis that providing services to an MSB was outside Santander UK's risk appetite, rather than because of specific financial crime concerns and did not detail the two previous occasions on which the SAR Unit had formed suspicions that Customer A was involved in money laundering. The Retail Financial Crime Team were not made aware of these by the SAR Unit and had no ability to access the SAR Unit's investigation records on the applicable platform. There was confusion within the Retail Financial Crime Team as to who should consider the referral and whether the OBE was the appropriate decision-maker. As a result, a

recommendation paper was not prepared for the OBE until 27 April 2015, over two months after the referral.

4.139 The OBE considered the case of Customer A on 30 April 2015 and decided to exit the relationship on the basis that Customer A had misled Santander UK as to the nature of its business and that it was operating an MSB, a high risk activity for which Santander UK did not have the controls. Despite being aware of adverse media in relation to Customer A, and that over £5 million had passed through Customer A's account in April 2015 alone, there is no record of whether the OBE considered the possibility that Customer A was engaged in financial crime, whether, as a result, the closure should be prioritised or whether other actions, such as enhanced monitoring, were needed. Certain standard fields in the OBE minutes were left uncompleted, including those requiring consideration of whether the customer should be escalated to Santander UK's MLRO.

4.140 Following the OBE's decision, there was further delay in actioning the closure of Customer A's account. Initially, this was because, since the minutes of the OBE meeting of 30 April 2015 were not signed off until 22 June 2015, no action was taken to close the account. Thereafter, there was confusion as to the process for actioning the OBE's decision which, because the FI Unit was not yet functioning, was forwarded to the CET and thereafter subject to an instruction to Central UK Operations. A request to close the account was sent by email to Central UK Operations on 30 June 2015 but, for unexplained reasons, no action was taken. On 12 August 2015, approximately six months after the SAR Unit's referral, the CET were still seeking an update from Central UK Operations on progress with closing the account.

4.141 In the meantime, Santander UK received further indications of suspicious activity by Customer A. On 30 April 2015, a Santander UK staff member made an internal report of suspicious activity, based on the significant cash flows going through the account and, on 20 and 22 May 2015, transaction monitoring alerts were triggered. Each of these was considered but no further action was taken, largely based on the SAR Unit's previous assessment in February 2015 that Customer A's activity on the account was consistent with that of a legitimate MSB. As a result, Customer A continued to operate its account with no changes to its risk rating or monitoring.

4.142 On 9 September 2015, the Court Order Unit received an information request from a law enforcement agency in relation to Customer A. The request included the information that Customer A was suspected of significant money laundering.

4.143 Such requests should be a valuable source of information for a bank in the identification and management of the risks associated with its customers. However, although the Court Order Unit proceeded to respond to the request, there is no evidence to suggest that the information was passed on for consideration by other teams. Senior financial crime staff subsequently told the Authority that they would have expected to have been alerted immediately, and an internal report of suspicious activity submitted. There is no documentation to suggest that either of these actions took place nor that the information was otherwise shared with those responsible for the management of Customer A or financial crime risks.

4.144 On 16 September 2015, one of the team responsible for conducting the review of the OBE's decisions identified that Customer A's account had not been closed and that "*there are millions of pounds going through the account*". An urgent review was conducted, a further request made of Central UK Operations to close Customer A's account and senior financial crime staff were alerted. However, these alerts did not include the information provided to the Court Order Unit the previous week since this information had not been notified to the relevant staff.

4.145 Later that day, while considering the case, SAR Unit staff members identified the information provided to the Court Order Unit on 9 September 2015. This prompted a swift reappraisal of Customer A by the SAR Unit. In contrast with its previous findings of 19 February 2015, the SAR Unit considered that Customer A's transactional activity was "*excessive for the profile of the business*" and placed reliance on the adverse media previously discounted. The SAR Unit concluded that Santander UK had taken the decision to exit the relationship due to suspicions that Customer A "*was set up as a front business in order to launder funds under the premise that this is a genuine money remittance service*".

