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:	**Nationwide Building Society**
Firm Reference Number:	**106078**
Address:	**Nationwide House Pipers Way Swindon SN38 1NW**
Date:	**11 December 2025**

1. ACTION

1.1 For the reasons given in this Final Notice, the Authority hereby imposes on Nationwide Building Society ("Nationwide" or "the Firm") a financial penalty of £44,078,500 pursuant to section 206 of the Act.

1.2 Nationwide has 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 £62,969,297 on Nationwide.

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. Under the Authority's rules, financial institutions operating in the UK are responsible for minimising the risk of being used for criminal purposes, including the risk of being used to facilitate money laundering or terrorist financing.

2.2 To mitigate this risk (and as part of their obligation to take reasonable care to organise and control their affairs responsibly and effectively, with adequate risk management systems), firms must establish and maintain an adequate risk-based anti-money laundering ("AML") control framework which is comprehensive and proportionate to the nature, scale and complexity of the firm's activities.

2.3 Such a framework must include measures to establish the identity of its customers accurately at the start of the relationship and gather other customer information (collectively known as "CDD") which will enable the firm to understand the purpose and nature of the customer's intended relationship so that the firm can assess the money laundering risks presented by the customer. Where those risks are high, the firm must carry out enhanced due diligence ("EDD").

2.4 Thereafter, the firm must monitor the activities of the customer, including monitoring transactions to ensure that they remain consistent with the firm's understanding of the customer and the associated money laundering risks. As part of this, the firm must keep information held on customers up-to-date and apply CDD (and where appropriate EDD) measures where it doubts the truth or adequacy of previously obtained documents, data or information. The extent and frequency of the monitoring in respect of each customer will depend on the particular risks they present. Where the risk associated with the customer relationship is high, enhanced ongoing monitoring of the relationship must be undertaken. Where a firm identifies that a customer's activities are not consistent with its understanding of the customer, or that the customer may be engaged in suspicious activity, it must take prompt action to investigate this, and where appropriate submit a suspicious activity report ("SAR") to the National Crime Agency ("NCA") and manage any money laundering risks.

2.5 Retail banking is a cornerstone of the UK's economy and includes the provision of standard current account, loan and savings products to personal and business customers by banks and building societies. There is an elevated risk of financial crime in the retail banking sector because of transaction volumes, simple onboarding processes and its mass market nature. Moreover, criminals often seek to integrate illicit funds into the sector in order that they can spend, store and use these monies. Additional AML steps are required in respect of SME banking customers.

Nationwide

2.6 Nationwide is the world's largest building society. By 1 July 2021 it had approximately 18 million UK customers and £170 billion in customer deposits across its products. It held a 10% market share of UK current accounts, which had grown significantly over the previous 4½ years from approximately 7%. Therefore, it was essential that Nationwide's financial crime prevention systems and controls were effective and tailored to the risks presented by its operations and customers.

Deficiencies in Nationwide's AML monitoring systems and controls

2.7 Between 1 October 2016 and 1 July 2021 ("the Relevant Period") there were deficiencies in Nationwide's AML systems and controls which had a material impact on its ability to monitor effectively its customer relationships. In particular:

(a) It did not have effective systems for refreshing CDD and conducting customer risk assessments. At the start of the Relevant Period, Nationwide's system for individually risk assessing customers was an unsophisticated, interim solution. Unless the customer fell into certain limited categories (one of which was if Nationwide's systems flagged that they had been charged or convicted of a financial crime), they were automatically classed as standard risk. Before the Relevant Period, Nationwide had commenced its RRP project which was intended to introduce a system which would automatically assess the financial crime risk presented by customers and in the interim added further risk assessment triggers. Likewise, measures to gather enhanced CDD were introduced. However, the RRP system was not fully operational until early 2019 and it was not until August 2020 that the additional data items (a number of which were pertinent to the Firm's obligations under the MLRs) were fed into Nationwide's RRP system, and not until April 2021 that the enhanced data was considered for customer risk scoring purposes.

Further, the measures introduced by Nationwide to gather enhanced CDD applied only to brand new customers and existing customers seeking new products, representing only a small percentage of customers. As at the end of the Relevant Period, Nationwide continued to hold concerns about gaps in CDD for existing customers, which were significant in some cases, including in relation to retrievable verification evidence. These gaps meant that it was not always possible to complete a customer risk assessment fully. It was not therefore possible for Nationwide to be confident that all high risk customers had been identified. Notwithstanding improvements made during the Relevant Period, the deficiencies in Nationwide's customer risk assessment architecture (in particular until August 2020) had a potentially material impact on its ability to monitor customer relationships effectively and within the risk appetite approved by Nationwide's board.

(b) Aside from customers already assessed as high risk (which in mid-2020 appears to have amounted to only some 2,000 customers), and (for the majority of the Relevant Period) in breach of its own policies, Nationwide had no process for undertaking either periodic or event-driven reviews of a substantial proportion of its customer relationships. The absence of these controls throughout the Relevant Period prolonged the time it would take for existing customer relationships to be reviewed and their CDD refreshed, so compromising Nationwide's ongoing understanding of its customers, particularly its existing customers who had been onboarded prior to previous uplifts in CDD measures, had not opened new accounts since, and were classified as standard or low risk before the introduction of RRP (which, as above, represented a substantial proportion of its customer base).

(c) The deficiencies in Nationwide's risk assessment and CDD procedures impacted on its transaction monitoring system as a means by which inconsistent or unusual customer behaviour could be detected, investigated and addressed on a risk-orientated basis. However, Nationwide's system for

monitoring customer transactions for unusual activity was inadequate and ineffective. In February 2017 an internal report noted that a recent FCA final notice against a major bank had highlighted the need for an effective, tuned and auditable transaction monitoring solution which took into account the CDD captured from customers. It referred to a 2016 internal review of the system which concluded at the time it was compliant with legal requirements but that there were weaknesses relating to data integrity, governance and understanding of rule amendments and design. Nationwide undertook work in response and engaged compliance consultants to assist in developing the system including from 2019, to outline key improvements required and a multi-year 'roadmap' to deliver them. This placed Nationwide's transaction monitoring maturity at stage two out of five (as compared with amalgamated peers, which were placed at four - a stage it was assessed Nationwide would not reach until 2021). Other than for high risk customers, Nationwide's existing transaction monitoring rules applied uniformly across its entire personal account customer base and a customer's individual circumstances (such as the CDD gathered) would only be taken into account if a rule triggered. The review also suggested that Nationwide needed to introduce peer-based and additional behavioural rules. A review in 2020 of the planned new rules described the existing rules as narrow in focus, limiting Nationwide's ability to cover the full range of money laundering risks to which it was exposed. The review recommended consideration be given to daily or weekly (as opposed to monthly) application of the rules to align with the general direction of travel in the industry. Concerns that alert thresholds for the pre-existing rules were set very high were also expressed by a senior member of Nationwide's financial crime function in 2020. By the end of the Relevant Period, although improved through a significant programme of work, the system still only provided partial coverage of the money laundering typology risks which Nationwide faced.

2.8 The Authority considers that these weaknesses significantly impacted Nationwide's ability effectively to maintain an up-to-date understanding and records of all its current account customers and to monitor these customer relationships on an appropriate risk-sensitive basis, including scrutinising customer transactions to ensure that they were consistent with what Nationwide knew about the customer. In combination, this created material risks over a protracted period that unusual activity by customers might remain undetected and/or that customers moving into the 'high risk' category over the course of their relationship might not be identified and actively managed.

2.9 This created a particularly high risk in respect of any of its customers who were using their personal current accounts for business activity in breach of Nationwide's terms and conditions. Unlike most large retail high street banks, Nationwide did not offer business banking current accounts for SMEs at any time during the Relevant Period. The financial crime risk profile of SME banking customers is different from, and potentially higher than, that of personal customers due to factors such as the greater complexity involved in identifying corporate customers and monitoring their transactional behaviour, and the size and number of the transactions. These and other factors mean that firms ordinarily apply charges for business bank accounts. As a result of these charges (and on occasions other factors - such as challenges faced by businesses operating in certain sectors in obtaining access to bank accounts), firms may identify customers seeking to use personal current accounts for business activity in breach of its terms and conditions. Whether to tolerate such

use is a matter for the firm to decide. However, a firm must continue to meet its legal and regulatory obligations, including its obligations to counter the risk that an account might be used to further financial crime.

2.10 Nationwide's financial crime prevention controls for personal current accounts were not set up for business use. In particular:

(a) Nationwide's CDD measures were not calibrated to capture business characteristics and this meant that Nationwide did not capture sufficient data on businesses (and in the event of the business being a legal entity other than the customer, their beneficial owners) to enable proper risk assessment, identification of customers operating in an industry or geographical area outside of Nationwide's risk appetite, and (if applicable) EDD.

(b) Transaction monitoring systems were not designed to identify unusual and/or suspicious behaviours pertinent to businesses. Nor could they be because the Firm had not gathered the necessary information from businesses on their activities and expected account usage to establish what comprised normal and unusual behaviour. There was a risk that when business use did occur on accounts it would become normalised or generate false transaction monitoring alerts for review.

(c) Training and processes did not include sufficient guidance on how to investigate accounts with potential business use. It was accordingly recognised that unusual/suspicious activity could remain undetected and not reported when appropriate to the NCA.

2.11 Allowing accounts designed for personal use to be used for business, without effective mitigating controls, exacerbated the existing AML monitoring weaknesses and created further risks across the customer lifecycle. These risks were in the Authority's view material and created a consequential risk that unusual or suspicious business activity could remain undetected and not reported to the NCA.

2.12 Prior records are not now available but various staff at Nationwide appear to have recognised from at least October 2016 the financial crime risks of "*unauthorised business use*" of its personal current accounts. In particular it was recognised that

(a) There could be increased external scrutiny and the risk of regulatory censure; and

(b) The Firm was exposed to the risk of being used to further money laundering and potentially committing criminal offences under the MLRs.

2.13 From October 2016 to September 2017 the Firm's staff carried out some initial work to assess the number of accounts subject to unauthorised business use and to develop an outline process for investigating and (where appropriate) closing those accounts. In September 2017 a decision was taken to temporarily tolerate the risks on the basis that Nationwide was planning to launch its own SME business banking product to which personal current accounts being used for business purposes could be migrated. Over a period of approximately two and a half years, the toleration decision was revisited but remained in place. In the Authority's view, that was inappropriate. Nationwide's financial crime prevention controls for personal current

accounts were not set up for business use. It had no settled methodology for calculating the number of personal current accounts subject to unauthorised use, and no framework for dealing with them. Its controls for maintaining an up to date understanding of, and monitoring, its personal current account customers were not operating effectively. Whilst some work continued in the interim to understand and address the business use risks, insufficient mitigation measures were implemented. It was not until around April 2020, when the planned business banking product launch was discontinued, that impactful steps were then taken to develop a model to identify business use and create a formal written framework for defining, investigating, managing and, if appropriate, exiting unauthorised business customers.

2.14 Nationwide was also aware during the Relevant Period of the wider monitoring weaknesses described above (see paragraph 2.7) and progressed or implemented a number of workstreams aimed at remediating or uplifting these matters, including through an ongoing project aimed at ensuring compliance with the MLRs 2017 (in force from 26 June 2017). However, these workstreams did not address the weaknesses in a sufficiently effective or timely manner and from 2020 Nationwide instructed a firm of compliance consultants to undertake a more comprehensive analysis of the effectiveness of its financial crime prevention framework and make recommendations on a target operating model. This produced a greater understanding of the work required to address weaknesses in the framework and resulted in the firm commencing from around June 2021, a more comprehensive financial crime transformation programme.

2.15 The failure by Nationwide to identify and/or address these various weaknesses across its AML monitoring systems and controls in a timely manner impacted in some cases its entire personal current account population (with an increased impact in respect of customers using their personal current accounts for business activity). In turn, this led to an unacceptable risk that inconsistent or unusual activity by customers might remain undetected and unaddressed. The Authority considers these deficiencies over a four-and-half year period comprised a breach by Nationwide of its obligation under Principle 3 to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

2.16 During the COVID-19 pandemic the government implemented the Coronavirus Job Retention Scheme ("JRS"), a temporary scheme announced on 20 March 2020 and designed to protect the UK economy by helping employers whose operations were affected by coronavirus to retain their employees. Receipt of JRS funds into a personal current account is a strong indicator of business use. In total 33,678 JRS payments totalling £64.6m were paid into 5,191 personal accounts at Nationwide.

2.17 In one egregious case, Nationwide missed opportunities to identify unusual activity on the part of one of Nationwide's customers, Customer A, who fraudulently claimed and received from HMRC into their Nationwide accounts 24 JRS furlough payments totalling £1.35m over the course of 13 months and then £26.01m over 8 days between 2020 and 2021. The Authority considers that those monies represented the proceeds of crime and that Customer A used their account to launder those funds. Transaction monitoring alerts were generated at the beginning of a month, based on retrospective transactional activity in the previous month. Accordingly, an alert was only issued in respect of the last four JRS deposits into Customer A's accounts (each of which were in excess of £6m) at the beginning of the ensuing month. Nationwide's procedures then allowed up to 20 working days for alerts to be investigated. In the event, HMRC identified the fraud before the month end and obtained account freezing

and forfeiture orders. However, during the 2020-2021 period in excess of £800,000 had already been transferred out of the accounts and was never recovered. The Authority considers that the Firm's systems and controls should have prompted a review of the unusual activities and consideration of the associated financial crime risks from at least late 2019.

2.18 The Authority therefore hereby imposes on Nationwide a financial penalty of £44,078,500 for its breach of Principle 3, and associated breaches of SYSC rules 6.1.1R and 6.3.1R pursuant to section 206 of the Act.

2.19 Nationwide has invested significantly in remedial steps and enhancing its financial crime framework since the end of the Relevant Period.

2.20 Nationwide has cooperated fully with the Authority throughout the course of its investigation.

2.21 For the avoidance of doubt, this Notice makes no criticism of any person other than Nationwide.

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

"the Banking Proposition Board" means Nationwide's body tasked with, amongst other matters, facilitating collective discussion and making recommendations to appropriate governance forums relating to Nationwide's end-to-end management of the banking, insurance and investment proposition;

"BACS payment" means Bankers' Automated Clearing System which is an electronic payment system used in the UK for transferring money between bank accounts;

"BBM" means a browser-based message used by Nationwide to communicate with its customers;

"the Conduct and Compliance Committee" means a sub-committee of Nationwide's executive risk committee and board risk committee, tasked with, amongst other matters, oversight of conduct and compliance matters;

"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;

"Customer A" means a banking customer of Nationwide between 2014 and 2021;

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

"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 Financial Crime Risk Forum" means a forum of Nationwide tasked with, amongst other matters, oversight of financial crime risks;

"FCTP" means Nationwide's large-scale financial crime transformation remediation programme which formally concluded in June 2024, designed to make significant and lasting enhancements to the financial crime control environment;

"FlexBasic" – the Firm's basic current account product;

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

"HMRC" means His Majesty's Revenue & Customs;

"ID&V means identification and verification, the process of identifying, and verifying the identity of, a customer or potential customer;

"Internal Audit" means a function of Nationwide tasked with providing independent assurance to its board and executive committee;

"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;

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

"JRS" means the Coronavirus Job Retention Scheme a temporary UK government scheme announced on 20 March 2020 and designed to protect the UK economy by helping employers whose operations were affected by coronavirus to retain their employees;

"KYC" means know your customer;

"Money Laundering" means the process by which the proceeds of crime are converted into assets which appear to have a legitimate origin, so that they can be retained permanently or recycled into further criminal enterprises;

"MSB" means a money service business which is a business that deals with currency exchange, money transmission, or cheque cashing;

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

"MLRO" means the Money Laundering Reporting Officer, an individual with responsibility for oversight of a firm's AML systems and controls whose role is to act as the focal point for all AML activity within the firm;

"Nationwide" or "the Firm means Nationwide Building Society;

"the NCA" means the National Crime Agency;

"POCA" means the Proceeds of Crime Act 2002;

"PSCs" means persons of significant control;

"the Relevant Period" means the period 1 October 2016 to 1 July 2021;

"Principles" means the Authority's Principles for Businesses as set out in the Handbook;

"SAR" means Suspicious Activity Report, a report which a firm is obliged to make to the NCA under Part 7 of POCA when it knows or suspects, or has reasonable grounds for knowing or suspecting, that a person has engaged in money laundering;

"SME" means a small and medium-sized enterprise, 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

Nationwide Building Society

4.1 Nationwide is an authorised firm that is regulated by the Authority and the PRA. It is the world's largest building society, is owned by over 16 million members and is a household name in the United Kingdom.

4.2 Nationwide offers retail banking products including mortgages, savings accounts and current accounts. Nationwide's banking business was, during the Relevant Period, predominantly focused on, and known for, its personal banking products and services.

4.3 By the end of the Relevant Period, Nationwide had approximately 18 million customers and approximately £170 billion in customer deposits across its products. It held a 10% market share of UK current accounts, which had grown significantly over the course of the Relevant Period from around 7% at the start of the Relevant Period.

4.4 Nationwide did not provide, at any stage during the Relevant Period, business current account products for its customers. The only business products offered by the Firm were three business savings account products – instant, notice and fixed term.

Retail Banking and financial crime risks

4.5 Retail banking is a cornerstone of the UK's economy and includes the provision of standard current account, loan and savings products to personal and business customers by banks and building societies. There is an elevated risk of financial crime in the retail banking sector because of transaction volumes, simple onboarding processes and its mass market nature. Moreover, criminals often seek to integrate illicit funds into the sector in order that they can spend, store and use these monies.

Relevant legal and regulatory obligations

4.6 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 which 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. Firms must carry out a regular assessment of the adequacy of these systems and controls to ensure that they continue to be effective. These obligations are set out in the Authority's Handbook and, during the Relevant Period, the MLRs which were supported by the JMLSG Guidance together with statements from the Authority.

4.7 The MLRs, as supported by the JMLSG guidance, required that firms undertake CDD to identify customers (including prospective customers), to verify their identities and gather information which would enable the firm to understand the purpose and nature of the customer's intended relationship. This includes where it doubts the truth or adequacy of previously obtained documents, data or information. Where the customer is a business, a firm must gather additional specified information to understand the business and its beneficial owners. Collectively, this information should be sufficient for the firm to obtain a comprehensive picture of who its customers are, and the risk associated with its customer relationships to provide a meaningful basis for subsequent monitoring.

4.8 Where the inherent risk associated with a customer relationship is increased, a firm must apply appropriate and risk-based EDD measures to manage and mitigate that heightened risk. This includes enhanced ongoing monitoring of the relationship.

4.9 Separately, a firm must carry out ongoing monitoring of its customer relationships on a risk-sensitive basis. This includes scrutinising transactions to ensure that they are consistent with what the firm knows about the customer and taking steps to ensure that the firm's knowledge remains current. To facilitate effective transaction monitoring, firms must keep documents, data and information obtained in the CDD context (including information about the purpose and intended nature of the customer relationship) up to date.

4.10 Firms' transaction monitoring systems may vary considerably in their approach to detecting and reporting unusual or suspicious activity. Nevertheless, as is clear from prevailing regulatory guidance on the MLRs, the efficacy of such systems depends upon the quality of the parameters and thresholds which underpin them.

4.11 Relevant extracts from the Authority's Handbook, relevant statutory and regulatory provisions as well as the JMLSG Guidance are set out in Annex A to this Notice.

The Authority's 2015 supervisory review

4.12 In March 2015 (i.e. prior to the Relevant Period), the Authority's financial crime supervision team reviewed Nationwide's AML and financial sanctions systems and controls. The Authority subsequently wrote to the Firm in April 2015 providing high-level feedback on its review. The Authority considered that, broadly, Nationwide was taking sufficient steps to manage AML and sanctions risks. Although the Authority's findings were largely positive, the feedback letter highlighted various areas for development. These areas included, but were not limited to, how the Firm assessed and managed the financial crime risks posed by its customers (including its prospective customers).

4.13 The Authority noted Nationwide had indicated that it was "*working towards*" individually risk-assessing all of its customers. Significantly, the Authority's letter referenced "*weaknesses*" in how the Firm was identifying high risk customers. In

particular, the Authority criticised Nationwide's approach of classifying prospective customers as standard risk unless they fell into certain very limited categories flagged by Nationwide's systems including customers who had been charged or convicted of a financial crime and customers with particular residency or balance levels. Further, the Authority drew attention to Nationwide's use of "*narrow event triggers*" for the purpose of flagging existing customers as being potentially high risk. As a result, the Authority expressed concern that Nationwide may be unable to identify both existing and new high risk customers.