4.146 Shortly thereafter, at the request of a law enforcement agency, Santander UK appropriately decided to keep Customer A's account open and in operation. The Authority does not criticise this decision which was made in good faith. However, given Santander UK's appreciation that Customer A was operating a business which Santander UK did not have the controls to monitor effectively, its knowledge of the amounts of money passing through Customer A's account and its suspicions that the account was being used to launder the proceeds of crime, it was imperative that the continuing operation of Customer A's account was subject to close scrutiny and maintained for no longer than was necessary.

4.147 However, although Customer A was initially subject to ongoing monitoring by the SAR Unit, the Court Order Unit failed to share a relevant item of information with the SAR Unit and, when Santander UK received further information in June 2016 that should have prompted it to confirm whether it was still appropriate to continue to allow the account to remain open, no such confirmation was sought. Although Santander UK kept the account open based on its previous engagement with law enforcement, it did not confirm with the law enforcement agency in question whether it should continue to do so and as a result, Customer A's account continued to operate for a further six months without appropriate monitoring.

4.148 In addition, there is no indication that, prior to December 2016, Santander UK identified potential shortcomings in the onboarding or monitoring of Customer A. While senior management were made aware of Customer A, this was generally cited as a positive example of Santander UK having acted to prevent financial crime, due to the coordination that had taken place with relevant law enforcement authorities, and failed to highlight shortcomings in its treatment of Customer A or whether these may be reflective of wider failings.

4.149 On 9 December 2016, the Authority wrote to Santander UK to request information relating to Customer A. In preparing the response to this request, staff identified that the account remained open and, after receiving confirmation from law enforcement that there was no reason to keep the account open, a block was placed on the account on 28 December 2016 and steps were commenced to close the account.

4.150 Customer A's account was closed on 16 March 2017. Approximately £269 million had been deposited into the account since Customer A was onboarded almost four years previously, most of which was transferred out to multiple third parties.

Other customers

4.151 Despite having decided to recommend closure of Customer B's account in July 2017, it was not until 22 September 2017 that the recommendation was made and a decision to close the account was made on 18 October 2017. The account was blocked the following day before it was closed in January 2018.

4.152 A referral for closure of Customer C's account was made on 11 August 2015. A decision to close the account was made by the OBE on 13 August 2015 and Customer C was given 60 days' notice of closure on 4 September 2015. Customer C's account was closed on 16 November 2015.

4.153 The OBE decided to close Customer D's account on 9 July 2015. However, on 27 July 2015, the CET identified that it had not been actioned. The CET proceeded to action the closure. Due to the 60 days' notice period, an agreed extension and charges on the account, the account was closed on 12 November 2015.

4.154 The OBE decided to close Customer E's account on 1 October 2015. A block was placed on the account between 28 October 2015 and 20 November 2015, after which Santander UK gave Customer E 60 days' notice of the closure of its account. Save for the period during which the above block was in place, the account continued to operate, with more than £700,000 credited to the account between 1 October 2015 and it being closed on 29 January 2016.

4.155 Customer F was recommended for closure on 3 July 2014. The OBE was not then in existence and internal emails illustrate some confusion about who was responsible for recommending account closure. Ultimately, closure was reported as approved by the Financial Crime Governance Forum in August 2014. However, a closure notice (with 60 days' notice) was not issued until December 2014 and the account was closed in February 2015.

4.156 By October 2017, the accounts of Customers A and C to F had been closed and the account of Customer B had been blocked. The combined funds which passed through these accounts during the Relevant Period was significant, amounting to approximately £298 million. Approximately £269 million of this was attributable to Customer A's account.

5. FAILINGS

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

5.2 Principle 3 required Santander UK to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. This includes appropriate measures to identify, assess, monitor and manage its money laundering risk.

5.3 Santander UK breached Principle 3 during the Relevant Period, in that:

5.3.1. Its AML governance framework for Business Banking was not designed and implemented adequately to provide for the management of the money laundering risk presented by its Business Banking portfolio. In particular, in the early part of the Relevant Period:

5.3.1.1 Business Banking failed to assess and take responsibility for the money laundering risks presented by its operations;

5.3.1.2 Controls were operated by separate teams with inadequate coordination and oversight of their activities to ensure that they were mutually supportive of achieving overall management of money laundering risk; and

5.3.1.3 Business Banking produced inadequate MI to enable senior managers to ensure the effectiveness of AML controls.

5.3.2. While some improvements were made to Santander UK's AML framework during the Relevant Period, these did not effectively address the underlying weaknesses and failed to ensure that, as a whole, Santander UK adequately managed the money laundering risks presented by its Business Banking customers.