4.14 Nationwide responded to the Authority's feedback letter on 29 May 2015 and indicated that a Retail Risk Profiling (RRP) project (see paragraph 4.19 below) was underway, to introduce a system to automatically assess the financial crime risk presented by each customer based on defined criteria. Ahead of completing that project, the Firm had developed, and intended to continue to develop, an interim solution for identifying and monitoring high risk customers. At that time, the interim solution generated monthly alerts based upon the application of certain event triggers (e.g. nationality/residency in a high risk country) and transaction monitoring rules (e.g. credits or debits to the account of a certain amount), to customer and transaction data, as well as receiving referrals from other business areas, such as the Police Liaison Team dealing with law enforcement bodies. Nationwide stated that the interim solution would be enhanced through the addition of further event triggers and monitoring informed by the higher risk money laundering and terrorist financing scenarios to which it was exposed. Moreover, Nationwide committed to review and enhance its policies and procedures as part of its continuous improvement process.

MLRO report

4.15 In September 2022 (i.e. following the Relevant Period), Nationwide completed its MLRO report for the period April 2021 to July 2022 which gave an update on the operation and effectiveness of its financial crime systems and controls. Specifically, the report noted that Nationwide had been acting outside of its financial crime risk appetite due to a need to improve a number of primary AML controls. The report highlighted a number of "*priority*" issues in need of remediation which affected many of its customers. These included, but were not limited to, gaps in required CDD data, no processes for risk based periodic and event driven reviews and transaction monitoring rules providing only partial scenario coverage of the AML risks which Nationwide was exposed to.

4.16 The report concluded that Nationwide's financial crime control environment was, at that time, only "*partially effective*" at mitigating AML (and terrorist financing) risks. Given the deficiencies in controls, its residual risk profile (i.e. Nationwide's risk profile as assessed against its AML risk control framework) was assessed to be higher than previously reported.

4.17 Although Nationwide did put in train a number of projects and actions to review and enhance relevant policies and procedures as part of its continuous improvement process, in line with the commitment given in May 2015, including the RRP project (see paragraph 4.19 below) and a project to improve transaction monitoring capabilities, Nationwide continued to suffer deficiencies in its financial crime prevention systems and controls during the Relevant Period (in the manner and with the impact set out in the paragraphs below).

(i) Refreshing CDD and conducting customer risk assessments

4.18 At the start of the Relevant Period, Nationwide's system for individually risk assessing customers was an unsophisticated, interim solution, with a formal scoring process still being developed at this time. Unless the customer fell into certain limited categories (one of which was if, for example, they were flagged by Nationwide's systems that they had been charged or convicted of a financial crime), they were automatically classed as standard risk. Consequently, Nationwide did not have a sophisticated understanding of the financial crime risks presented by its individual customer relationships, such that the Authority was concerned the Firm had not identified (and would not identify) all of its high risk customers, either at onboarding or on an ongoing basis.

4.19 Before the Relevant Period, Nationwide had commenced its RRP project which was intended to introduce a system which, amongst other things, would automatically assess the financial crime risk presented by customers based on defined criteria. In the meantime, Nationwide sought to mitigate its customer risk by adding a range of additional CRA event triggers (the majority of which initially centred upon a customer's nationality/residency) and later expanding its interim CRA solution to trial various individual risk assessment metrics, pending the planned launch of its permanent solution in October 2018.

4.20 However, the RRP system was not fully operational until early 2019. In May 2019, Nationwide Internal Audit conducted a review of the CDD data which the RRP customer risk assessment utilised, and how the system's defined criteria were being applied. The review was conducted by Nationwide's Internal Audit function against the risk that Nationwide was unable to identify high risk customers and therefore take appropriate steps to manage those relationships. Internal Audit concluded that the controls over the quality of data for the RRP system required "*significant improvement*", partly due to discrepancies in the number of records across systems utilised by the RRP. Relatedly, Internal Audit also identified a lack of oversight to ensure the quality of data being transferred between those systems. These issues, which culminated in 44,957 customer accounts having not been fed into Nationwide's customer risk assessment tool, were subsequently investigated and resolved (with most of the outstanding accounts being fed into the risk assessment tool by late 2019).

4.21 The MLRO report for the year ending March 2020 noted that, from July 2019, the firm had enhanced the CDD it was gathering. However, the uplift in CDD information only applied to some 888,618 customers that year (either brand new customers or existing customers seeking new products), representing just 5% of Nationwide's customer base.

4.22 Additionally, whilst this enhanced CDD was placed on a database available to the SARs and EDD teams, it had not been fed into the firm's main customer data repository and so did not inform the RRP customer risk assessment or transaction monitoring systems. Furthermore, the Firm did not consider certain information which was pertinent to its obligations under the MLRs (i.e. of relevance to its understanding of the purpose and nature of the business relationship with a customer) so that it could undertake an effective customer risk assessment.

4.23 Nationwide's RRP and MLR17 projects were working towards ensuring that the enhanced CDD data items fed into the RRP system. This was achieved from August

2020. However, these data items could not be considered for customer risk scoring purposes until April 2021. The MLR17 project had also been working on an event-driven review capability, but this had been deferred to focus on the capture and use of customer data. This position was revisited by Nationwide in June 2020, with a recommendation that further advice be sought on the compliance gaps (and planned remediation steps) which remained, namely that: (i) there was no refresh planned for back-book customers (i.e. those who do not open new products); (ii) there was no trigger mechanism or technical solution scheduled to be delivered in order to refresh CDD on an ongoing basis; and (iii) the additional CDD being captured would not be consumed by Nationwide's transaction monitoring tool.

4.24 In October 2020 a review commissioned by Nationwide from a firm of compliance consultants identified the need for improvements. In particular, it expressed concern about whether Nationwide had accurately identified the full extent of its high risk customer population, which at that time numbered just over 2,000 customers. The report observed that this number was "*exceptionally low*" when compared to the overall population of approximately 18 million customers.

4.25 Notably, following improvements to the Firm's customer risk assessment tool as part of the financial crime transformation programme, Nationwide identified that over 18,000 customers (in addition to those that fell into certain very specific categories, for example, they were flagged by Nationwide's systems as having been charged or convicted of a financial crime) were potentially high risk.

4.26 By the end of the Relevant Period, Nationwide also continued to have concerns about gaps in CDD for customers, which were significant in some cases, including in relation to retrievable verification evidence. The CDD gaps meant it was not always possible to complete a customer risk assessment fully and, therefore, it was not possible for Nationwide to be confident that all high risk customers had been identified. In particular, Nationwide recorded in its MLRO report for 2021/22 that significant gaps existed across the CDD data of numerous customers (including personal current account customers). Specifically, it was only by September 2022 that Nationwide had successfully updated the ID&V records of 190,000 customers, with a further 110,000 active customers with incomplete ID&V records due to gaps in data requiring remediation.

4.27 Likewise, the report recorded that a cohort of approximately 830,000 existing customers needed fuller CDD as a "*priority*" on the basis that "*these may be assessed as high-risk once the required CDD data is collected*". Nationwide considered that the CDD gaps impacting the remaining "*15m*" customers were "*less material*" or "*not material*" and it was therefore "*unlikely*" or "*very unlikely*" that those customers were high risk, although this needed to be validated.

4.28 Subsequently, through testing and remedial work undertaken after the Relevant Period, which resulted in Nationwide reviewing over 18,000 potentially high risk customers, confirming the high risk categorisation of certain of those customers (in addition to increasing the risk categorisation of a large number of customers from standard to medium risk), and exiting existing customers identified as outside the Firm's risk appetite, Nationwide considered that its remaining customer base was generally low risk.

4.29 Accordingly, notwithstanding the improvements made, the deficiencies in Nationwide's customer risk assessment architecture during the Relevant Period (in

particular until August 2020 – see paragraph 4.23 above) were relevant to its monitoring of many of its customer relationships. This had a potentially material impact on its ability to monitor effectively customer relationships on an appropriate basis and within the risk appetite approved by its board.

(ii) Periodic and event-driven reviews

4.30 Pursuant to the MLRs, firms (including Nationwide) must maintain up-to-date knowledge and understanding of their customers and business relationships. Firms are therefore required to undertake reviews of existing customer records to ensure that documents and information obtained for CDD and EDD purposes remain accurate. In respect of ID&V documentation and information, there is no obligation to re-verify a customer's identity, providing it has been satisfactorily verified and a firm has no doubts regarding the veracity or adequacy of the ID&V evidence previously obtained. In order to be reasonably satisfied as to a customer's identity, firms must exercise a risk-based approach taking into account factors including the nature and length of any existing or previous relationship with the customer.

4.31 Periodic reviews involve a firm reviewing customer relationships at defined intervals, with the frequency dictated by the customer's risk assessment. Event driven or trigger reviews involve customer reviews occurring outside of this set schedule, when events take place impacting on the risk presented by the customer. It is for firms to determine what events should trigger such a review as part of an overall effective framework. Common examples include customer-initiated events (such as an application to the firm for a further account or product) and on the occurrence of heightened risks identified through other monitoring controls (such as the firm's transaction monitoring and/or its internal suspicious activity reporting systems).

4.32 From October 2018 to November 2019, Nationwide's policies and procedures made it mandatory for all business areas to undertake periodic reviews every two years for high risk customers, every three years for standard risk customers, and every five years for low risk customers. From November 2019 to June 2021, a periodic refresh was required every two years for high risk customers and every 5 years for standard risk customers, to be complemented by an event driven review process. Nationwide's policies and procedures also made it mandatory for CDD to be updated/gathered when additional relationships were established with a customer and when certain other defined risk events occurred. These included, for example, transactions occurring on a customer's account which were significant in value and exceeding typical activity and/or complex in nature and/or executed with no obvious reason.

4.33 However, for a substantial proportion of its customer base, Nationwide lacked appropriate systems to give effect to these internally mandated requirements. A December 2017 external review had recommended that Nationwide consider a potential enhancement in the form of an effective event driven review process linked to the outcome of customer risk assessments. At this time, Nationwide had put in place a project to design and develop its ability to undertake periodic and event driven reviews. However, this was then deferred to focus on the IT build necessary to deliver usable CDD data (and therefore CDD refreshes). In October 2020 and June 2021, external reviews highlighted that periodic reviews were not being performed at all on existing customers who had not been assessed as high risk, which for standard risk customers was a breach of Nationwide's policy requirements. Further, at the end of the Relevant Period, the work to deliver an event driven review process (outside of new account openings) had still not been completed.

4.34 The deficiencies in various controls during the Relevant Period prolonged the time it would take for existing customer relationships to be reviewed and their CDD refreshed, so compromising Nationwide's ongoing understanding of its customers, particularly its existing customers who had been onboarded prior to previous uplifts in CDD measures, had not opened new accounts since, and were classified as standard or low risk before the introduction of RRP (which represented a substantial proportion of its customer base).