5.3.3. Santander UK's processes failed to ensure that staff onboarding Business Banking customers obtained sufficient information to understand the nature of a customer's business. This had the effect that Santander UK was unable to understand adequately the nature of the customers' businesses and to assess accurately the money laundering risks involved in providing banking services to them.

5.3.4. The training that was provided to staff involved in taking on new Business Banking customers was not sufficiently targeted to their role to enable them to understand their legal and regulatory AML responsibilities in sufficient detail, and to enable them to scrutinise adequately information provided by customers, to challenge discrepancies within it and to ensure that Santander UK adequately understood the nature of the customers' business.

5.3.5. As a result, Santander UK failed to ensure that its onboarding processes were able to identify accurately the money laundering risks presented by its Business Banking customers.

5.3.6. For the period from 31 December 2012 to 15 April 2015, customers' risk ratings were not readily made available to staff dealing with Business Banking customers, meaning that they could not easily take them into

account when assessing money laundering risks, nor update them as necessary in light of new information.

5.3.7. Until May 2015, Santander UK's processes did not require staff to update the risk ratings of Business Banking customers post onboarding. From May 2015, following the introduction of the CRA System, any update depended on a trigger event or bespoke projects.

5.3.8. Until August 2016, Santander UK failed to conduct any periodic, or other systematic, reviews of its Business Banking customers; thereafter, it conducted periodic and event driven reviews but only of customers assessed to be high risk.

5.3.9. As a result, Santander UK failed to ensure that its assessments of the money laundering risks presented by its Business Banking customers were kept accurate and up to date and that these risks were appropriately managed.

5.3.10. Santander UK's automated transaction monitoring system did not take account of information on anticipated Business Banking customer turnover collected at onboarding. While regular reviews of parameters appear to have been carried out for much of the Relevant Period, they were not effective in ensuring that the parameters captured key money laundering risks.

5.3.11. The teams responsible for reviewing automated transaction monitoring alerts and internal reports of suspicious activity on Business Banking customers experienced periods of under resourcing meaning that, at times, transaction monitoring alerts which might, on investigation, have given rise to grounds for suspicion of money laundering were not investigated, and any necessary action taken, sufficiently promptly.

5.3.12. Santander UK's processes failed to ensure that the information identified as a result of its investigations following transaction monitoring alerts and internal reports of suspicious activity was appropriately taken into account when assessing the money laundering risks presented by Business Banking customers or in determining the appropriate level of customer monitoring.

5.3.13. Santander UK's processes and systems did not enable other teams which received information relevant to the risk assessments or ongoing monitoring of Business Banking customers to disseminate that information appropriately, and the improvements that resulted from the introduction of the CET did not fully address this issue.

5.3.14. Investigators and staff involved in taking on new Business Banking customers were not provided with sufficient training on the money laundering risks presented by MSB customers. As a result, there was a risk that they would fail to identify or accurately assess the risks associated with such customers.

5.3.15. Processes for terminating relationships with Business Banking customers where Santander UK considered that money laundering risks could not otherwise be appropriately managed, did not ensure that terminations were always progressed promptly and ongoing activity stopped.

5.4 As a consequence of these inadequacies in Santander UK's Business Banking AML control framework, it was unable adequately to identify, assess, monitor or manage its money laundering risk in its Business Banking portfolio and had not adequately implemented policies and procedures within Business Banking to ensure its compliance with its obligation to counter the risk that the firm might be used to further financial crime.

6. SANCTION

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 Santander UK 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 Santander UK is indicative of the harm or potential harm caused by its breach. The Authority has therefore determined a figure based on a percentage of Santander UK's relevant revenue. Santander UK's relevant revenue is the revenue derived by Santander UK's Business Banking unit during the period of the breach. The period of Santander UK's breach was from 31 December 2012 to 18 October 2017. The Authority considers Santander UK's relevant revenue for this period to be £892,698,346.