(iii) Transaction monitoring

4.35 The weaknesses outlined above in Nationwide's monitoring controls impacted on its transaction monitoring system as a means by which inconsistent or unusual customer behaviour could be detected, investigated and addressed on a risk orientated basis. However, over the Relevant Period there were concerns about the effectiveness of the system which in the Authority's view were material.

4.36 In February 2017 an internal report noted that a recent FCA final notice against a major bank had highlighted the need for an effective, tuned and auditable transaction monitoring solution which took into account the CDD captured from customers. It referred to an earlier internal review of Nationwide's transaction monitoring system completed in July 2016 with a rating of 'some improvement required' which identified weaknesses around data integrity, governance and understanding of rule amendments and design. Whilst the internal review concluded at the time that the system was compliant with the MLRs 2007 it noted, for example, that *"…Although* [the transaction monitoring] *rules are generating alerts to allow for the identification of activity for investigation, there is no formal documentation which determines the purpose of the rules, the anticipated tolerances for alerting volumes, what the success of the rules should look like and whether or not they are relevant to* [Nationwide's] *line of business and the external AML/ Counter Terrorist Financing (CTF) risk factors."*

4.37 Later in 2017 Nationwide completed a review of its rules, making some changes and introducing rule documentation in response to the above review. The MLRO's report for the year ending March 2018 noted that a review of transaction monitoring had been completed in conjunction with a firm of compliance consultants and a target operating model developed. The second phase of the RRP project, which had been intended to deliver integrated transaction monitoring capability was however unfunded.

4.38 By at least late October 2018, Nationwide's policies and procedures (specifically its Financial Crime Minimum Control Standards) made it mandatory for all business areas to apply transaction monitoring controls appropriate to the risk presented by the relationship and the circumstances of the customer including CDD/EDD gathered. However, the Minimum Control Standards document also recorded that "*There may be occasions where transaction monitoring is applied to all customer accounts without consideration for individual circumstances*." This reflected the fact that whilst Nationwide had specific rules targeted at high risk customers, its transaction monitoring rules otherwise applied uniformly across its entire personal account customer base and a customer's individual circumstances (such as the CDD gathered) would only be taken into account by transaction monitoring alert investigators, if a rule triggered.

4.39 In 2019, Nationwide engaged a firm of compliance consultants and commenced a project to review and improve its transaction monitoring systems and controls. A key area for development identified by the review concerned the matters in the paragraph above – the prescriptive nature of the transaction monitoring rules, which were categorised by product with singular thresholds applied to all customers and the need to introduce behavioural and peer comparison based rules via segmentation of customers. Other areas identified for improvement related to data integrity, the risk and control framework, emerging risk identification, use of CDD information, oversight and assurance and high risk countries. The 2019 review resulted in a four year 'roadmap' and placed Nationwide's transaction monitoring technological and operational maturity at stage two out of five. By way of comparison Nationwide's peer financial institutions were (when amalgamated) placed at stage four, a stage the roadmap assessed Nationwide would not reach until approximately 2021.

4.40 On 30 January 2020 Nationwide responded to questions from the Authority about its transaction monitoring system, and its ability to detect large transactions which occurred on the personal account of a customer under investigation by various authorities for investment fraud (see further details at paragraph 4.58(d) below). Nationwide explained that the system was not fed by individual customer CDD such as expected income or usage and the rules in place had not alerted when the customer's account received two credits of £40,000 and one credit of £50,000, each of which were in excess of the customer's declared annual income of £37,500. Nationwide described its "*risk-based approach*" as: (i) monitoring customer transactions against what is expected for a retail financial services product (their "*rules-based*" approach); and (ii) monitoring customer behaviours, through a design that would alert in cases where activity did not meet the thresholds of rules-based scenarios (their "*behavioural*" approach). As part of the analysis of the customer in question, Nationwide confirmed that it was considering the introduction of additional 'behavioural' style rules, including potential ratio-based comparison between the customer's income (from CDD held) and the account turnover to better reveal potentially suspicious activity. The customer in question prompted Nationwide to review the system and explore applying lower frequency, volume and/or value alert thresholds. However, Nationwide decided against this because (amongst other matters) it would introduce significantly increased false positive alert levels, no other significant unknown risk exposures had been identified, and the roadmap was underway to review and improve the transaction monitoring system.

4.41 In August 2020 the firm of compliance consultants reported on the new rules devised for the system. It considered these appeared to provide adequate risk coverage and would align it with Nationwide's peers. However the report highlighted that a number of the proposed new rules relied on salary/income information, which was not currently being fed into the system and in addition might not be accurate. It also evaluated the existing rules adopted by Nationwide in its transaction monitoring and observed "*The rules currently in production have a narrow focus, utilising very specific ML detection logic. This has limited* [Nationwide's] *ability to cover the full range of its ML risks. There were also significant risk gaps observed when comparing risk typologies against those observed in other peer retail organisations*". The report recommended consideration should be given to daily and weekly (as opposed to monthly) batch process to align with "*the general direction of the industry and peer organisations*". A monthly batch process involves an alert being generated based on the previous month's activity. In common with all retrospective controls, monthly batch processing of alerts gives rise to the possibility that any funds associated with those alerts may have been transferred away before the alert is reviewed.

4.42 In February 2021 Nationwide's staff performed a financial crime state of the nation control assessment. Overall, it rated Nationwide's transaction monitoring as needing "*significant improvement*" including to ensure its transaction monitoring systems fully mitigated against the relevant threats, typologies and scenarios to which the retail product range was exposed.

4.43 At the end of the Relevant Period, although improved through a significant programme of work, the transaction monitoring system still required development to be fully effective. In early 2022 Nationwide's staff undertook a gap analysis to compare the findings in a recent FCA final notice against a major bank in respect of transaction monitoring, with Nationwide's own applicable systems and controls. The analysis noted that whilst various workstreams were underway, there were continuing potential gaps in Nationwide's transaction monitoring controls with respect to scenario coverage, parameters and data. For example, Nationwide needed to revisit the thresholds set before transaction monitoring alerts triggered to ensure that they remained appropriate and document its processes for monitoring such thresholds. Concerns about "*very high*" thresholds in the previously applicable rules had also been expressed by a senior member of Nationwide's financial crime function in 2020. The absence of complete and/or up to date CDD for certain customers also continued to impact the system to identify inconsistent or unusual activity by customers. The MLRO report for the year ending July 2022 found: "*Improvements are needed to the Transaction Monitoring capabilities and controls, as the current set of rules implemented, only provide partial coverage of risks and money laundering typologies that Nationwide is exposed to. As a result, unusual activity that requires investigation to determine if it appears to be suspicious, may remain undetected*."

(iv) Impact of the monitoring issues

4.44 Nationwide implemented various workstreams to address these monitoring problems, including from June 2021 a financial crime transformation programme. However the cumulative impact of the above gaps was that even at the end of the Relevant Period Nationwide lacked fully effective systems for: (i) ensuring that its knowledge (including CDD) of customers remained current; (ii) monitoring its existing customer relationships on a risk-sensitive basis; and (iii) scrutinising transactions to ensure that they were consistent with what Nationwide knew about the customer. The risk that unusual activity by customers might remain undetected and/or that customers moving into the 'high risk' category over the course of their relationship might not be identified and actively managed, therefore persisted.

(v) Lack of additional monitoring where personal customer accounts used for business activity

4.45 A notable example of a particular cohort of Nationwide's customers impacted over the Relevant Period were customers using their personal current accounts for business activity. The Authority considers that, over the Relevant Period, Nationwide's failure to address in an effective or timely way the above financial crime weaknesses created a particularly high risk in respect of customers using their personal current accounts for business activity in breach of Nationwide's terms and conditions.

AML measures and risks associated with SME banking

4.46 Unlike most large retail high street banks, Nationwide did not offer business banking accounts for SMEs at any time during the Relevant Period. Further, Nationwide's contractual terms and conditions prohibited personal current accounts from being used for business purposes.

4.47 The financial crime risk profile of small and medium-sized business banking customers is different from, and may be higher than, personal customers due to factors such as the greater complexity involved in identifying corporate customers, the size and number of the transactions and monitoring their transactional behaviour.

4.48 These and other factors mean that firms ordinarily apply charges for business bank accounts. As a result of these charges (and on occasions other factors - such as challenges faced by businesses operating in certain sectors in obtaining access to bank accounts), firms may identify customers seeking to use personal current accounts for business activity in breach of their terms and conditions. Whether to tolerate such use is a matter for the firm to decide. However, a firm must continue to meet its legal and regulatory obligations, including its obligations to counter the risk that the account might be used to further financial crime.

4.49 During the Relevant Period, the Authority's guidance to firms on prevention of financial crime warned, in the section dealing with handling higher-risk situations and enhanced monitoring, that an example of poor practice would be where a firm makes no enquiries when accounts are used for purposes inconsistent with expected activity (e.g. personal current accounts being used for business).

Recognition of risks presented by customers using personal current accounts for business activity

4.50 On 19 October 2016, Nationwide's Internal Audit team produced a 'short form' report to identify the extent to which personal current accounts were being used for business purposes. The report was prompted by several conversations between Internal Audit and business stakeholders which made it apparent that 'business use' was known and tolerated within the firm. The executive summary stated:

"Nationwide's T&Cs do not allow current accounts to be used for business purposes. However, there are no agreed appetite measures to monitor, manage and exit accounts that operate in contravention of the T&Cs. There are c.2700 accounts that are clearly being used to facilitate business transactions. As these accounts were opened for private use, Know Your Business due diligence has not been undertaken creating a risk that Nationwide is facilitating business transactions for individuals and limited companies where we have no knowledge of the business activity.."

4.51 The October 2016 Internal Audit report noted:

(a) Impacted products included Flex, Flex Direct, Flex One, Flex Plus and Flex Basic (a product designed for customers otherwise unable to open a standard bank account with limited functionality).

(b) The estimate of 2,762 accounts dated back to July 2016 and related to personal account customers receiving 40-2,700 credits into their account in

a month. The average personal account customer received 4 credits in a month.

(c) Four customers were included in the analysis by way of example. This included a customer who had received numerous cash credits and appeared to be operating in what Nationwide subsequently defined as a 'high risk industry'.

(d) The root cause of the issues was that there was an awareness across Nationwide that in practice customers might use their personal current account for business purposes, but accountability was not assigned for the setting and managing of risk appetite as there was no clear owner for doing so.

4.52 The report set a 'Issue Target date' of 15 May 2017 but noted in the 'Management Action Plan' that resolution of the issue was subject to dependencies including roles and accountabilities which still needed to be defined.

Recognition of multiple AML risks arising from the issue

4.53 In addition to the risks identified above during and/or after the Relevant Period the Firm also identified what the Authority considers to have been significant financial crime risks arising from the business use of personal current accounts including:

(a) Nationwide's financial crime control framework was not set up to manage the specific financial crime risks associated with operating accounts for businesses. Nationwide was facilitating business transactions for individuals and limited companies where it had no knowledge of the business activity. Risks arising from allowing accounts designed to be used by individuals to be used for business activity spanned systems and controls across all stages of the customer relationship lifecycle and involved:

(i) CDD measures which were not calibrated to business customers. For example, the Firm's questions were designed to understand personal income, occupation and lifestyle, and not business characteristics. The Firm's questions did not capture basic information relevant to businesses such as the nature of the business and expected trading patterns.

(ii) Insufficient CDD meant the Firm was in some cases not capturing data for businesses, and if applicable (i.e. in the event of the business being that of a legal entity other than the customer), their owners and controllers to ensure they could be screened appropriately, to include, for example, for sanctions or adverse media matches. This created a risk that in such cases the Firm would not identify that it was facilitating transactions for sanctioned entities.

(iii) Insufficient CDD meant Nationwide could not identify customers operating in an industry or geographical area which was outside the Firm's risk appetite. In particular, the Firm's AML teams had identified accounts being operated by money service businesses which Nationwide considered to be high risk and to require additional due diligence over and above that ordinarily required.

(iv) Insufficient CDD also hampered the Firm's ability to produce accurate risk assessments to inform effective EDD and transaction monitoring. For example, transaction monitoring controls were not designed and calibrated to identify unusual and/or suspicious behaviours pertinent to businesses. Nor could they be because the Firm had not gathered the necessary information from businesses on their activities and expected account usage to establish what comprised normal and unusual behaviour. There was a risk that when business use did occur on accounts it would become normalised or generate false transaction monitoring alerts for the AML team to review. Nationwide identified that such false alerts were diverting resources in its suspicious activity and investigations team which was operating at full capacity.

(v) Training and processes did not include sufficient guidance on how to investigate accounts with potential business use. For example, a process for branch staff to close accounts used for business purposes was rarely used due to the lack of guidance to support identification of a business account and subsequent conversations with a customer. It was accordingly recognised that unusual/suspicious activity could remain undetected and not reported when appropriate to the NCA.

(b) In relation to potential impact, internal concerns highlighted that: (i) there could be increased external scrutiny and the risk of regulatory censure; and (ii) Nationwide was exposed to the risk of being used to further money laundering, terrorist financing and/or tax evasion, and potentially committing criminal offences under the MLRs.

Nationwide's insufficient and untimely response to the issues identified in the Internal Audit report in the period 2016-2020

4.54 In the period between the October 2016 Internal Audit report and July 2020, the steps taken by the Firm to address the issues outlined in it were insufficient and untimely:

(a) From April 2017 the Firm's current account product team prepared papers for its Banking Proposition Board proposing a cross-community project be set up with the objective of: (i) defining acceptable and unacceptable business use; (ii) developing a process that identified and monitored accounts used for business purposes; and (iii) closing accounts being used for business purposes. In addition to the financial crime risks, the papers identified other risks associated with allowing customers to continue to use personal accounts for business activity such as commercial risks (the higher running costs to Nationwide and absence of business banking charges), operational risks, and payment services risks (Nationwide's systems were not designed for the volume of transactions associated with business activity). At the same time, it recognised that closing the accounts could present risks to the account holders (particularly given the challenge of defining business use) and proposed these be mitigated through investigation of the accounts, and appropriate notice to the account holders to change their behaviour or make alternative arrangements.

(b) That project was set up by July 2017, began working on a definition of business use and prepared an outline process for investigating and closing them, noting it was "…*essential that this weakness in Nationwide's AML controls (identified in October 2016) is addressed as soon as possible…".*

(c) However, in September 2017 the project reported that Nationwide lacked the capability to undertake the account investigations and it would take at least 12 months of work, once capability had been identified, to pilot a process to target the worst offenders. The project recommended that the Firm's Banking Proposition Board tolerate the risks on the basis that Nationwide was planning to launch its own business banking product to which personal current accounts being used for business purposes could be migrated. This was agreed by the Banking Proposition Board for three months during which the Firm's financial crime team were to "*refine the risk assessment regarding 'Know Your Business' requirements"*.

(d) In February 2018 this risk assessment concluded that controls across the Firm's framework (CDD, transaction monitoring, training, identifying and reporting of suspicions, screening and EDD controls) were not effectively designed for business activity, and that business use customers produced a significant and disproportionate percentage (10%) of all internal SARs submitted by employees and transaction monitoring alerts triggered by its systems. It outlined two options to address the risk:

(i) risk avoidance – progressing the work undertaken since 2017 and closing accounts where business use is identified; and

(ii) risk mitigation – establishing the required controls. The "*minimum"* controls required "*to achieve an effective control framework"* included: completing ID&V on business entities; screening them; obtaining CDD to understand the nature of the business relationships and their intended account usage; risk assessing the relationships; applying EDD where appropriate; ring-fencing the accounts; and calibrating the transaction monitoring system.

(e) Despite the risks, on or around May 2018, the Banking Proposition Board elected to continue tolerating the risk of business use of personal current accounts. This decision remained in place until around April 2020, when the planned business banking product launch was discontinued. That decision was inappropriate in circumstances where: (i) Nationwide's financial crime prevention controls for personal current accounts were not set up for business use; (ii) it had no settled methodology for calculating the number of personal current accounts subject to unauthorised use, and no framework for dealing with them; (iii) its controls for maintaining an up to date understanding of, and monitoring, its personal current account customers were not operating effectively; and (iv) whilst some work continued in the interim to understand and address the business use risks, insufficient mitigation measures were implemented.

4.55 Subsequently, in July 2020, the Firm's Financial Crime Risk Forum, noting that the risk from the issue was "*significant*" and presented "*multiple financial crime risks*" that needed to be addressed, reported that work was still required to understand the scale of the problem and develop a process to manage the risks.

Eventual steps by the Firm to identify the scale of the issue and mitigate the risks

4.56 Following the Firm's decision to cease development of the business bank account product, it revisited the decision to tolerate the risk of business use of personal current accounts:

(a) Work recommenced on assessing the scale of the issue and a proportionate response. Whilst work was plainly still required to enable the Firm to build an accurate understanding of the numbers of customers involved, there was at the time a view within at least the Firm's financial crime function, that it had been well known for five years or more that customers were using their personal current accounts in this way.

(b) Analysis had been undertaken in late 2019 which led to an early estimate that 17,000 customers might be using their personal current accounts for business activity. From around August 2020 members of the Firm's data and analytics team were tasked with developing a model to identify accounts potentially being used for business purposes. This was not straightforward, given that most business use occurred in 'mixed' accounts, that is accounts that were used both as a personal account and for some business activity. A three-month pilot of the model commenced in May 2021 and ran to July 2021. By 6 July 2021, the model generated a figure of 133,200 customers which (depending on Nationwide's chosen approach) might need to be reviewed to assess if they were using their accounts for business. The consequence was that c.16,000 accounts were ultimately identified for exit on the grounds of misuse of the account (see paragraph 4.58(b) below).

(c) On 26 May 2021 Nationwide approved a business use framework. For the first time this incorporated an agreed definition of potential business use, documented the Firm's applicable risk appetite, and laid out a policy for managing business use of current accounts as well as accountabilities, roles and responsibilities. Senior management oversight mechanisms were also implemented.

4.57 In July 2021, management in the Firm's current account business closed the issues in the report on the basis there was now: clear accountability for the issue; the key risks had been identified; systems and controls to mitigate the risks designed and implemented; and appropriate resources applied. A subsequent report by Internal Audit validated this decision and found that progress had been made to reduce the risk of business use of personal current accounts.

Risks and impact over the Relevant Period

4.58 The Authority considers that the extended period of time which elapsed between the firm's identification of a group of personal current account customers using their accounts for business activity and the Firm taking impactful steps to address it, comprised a failure by the Firm to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. The risks flowing from these failures were not merely theoretical.

(a) Whilst the Firm did not, until the end of the Relevant Period, have what it considered to be an accurate estimate of the number of customers using

their accounts in this way, such use was known about and tolerated (see paragraphs 4.50 and 4.56(a)). The February 2018 risk assessment (see paragraph 4.54(d)) noted that business use customers produced 10% of all internal SARs and transaction monitoring alerts. Although the number of these which resulted in external SARs were comparatively low (see paragraph 4.58(c)) this data made it clear that any low estimates of customers using their personal current accounts for business activity (for example, the figure of c.2,700 in the Internal Audit report) were unlikely to represent the true scale of the issue.

(b) Applying the approved business use framework, in the period August 2020 to August 2024, Nationwide determined that c.16,000 personal current accounts were being used for business activity and closed the vast majority, with c.600 awaiting closure pending the outcome of matters outside the Firm's control (for example, the account being subject to a freezing injunction or other court order).

(c) Whilst (as noted at paragraph 4.53(a)(iv)) a significant proportion of the transaction monitoring alerts and internal reports of suspicious activity raised early in the Relevant Period did not ultimately result in external SAR disclosures (Nationwide's SAR team presumably having concluded that they did not meet the threshold for reporting), approximately 2,147 external SARs were submitted to the NCA.

(d) The submission of an external SAR does not automatically equate to crystalised risk. However, in late 2019 there was an awareness within Nationwide that there were two serious incidences of harm involving customers who were able to use their personal current account(s) for business activity over an extended period of time without intervention. The Firm's 2019 MLRO report flagged that "*…two…cases in late 2019 brought to life these* [i.e. business use] *risks which attracted external press coverage and regulatory scrutiny*. In July 2020 another paper highlighted that one of the customers was subject to investigation by the authorities for investment fraud. It was noted: "*These cases significantly impacted Members"* and whilst staff at the Firm had spotted unusual activity, investigation using the CDD available had been unable at the time to confirm suspicious activity. The paper indicated that these were not the only two examples of the risk of business use: "*Multiple more recent cases highlight the risks from business use and the partially effective nature of our FC control environment".*

4.59 During the COVID-19 pandemic the government implemented JRS, a temporary scheme announced on 20 March 2020 and designed to protect the UK economy by helping employers whose operations were affected by coronavirus to retain their employees. Only entities with a UK payroll and meeting other scheme conditions could claim. However:

(a) The Firm's records show that it was aware by at least May 2020 that around 5,000 of its personal accounts had received furlough or grant payments in relation to COVID-19 and it was noted in May 2020: "*These provide a strong indicator of business use on the account".*

(b) On 24 September 2020 it was reported to the Conduct and Compliance Committee that JRS payments in excess of £17m had been deposited.