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:

(b) "*the breach revealed serious or systemic weaknesses in the firm's procedures or in the management systems or internal controls relating to all or part of the firm's business*";

(d) "*the breach created a significant risk that financial crime would be facilitated, occasioned or otherwise occur*";

6.9 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:

(e) "the breach was committed negligently or inadvertently".

6.10 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 £892,698,346.

6.11 Step 2 is therefore £133,904,752.

Step 3: mitigating and aggravating factors

6.12 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.

6.13 The Authority considers that the following factors aggravate the breach.

6.14 The Authority has imposed financial penalties on Santander UK for breaches of regulatory requirements on previous occasions:

6.14.1. in 2003, the Authority fined Abbey National plc (the predecessor company of Santander UK which, at the time, was under different controllers and managers) £2 million for serious AML failings. Some of those failings (such as insufficient resource to consider and report SARs promptly and CDD failings when onboarding customers) existed during the Relevant Period;

6.14.2. in February 2012, the Authority fined Santander UK £1.5 million for failings relating to sales of its structured products;

6.14.3. in March 2014, the Authority fined Santander UK £12,377,800 for failing to ensure that it gave suitable advice to its customers and to ensure

that its financial promotions and communications with customers were clear, fair and not misleading*;* and

6.14.4. in December 2018, the Authority fined Santander UK £32,817,800 for breaches of Principles 3, 6 and 11 relating to governance, unfair treatment of customers, failing to act on information appropriately and failing to be open and co-operative in the retail bank sector.

6.15 Before, or during, the Relevant Period, the Authority published the following guidance relating to AML controls:

6.15.1. In March 2008, the Authority issued its findings of a thematic review of firms' AML processes in a report titled "*Review of firms' implementation of a risk- based approach to anti-money laundering*". This report included examples of good and poor industry practice and reminded firms that their approach to AML should be aligned with the JMLSG guidance;

6.15.2. In June 2011, the Authority issued a report titled "*Banks' management of high money-laundering risk situations: How banks deal with high-risk customers (including politically exposed persons), correspondent banking relationships and wire transfers*". The report highlighted a failure by banks to apply meaningful EDD measures in higher risk situations and noted the importance of carrying out enhanced monitoring with high-risk customers throughout the relationship;

6.15.3. In December 2011, the Authority's published "*Financial Crime: A Guide for Firms*" which aims to enhance firms' understanding of the Authority's expectations and is designed to assist firms to adopt a more effective, risk- based and outcomes-focused approach to mitigating financial crime risk;

6.15.4. In April 2015, the Authority published "*Financial Crime: A Guide for Firms. Part 1: A firm's guide to preventing financial crime*";

6.16 The JMLSG published guidance to assist those in the financial industry to comply with their obligations, the Authority's guidance or other published materials. JMLSG guidance was published in 2006, 2007, 2009, 2010, 2011, 2013, 2014 and 2017.

6.17 The Authority has published several Notices against firms for AML weaknesses both before and during the relevant period, including in respect of EFG Private Bank Ltd

in March 2013, Guaranty Trust Bank (UK) in August 2013, Standard Bank PLC in January 2014, Barclays Bank PLC in November 2015, Sonali Bank (UK) Ltd in October 2016 and Deutsche Bank AG in January 2017.

6.18 Consequently, Santander UK was aware, or should have been aware, of the importance of identifying, assessing, monitoring and managing its money laundering risk and establishing, implementing and maintaining adequate policies and procedures to ensure its compliance with its obligation to counter the risk that the firm might be used to further financial crime.

6.19 The Authority considers that the following factors mitigate the breach.

6.20 As outlined above, in late 2017, Santander UK established the Realigned Financial Crime Transformation and Remediation Programme. This is a substantial project with the objective of widespread restructuring and enhancements to the financial crime systems and controls across Santander UK.

6.21 In 2019, in order to mitigate AML risk, Santander UK voluntarily ceased the onboarding of Business Banking Customers through online and telephone channels. In 2021, again to mitigate AML risks, Santander UK voluntarily restricted the onboarding of Business Banking customers deemed to be high-risk.

6.22 Having taken into account these factors, the Authority considers that the Step 2 figure should be increased by 15%.

6.23 Step 3 is therefore £153,990,465.

Step 4: adjustment for deterrence

6.24 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.