(c) In total 33,678 JRS payments totalling £64.6m were paid into 5,191 personal accounts at Nationwide. Furthermore, 93 of the Firm's customers (including a number using a Flex Basic account) were able to use their personal accounts to receive JRS payments exceeding £50,000.

(d) As set out in further detail below, over a period of 15 months between 2020 and 2021 one of these customers, Customer A, received into their personal Flex Basic bank account 24 JRS payments totalling £1.35m over 13 months and £26.01m over 8 days following fraudulent claims to HMRC. Nationwide recognised Customer A's suspicious activity and reported it externally on one occasion. However, the account remained open for a prolonged period of time and Nationwide missed opportunities to identify unusual activity, make additional suspicious activity reports and/or terminate the relationship with Customer A sooner.

4.60 JRS payments were made in support of businesses during the pandemic, and the receipt of such sums into Nationwide personal current accounts indicated unauthorised business use of personal current accounts. Nationwide's business model was exclusively retail-focused and the Firm did not have an adequate AML framework for monitoring business banking. An adequate business use framework and better monitoring controls would likely have provided Nationwide with several additional opportunities to close Customer A's accounts. The Authority therefore considers Customer A's case to be an example of the deficiencies in Nationwide's systems for monitoring its customers and for managing the risk of business use of personal current accounts.

Nationwide's relationship with Customer A

4.61 In Summer 2021, Customer A was subject to account freezing orders based on the allegation that Customer A attempted to commit a large-scale fraud by way of successfully claiming some £27.36m of JRS payments from HMRC. These fraudulently obtained funds had been paid by HMRC into their Nationwide accounts during 2020 and 2021, with £26.01m received over 8 days in the calendar month before the freezing orders. A couple of months later in 2021 HMRC obtained forfeiture orders against five Nationwide accounts held by Customer A and seized some £26.54m from these accounts. However, some £820,687 remains unrecovered.

4.62 Customer A applied for their first account with Nationwide on 25 April 2014. When they opened their first account, Customer A stated that they had lived at the address they provided since 1 January 2007 and that they were an owner-occupier. However, the address given was self-evidently not a residential property (i.e. the address name contained "*office*"). Customer A declared an income of £80,000 and advised that they were employed by Company X. Customer A was rated as standard risk at onboarding.

4.63 In the period prior to 2020, Customer A commenced a number of applications to Nationwide for current accounts, savings accounts and credit cards.

(a) Most of the applications were never completed by Customer A. All credit card applications were automatically declined for credit reasons (with one

application in 2014 being declined additionally because Customer A's address was not confirmed).

(b) All but one of the applications were made under the same customer profile.

(c) One account application made by Customer A in July 2019 stated that they were a new customer to Nationwide and provided a different address to that which was held for them. This created a new customer profile on Nationwide's Customer Information System which required Customer A to provide ID&V to enable the July 2019 application to proceed. As Customer A never provided that ID&V, the account was never opened, and the application remained in abeyance until it was ultimately declined in October 2019. That action to decline the application coincided with Nationwide declining two Flex Basic account applications from other prospective customers as linked to a fraud network. The address used in those two applications was the same as that used by Customer A in his July 2019 application.

(d) Subsequently, in July 2020, a further account application made by Customer A was declined as a result of a name and address fraud network match alert flagging the earlier July 2019 application. This was escalated internally on the basis that Customer A was suspected of being part of a fraud network of non-UK nationals living at the same address. It was also noted that Customer A had at that time received a substantial amount in JRS payments (over £100,000), in circumstances where he had previously declared an annual income of £80,000 and he had not previously transacted

4.64 In 2021, after Nationwide became aware of Customer A's fraudulent attempts to obtain JRS funds, they investigated the information provided by Customer A when they opened their first account and their subsequent account applications and found that all of them contained material falsehoods regarding their address, occupancy status and income. Nationwide's investigation established that, during their 7-year relationship with Nationwide:

(a) Customer A commenced over 20 account applications to Nationwide for current accounts, savings accounts and credit cards. Many of these account applications were either abandoned by Customer A or denied by the Firm due to Customer A having a low credit score, their address being linked to a fraud network or that the Firm was unable to confirm their address;

(b) There were a number of interlinked applications involving family members. They all shared the same email provider and addresses. The majority of these were declined before the accounts were opened;

(c) Customer A communicated with the Firm several times when one of their overdrawn accounts were referred to a debt collection agency; and that

(d) Customer A had made material changes to their address 5 times (and 11 times in total). It was further established that Nationwide's systems had not flagged that:

(i) none of the addresses were residential and 2 contained indications that they were virtual office addresses such as mail redirection services, office accommodation or short-term storage facilities

(e.g. the addresses contained words such as 'storage' and 'office'); and

(ii) one of the addresses provided by Customer A was heavily linked to company registration activity with 59,666 companies linked to it.

4.65 Accordingly, it is the Authority's opinion that from at least late 2019: (i) the Firm had opportunities to review their relationship with Customer A; and (ii) given the potential red flags, that its systems and controls should have prompted a review of the unusual activities and consideration of the associated financial crime risks.

The JRS payments and interactions with Customer A from March 2020

4.66 On 20 March 2020, after the beginning of the COVID-19 pandemic, the UK government announced the JRS Scheme. Over a 14-month period, a total of some £27.36m was paid into Customer A's FlexBasic account from HMRC.

4.67 Between March and July 2020, Customer A received c.£100,000 of JRS payments. In July 2020, Nationwide's systems connected the main customer profile for Customer A to a suspected fraud network. This led to an internal suspicious activity report being made about Customer A and his receipt of JRS payments. When this internal suspicious activity report was reviewed, it was assessed not to be suspicious. There appears to have been inadequate consideration as to why JRS funds, which would typically have been paid to a limited company for onwards payment to employees (and not to an individual payee such as Customer A), were paid into a personal current account. Furthermore, red flags, such as large payments to a well-known MSB from an account that did not have significant transactional activity before April 2020, were not taken into consideration. If Customer A's other account applications, their CDD information and their transaction history had been included in the Firm's assessment of their activities, this would have significantly increased the likelihood of Nationwide making an external report at this time (i.e. several months earlier than it did). In turn, this would potentially have helped to prevent further fraudulent activity. The Authority considers that the flawed assessment in relation to the internal report is an example of the risks arising from seeking to assess whether potential business activity is suspicious without access to business CDD information, as referred to at paragraph 4.50.

4.68 Nationwide's own 'Lessons Learnt' review in respect of Customer A (which was referenced in the Nationwide 's 2021 MLRO Report) concluded that a more robust control environment would have significantly increased the likelihood of the Firm identifying Customer A's activity earlier and exiting the relationship.

4.69 Further, this was in the context of Nationwide's terms and conditions contractually prohibiting customers from using their personal current accounts for business purposes. The absence of a Business Use framework until 2021, impacted adversely the Firm's ability to manage unusual activity appropriately.

4.70 During this period Nationwide's Internal Audit team was working on a project regarding business use of current accounts. As part of this project, the Firm's Internal Audit team was considering JRS payments as a business use indicator. They identified Customer A's account as being the customer account having received the largest JRS credits. On 17 December 2020, upon review of Customer A's account activity, they raised an internal report of suspicious transactions, noting that the account had

received significant JRS payments which were transferred abroad using a MSB and concluding that these JRS payments may have been claimed fraudulently. In January 2021, Nationwide alerted relevant authorities based on the December 2020 internal report.

4.71 The Authority has seen no evidence that, in light of forming a suspicion in January 2021 that Customer A was engaged in illegal activities (and using his personal current account for such purposes), the Firm took this opportunity to gather further CDD to verify that Customer A was a legitimate customer. The Firm also did not take any steps to restrict their account or to exit the relationship. Had Nationwide done so, Customer A would not have been able to receive any further fraudulently obtained JRS funds into their Nationwide accounts.

4.72 On 10 March 2021, Customer A contacted the Firm using BBM. The Firm's call centre considered their account activity as suspicious and raised a further internal report of suspicious activity. However, the AML Operations team concluded that as the Firm had alerted the relevant authorities within the previous three months in respect of the same type of activity, no further notification was required, in accordance with Nationwide's internal procedure at the time (the 'three-month rule').

4.73 Although the three-month rule was designed to reduce duplicative reporting, it was inappropriate. There is a statutory obligation to report any knowledge or suspicions of money laundering to the NCA by submitting a SAR as soon as is reasonably practicable after the information is received. There is no qualification in the relevant legislation which allows a firm to disregard it simply because previous suspicions were raised within a period of 3 months in respect of the same activity.

4.74 Also in March 2021, Nationwide was made aware of HMRC's interest in Customer A's account activity. During the same period that Customer A received the JRS payments, they also applied for 3 current and 3 savings accounts. All the current account applications were declined or blocked, due to a fraud alert. However, Nationwide allowed the 3 savings accounts to be opened in April, May and June 2021, including one savings account which was opened two days after the receipt of the first extraordinarily large, unusual JRS payment. Two of the savings accounts received a significant amount, by way of internal account transfers, of the JRS payments from the FlexBasic account into which HMRC had paid the JRS payments.

4.75 Only one of Customer A's applications resulted in an internal SAR being made (see paragraph 4.67 above). As such, despite having several opportunities to do so, the Firm failed to act appropriately. In the Authority's opinion, there were gaps in the Firm's control environment and, where there were controls in place, these either did not operate effectively or were not appropriately actioned.

Account activity and transaction monitoring

4.76 As explained at paragraph 4.39 above, in 2019 Nationwide commenced a project to review and improve its transaction monitoring systems and controls, which had by that point been acknowledged internally as "*far too narrow*". Despite this remedial work, Nationwide's transaction monitoring controls did not alert it of the suspicious and unusual activity on Customer A's accounts until the month following the receipt of approximately £26m of JRS payments.

4.77 In terms of account behaviour, Customer A did not conduct any branch-based transactions and all activity was done by on-line banking or through the use of their debit card. The FlexBasic account that received the JRS funds showed very little activity before March 2020. The only external credits received before the JRS payments were from what appears to be a payment service company for £40.86 and no salary credits were ever received into the account.

4.78 Upon receipt of the JRS funds, Customer A subsequently dispersed these funds, by way of internal account transfers, across the several savings accounts in their name and into a previously overdrawn personal current account. Customer A also transferred some of the JRS funds externally. From 30 April 2021, the total value of withdrawals from Customer A's accounts were £1.17m. The bulk of the payments were made to a payment service which allows rapid money transfer abroad and a prominent MSB. However, a total of £250,000 of the payments to the payment service company were returned as visa credits over an 11 day period a month or so later. There were also a number of payments made to American and UK Government Departments, American accountancy and law firms and payments to Companies House.

4.79 Automated transaction monitoring alerts applicable to Customer A's accounts were triggered at the beginning of the month following the receipt of approximately £26m of JRS payments into their account, which was also after a production order from HMRC was received and steps had been initiated to freeze all of Customer A's accounts. The Firm's transaction monitoring alerts are generated at the beginning of the month, based on retrospective transactional activity in the previous month. AML Operations were then required to investigate alerts within 20 working days. This means that an alert may not actually be triggered until several weeks after the activity occurs.

4.80 Prior to 2021 the Firm's transaction monitoring rules were limited in their ability to identify transactions which deviated from a given customer's historical activity or anticipated activity. This compromised Nationwide's ability to assess effectively the legitimacy of particular transactions on customer accounts and generate appropriate alerts. During the Relevant Period, Nationwide did deploy a '£1m+ payments' rule which triggered manual referrals to AML Operations, however this only identified CHAPS/Swift and SEPA payments over £1m and not BACS payments. All JRS payments to Customer A's accounts were made via BACS. This rule was an inadequate control mechanism, especially if customers were using their personal current accounts for business use when they were prohibited from doing so under the Firm's terms and conditions. There was also no real-time fraud monitoring of incoming payments.

4.81 In the Authority's opinion, a more robust control environment would have significantly increased the likelihood of the Firm identifying Customer A's activity earlier and, if so, potentially exiting the relationship in late 2020 or early 2021.

Response to Suspicious activity reports

4.82 Although the activity on Customer A's accounts did raise some internal suspicious activity reports by staff members, as described above these reviews were not always dealt with adequately. In particular, the absence of a Business Use Framework until 2021 may have impacted adversely the Firm's review of at least the first internal suspicious activity report in 2020 and the actions taken in response to the other

internal suspicious activity reports. If Customer A's other account applications, their CDD information and their transaction history had been included in the Firm's assessment of their activities this would have significantly increased the likelihood of Nationwide identifying the suspicious activity much sooner and this would have helped to prevent further fraudulent activity.

4.83 In November 2019 the Firm prepared internal draft guidance on which kinds of customer account use may indicate business use and therefore require account closure. It is notable that the criteria for closure of accounts which would lead to an exit included criteria that would have been relevant had they been applied to the Firm's relationship with Customer A.

4.84 If the Firm had implemented and enforced this guidance it is very likely that they would have exited their relationship with Customer A before at least some of their fraudulent claims for JRS funds. The Authority considers that this demonstrates that the absence or inadequacy of appropriate AML systems and controls (including in relation to unauthorised business use) adversely impacted the Firm's ability to manage the risk of being used as a vehicle for financial crime.

5. FAILINGS

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

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

5.3 Further, rules in SYSC required Nationwide: (i) to establish, implement and maintain adequate policies and procedures sufficient to ensure the firm's compliance with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime (SYSC 6.1.1R); and (ii) ensure its policies and procedures enable it to identify, assess, monitor and manage money laundering risk, and are comprehensive and proportionate to the nature, scale and complexity of its activities (SYSC 6.3.1R).

5.4 Nationwide breached Principle 3 and SYSC rules 6.1.1R and 6.3.1R in that, during the Relevant Period there were deficiencies in Nationwide's AML systems and controls which had a material impact on its ability to monitor effectively its customer relationships as set out in this Notice:

(a) Nationwide did not have effective systems for refreshing CDD and for conducting customer risk assessments. At the start of the Relevant Period, Nationwide's system for individually risk assessing customers was an unsophisticated, interim solution, with a formal scoring process still being developed. Unless the customer fell into certain very limited categories (one of which was if Nationwide's systems flagged that the customer had been charged or convicted of a financial crime offence), they were automatically classed as standard risk. This led to an exceptionally low number of only some 2,000 customers being categorised as high risk (out of up to 18 million customers). Before the Relevant Period, Nationwide had commenced its RRP project which was intended to introduce a system which would automatically assess the financial crime risk presented by customers, and in the interim added further risk assessment triggers. Likewise, measures to gather enhanced CDD were

introduced. However, the RRP system was not fully operational until early 2019. In May 2019, Nationwide Internal Audit had conducted a review of the CDD data which the RRP customer risk assessment utilised, and how the system's defined criteria were being applied. The review was conducted by Nationwide's Internal Audit function against the risk that Nationwide was unable to identify high risk customers and therefore take appropriate steps to manage those relationships. Internal Audit concluded that the controls over the quality of data for the RRP system required "*significant improvement*", partly due to discrepancies in the number of records across systems utilised by the RRP. Relatedly, Internal Audit also identified a lack of oversight to ensure the quality of data being transferred between those systems. These issues, which culminated in 44,957 customer accounts having not being fed into Nationwide's customer risk assessment tool, were subsequently investigated and resolved (with most of the outstanding accounts being fed into the risk assessment tool by late 2019). It was not until August 2020 that the additional data items (a number of which were pertinent to the Firm's obligations under the MLRs) were fed into Nationwide's RRP system, and not until April 2021 that the enhanced data was considered for customer risk assessment purposes.

Further, the measures introduced by Nationwide to gather enhanced CDD applied only to brand new customers and existing customers seeking new products, representing only a small percentage of customers. As at the end of the Relevant Period, Nationwide continued to hold concerns about gaps in CDD for existing customers, which were significant in some cases, including in relation to retrievable verification evidence. These gaps meant that it was not always possible to complete a customer risk assessment fully. It was not therefore possible for Nationwide to be confident that all high risk customers had been identified. Notably, following improvements to the Firm's customer risk assessment tool as part of the FCTP, Nationwide identified that over 18,000 customers (in addition to those that fell into certain very specific categories, for example they were flagged as having been charged or convicted of a financial crime) were potentially high risk. Notwithstanding improvements made during the Relevant Period, the deficiencies in Nationwide's customer risk assessment architecture (in particular until August 2020) were relevant to its monitoring of many of its customer relationships and had a potentially material impact on its ability to monitor effectively customer relationships and within the risk appetite approved by Nationwide's board;

(b) Aside from customers already assessed as high risk (which in mid-2020 appears to have amounted to only some 2,000 customers), and (for the majority of the Relevant Period) in breach of its own policies, Nationwide had no process for undertaking either periodic or event-driven AML reviews of a substantial proportion of its customer relationships. . The absence of these controls throughout the Relevant Period prolonged the time it took for existing customer relationships to be reviewed and their CDD refreshed, so compromising Nationwide's ongoing understanding of its customers, particularly its existing customers who had been onboarded prior to previous uplifts in CDD measures, had not opened new accounts since, and were classified as standard or low risk before the introduction of the RRP (which, as above, represented a substantial proportion of its customer base);

(c) The deficiencies in Nationwide's risk assessment and CDD procedures impacted on its transaction monitoring system as a means by which inconsistent or unusual customer behaviour could be detected, investigated and addressed on a risk-orientated basis. However, Nationwide's system for monitoring customer transactions for unusual activity was inadequate and ineffective. In February 2017 when an internal report noted that a recent FCA final notice against a major bank had highlighted the need for an effective, tuned and auditable transaction monitoring solution which took into account the CDD captured from customers. It referred to a 2016 internal review of the system which concluded at the time it was compliant with legal requirements but that there were weaknesses relating to data integrity, governance and understanding of rule amendments and design. Nationwide undertook work in response and engaged compliance consultants to assist in developing the system including from 2019, to outline key improvements required and a multi-year 'roadmap' to deliver them. This placed Nationwide's transaction monitoring maturity at stage two out of five (as compared with amalgamated peers, which were placed at four – a stage it was assessed in it that Nationwide would not reach until 2021). Other than for high risk customers, Nationwide's existing transaction monitoring rules applied uniformly across its entire personal account customer base and a customer's individual circumstances (such as the CDD gathered) would only be taken into account if a rule triggered. The review also suggested that Nationwide needed to introduce peer-based and additional behavioural rules. A review in 2020 of the planned new rules described the existing rules as narrow in focus, limiting Nationwide's ability to cover the full range of money laundering risks to which Nationwide it was exposed. The review recommended consideration be given to daily or weekly (as opposed to monthly) application of rules to align with the general direction of travel of the industry. Concerns that alert thresholds for the pre-existing rules were set very high were also expressed by a senior member of Nationwide's financial crime function in 2020. By the end of the Relevant Period, although improved by a significant programme of work, the system provided only partial coverage of the money laundering typology risks which Nationwide faced;

(d) The Authority considers that these weaknesses significantly impacted Nationwide's ability effectively to maintain an up-to-date understanding and records of all its current account customers and to monitor these customer relationships on an appropriate risk-sensitive basis, including scrutinising customer transactions to ensure that they were consistent with what Nationwide knew about the customer. In combination, this created material risks over a protracted period that unusual activity by customers might remain undetected and/or that customers moving into the 'high risk' category over the course of their relationship might not be identified and actively managed;

(e) There was a particularly high risk created by the above weaknesses in respect of customers who were using their personal current accounts for business activity in breach of Nationwide's terms and conditions throughout the Relevant Period. Nationwide's financial crime prevention controls for personal current accounts were not set up for business use (as Nationwide did not offer business banking current accounts for SMEs at any time during the Relevant Period). In particular:

(i) Nationwide's CDD measures were not calibrated to capture business characteristics and meant that Nationwide did not capture sufficient data on businesses (and in the event of the business being a legal entity other than the customer, their beneficial owners) to enable proper risk assessment, identification of customers operating in an industry or geographical area outside of Nationwide's risk appetite, and (if applicable) EDD or other similar issues;

(ii) Transaction monitoring controls were not designed to identify unusual and/or suspicious behaviours pertinent to businesses. Nor could they be because the Firm had not gathered the necessary information from businesses on their activities and expected account usage to establish what comprised normal and unusual behaviour. There was a risk that when business use did occur on accounts it would become normalised or generate false transaction monitoring alerts for review; and

(iii) Training and processes did not include sufficient guidance on how to investigate accounts with potential business use. It was accordingly recognised that unusual/suspicious activity could remain undetected and not reported when appropriate to the NCA.