6.25 The Authority considers that the Step 3 figure of £153,990,465 represents a sufficient deterrent to Santander UK and others, and so has not increased the penalty at Step 4.

6.26 Step 4 is therefore £153,990,465.

Step 5: settlement discount

6.27 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.

6.28 The Authority and Santander UK reached agreement at Stage 1 and so a 30% discount applies to the Step 4 figure.

6.29 Step 5 is therefore £107,793,325.

6.30 The Authority therefore imposes a total financial penalty of £107,793,300 on Santander UK for breaching Principle 3.

7. PROCEDURAL MATTERS

7.1 This Notice is given to Santander UK under and in accordance with section 390 of the Act.

Decision maker

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

Manner and time for payment

7.3 The financial penalty must be paid in full by Santander UK to the Authority no later than 22 December 2022.

If the financial penalty is not paid

7.4 If all or any of the financial penalty is outstanding on 23 December 2022, the Authority may recover the outstanding amount as a debt owed by Santander UK 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 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 Santander UK, prejudicial to the interests of consumers or detrimental to the stability of the UK financial system.

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

Authority contacts

7.7 For more information concerning this matter generally, contact Anthony Williams (direct line: 020 7066 2196/email: Anthony.Williams@fca.org.uk) or Laurenz Maurer (direct line: 020 7066 8096/email: Laurenz.Maurer@fca.org.uk) at the Authority.

Lauren Rafter

Head of Department

Enforcement and Market Oversight Division

ANNEX A – PROVISIONS RELEVANT TO THIS NOTICE

Relevant Statutory Provisions

1. The Authority's operational objectives, established in section 1B of the Act, include protecting and enhancing the integrity of the UK financial system (section 1D(1) of the Act). The integrity of the UK financial system includes it not being used for a purpose connected with financial crime (section 1D(2)(b) of the Act).

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.

Relevant Regulatory Provisions

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

The Principles

4. The Principles are a general statement of the fundamental obligations of firms under the regulatory system and are set out in the Handbook.

5. 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")

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."

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.*"

8. SYSC 6.3.3R provides:

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

9. SYSC 6.3.6G provides:

"*In identifying its risk and in establishing the nature of these systems and controls, a should consider a range of factors, including:*
(1) its customer, product and activity profiles;
(2) its distribution channels;
(3) the complexity and volume of its transactions;
(4) its processes and systems; and
(5) its operating environment."

10. SYSC 6.3.7G provides:

"A firm should ensure that the systems and controls include:
(1) appropriate training for its employees in relation to money laundering;
(2) appropriate provision of information to its governing body and senior management, including a report at least annually by that firm's money laundering reporting officer (MLRO) on the operation and effectiveness of those systems and controls;
(3) appropriate documentation of its risk management policies and risk profile in relation to money laundering, including documentation of its application of those policies (see SYSC 9);
(4) appropriate measures to ensure that money laundering risk is taken into account in its day-to-day operation, including in relation to:

(a) the development of new products;
(b) the taking-on of new customers; and
(c) changes in its business profile; and

(5) appropriate measures to ensure that procedures for identification of new customers do not unreasonably deny access to its services to potential customers who cannot reasonably be expected to produce detailed evidence of identity."

11. SYSC 6.3.8R(1) provides:

"*A firm must allocate to a director or senior manager (who may also be the money laundering reporting officer) overall responsibility within the firm for the establishment and maintenance of effective anti-money laundering systems and controls*."

12. SYSC 6.3.9R provides:

"A firm (with the exception of a sole trader who has no employees) must:
(1) appoint an individual as MLRO, with responsibility for oversight of its compliance with the FSA's rules on systems and controls against money laundering; and
(2) ensure that its MLRO has a level of authority and independence within the firm and access to resources and information sufficient to enable him to carry out that responsibility."

13. SYSC 6.3.10G provides:

"*The job of the MLRO within a firm is to act as the focal point for all activity within the firm relating to anti-money laundering. The FSA expects that a firm's MLRO will be based in the United Kingdom*."

Decision Procedure and Penalties Manual ("DEPP")

14. 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.

The Enforcement Guide

15. The Enforcement Guide sets out the Authority's approach to taking disciplinary action. The Authority's approach to financial penalties is set out in Chapter 7 of the Enforcement Guide.