(f) Whether to tolerate unauthorised business use of personal current accounts was a matter for Nationwide to decide. However, allowing accounts designed for personal use to be used for business, without effective mitigating controls through adequate policies and procedures, exacerbated Nationwide's AML monitoring weaknesses and created further risks across the customer lifecycle. The financial crime risk profile of SME banking customers is different from, and potentially higher than, that of personal customers due to factors such as the greater complexity involved in identifying corporate customers and monitoring their transactional behaviour, and the size and number of the transactions. These risks were material and created a consequential risk that unusual or suspicious business activity could remain undetected and not reported to the NCA;

(g) From October 2016 to September 2017 the Firm's staff carried out some initial work to assess the number of accounts subject to unauthorised business use and to develop an outline process for investigating and (where appropriate) closing those accounts. In September 2017 a decision was taken to temporarily tolerate the risks on the basis that Nationwide was planning to launch its own SME business banking product to which personal current accounts being used for business purposes could be migrated. Over a period of approximately two and a half years, the toleration decision was revisited but remained in place. In the Authority's view, that was inappropriate. Nationwide's financial crime prevention controls for personal current accounts were not set up for business use. It had no settled methodology for calculating the number of personal current accounts subject to unauthorised use, and no framework for dealing with them. Its controls for maintaining an up to date understanding of, and monitoring, its personal current account customers were not operating effectively. Whilst some work continued in the interim to understand and address the business use risks, insufficient mitigation measures were implemented. It was not until around April 2020, when the planned business banking product launch was discontinued, that impactful steps were then taken

to develop a model to identify business use and create a formal written framework for defining, investigating, managing and, if appropriate, exiting unauthorised business customers; and

(h) Nationwide was aware during the Relevant Period of the wider monitoring weaknesses described above, and progressed or implemented a number of workstreams aimed at remediating or uplifting these matters, including through an ongoing project aimed at ensuring compliance with the MLRs 2017. However, these workstreams did not address the weaknesses in a sufficiently effective or timely manner and from 2020 Nationwide instructed a firm of compliance consultants to undertake a more comprehensive analysis of the effectiveness of its financial crime prevention framework and make recommendations on a target operating model. This produced a greater understanding of the work required to address weaknesses in the framework and resulted in the firm commencing from around June 2021 a more comprehensive financial crime transformation programme.

5.5 Because of these weaknesses in its AML control framework, policies and procedures, which it did not address in a timely manner, Nationwide was unable to effectively identify, assess, monitor or manage its money laundering risk in respect of its personal current account customers (with an increased impact in respect of customers using their personal current accounts for business activity); it also did not adequately implement policies and procedures to ensure its compliance with its obligations to counter the risk that the firm might be used to further financial crime. As a result, there was an unacceptable risk throughout the Relevant Period that inconsistent or unusual activity by customers might remain undetected and unaddressed. In addition, despite various opportunities, Nationwide failed to identify unusual activity on the part of Customer A in particular, who fraudulently claimed and received from HMRC into their Nationwide accounts 24 JRS furlough payments totalling £1.35m over the course of 13 months and then £26.01m over 8 days between 2020 and 2021. The Authority considers that those monies represented the proceeds of crime and that Customer A used their account to launder those funds. The Authority also considers that the Firm's systems and controls should have prompted a review of the unusual activities and consideration of the associated financial crime risks from at least late 2019.

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 2020, 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 Nationwide 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 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 gross revenue generated by Nationwide from its customers' personal current accounts during the Relevant Period is indicative of the harm or potential harm caused by its breach. The Authority considers that Nationwide's relevant revenue for this period to be £1,659,270,000.

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

Level 1 – 0%
Level 2 – 5%
Level 3 – 10%
Level 4 – 15%
Level 5 – 20%

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

(a) 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;

(b) Financial crime was facilitated, occasioned or otherwise attributable to the breach;

(c) 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:

(a) "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 £1,659,270,000.

6.11 Step 2 is therefore £248,890,500.

6.12 Pursuant to DEPP 6.5.3(3)G, the Authority may decrease the level of penalty arrived at after applying Step 2 of the framework if it considers that the penalty is disproportionately high for the breaches concerned. Notwithstanding the serious and long-running nature of the breaches, the Authority considers that the level of penalty would nonetheless be disproportionate if it were not reduced and should be adjusted.

6.13 In order to achieve a penalty that (at Step 2) is proportionate to the breach, and having taken into account previous cases, the Step 2 figure is reduced to £57,244,815.

Step 3: aggravating and mitigating factors

6.14 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.

6.15 The Authority considers the following factors aggravate the breach:

(1) Since 1990, JMLSG published detailed written guidance on AML controls. During the Relevant Period, JMLSG provided guidance on compliance with the regulatory requirements in the Handbook and evolving practice in the financial services industry.

(2) Before, or during, the Relevant Period the Authority has issued various written guidance in relation to AML controls to remind firms of the importance of having robust systems and controls in place to ensure compliance with regulatory requirements. These have included, in March 2008 the Authority's publication of 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" (included examples of good and poor industry practice and reminded firms that their approach to AML should be aligned with the JMLSG Guidance), its publication in December 2011 of "Financial Crime: A Guide for Firms" (which highlighted the need to conduct adequate CDD checks, perform ongoing monitoring and carry out EDD measures and enhanced ongoing monitoring when handling higher risk situations), and its publication in April 2015 of "Financial crime: a guide for firms Part 1: A firm's guide to preventing financial crime" (which set out examples of good and poor industry practice to assist firms).

(3) The Authority has published a number of notices against firms for AML weaknesses both before and during the Relevant Period, including in respect of Coutts & Company in March 2012, Habib Bank AG Zurich in May 2012, Turkish Bank (UK) Ltd in July 2012, EFG Private Bank Ltd in April 2013, Guaranty Trust Bank (UK) Ltd in August 2013, Standard Bank Plc on 22 January 2014, Barclays Bank Plc on 25 November 2015, Deutsche Bank AG on 30 January 2017, Standard Chartered Bank on 5 February 2019 and Commerzbank AG on 17 June 2020.

6.16 Consequently, Nationwide was aware, or ought to have been aware, of the importance of establishing, implementing and maintaining adequate AML systems and controls.

6.17 The Authority considers that the following factors mitigate the breach:

(a) Since the end of the Relevant Period, Nationwide has taken remedial steps in respect of its financial crime framework through the FCTP. This has included investing significantly in additional resource and capability to manage financial crime risk across its business (including aspects of its control framework which do not form part of the subject matter of this Notice).

6.18 The Authority acknowledges that Nationwide cooperated fully with the Authority throughout the course of its investigation. However, this reflects the Authority's expectations of authorised firms and is not a factor that mitigates the breach.

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

6.20 The Step 3 figure is therefore £62,969,297.

Step 4: adjustment for deterrence

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

6.22 The Authority considers that the Step 3 figure of £62,969,297 represents a sufficient deterrent to Nationwide and others, and so has not increased the penalty at Step 4.

6.23 Step 4 is therefore £62,969,297.

Step 5: settlement discount

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

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

6.26 Step 5 is therefore £44,078,500 (rounded down to the nearest £100).

Penalty

6.27 The Authority therefore hereby imposes a total financial penalty of £44,078,500 on Nationwide for breaching Principle 3.

7. PROCEDURAL MATTERS

7.1 This Notice is given to Nationwide 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 Nationwide to the Authority no later than 29 December 2025.

If the financial penalty is not paid

7.4 If all or any of the financial penalty is outstanding on 30 December 2025 (being the next business day post the due date specified in 7.3 above), the Authority may recover the outstanding amount as a debt owed by Nationwide 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 Nationwide or 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 Final Notice relates as it considers appropriate.

Authority contacts

7.7 For more information concerning this matter generally, contact Calum Duncan at the Authority (email: Calum.Duncan@fca.org.uk / 0207 066 2536).

Dharmesh Gadhavi
Head of Department
Financial Conduct Authority, Enforcement and Market Oversight Division

ANNEX A

RELEVANT STATUTORY AND REGULATORY PROVISIONS

1. Relevant Statutory Provisions

The Financial Services and Markets Act 2000

1.1 In discharging its general functions, the Authority must, so far as reasonably possible, act in a way which is compatible with its strategic objective and advances one or more of its operational objectives (section 1B(1) of the Act). The Authority's strategic objective is ensuring that the relevant markets function well (section 1B of the Act). The Authority has three operational objectives (section 1B(3) of the Act).

1.2 The Authority's statutory objectives, set out in section 1B(3) of the Act, include the integrity objective (protecting and enhancing the integrity of the UK financial system). 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).

1.3 Section 206(1) of the Act provides:

"If the appropriate regulator considers that an authorised person has contravened a relevant requirement imposed on the person, it may impose on him a penalty, in respect of the contravention, of such amount as it considers appropriate."

Relevant Regulatory Provisions

1.4 The relevant regulatory provisions (and guidance) in force during the Relevant Period are set out below.

Principles for Businesses

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

1.6 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)

1.7 SYSC 6.1.1R states:

"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."

1.8 SYSC 6.3.1R states:

"A firm must ensure the policies and procedures established under SYSC 6.1.1R include systems and controls that:

(a) enable it to identify, assess, monitor and manage money laundering risk, and

(b) are comprehensive and proportionate to the nature, scale and complexity of its activities.

1.9 SYSC 6.3.4G states:

"A firm may also have separate obligations to comply with relevant legal requirements including the Terrorism Act 2000, the Proceeds of Crime Act 2002 and the Money Laundering Regulations."

1.10 SYSC 6.3.5G states:

"The FCA when considering whether a breach of its rules on systems and controls against money laundering has occurred, will have regard to whether a firm has followed relevant provisions in the guidance for the United Kingdom financial sector issued by the Joint Money Laundering Steering Group."

DEPP

1.11 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.

The Enforcement Guide

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

1.13 During the Relevant Period, Chapter 7 of the Enforcement Guide set out the Authority's approach to exercising its power to impose a financial penalty.

JMLSG Guidance

1.14 The purpose of the Joint Money Laundering Steering Group (JMLSG) Guidance is to outline the legal and regulatory framework for anti-money laundering/countering terrorist financing requirements and systems across the financial services sector. It provides interpretation on the requirements of the relevant law and legislation and indicates good industry practice through a proportionate, risk-based approach. It also assists firms to design and implement the systems and controls necessary to mitigate the risks of the firm being used in connection with money laundering and the financing of terrorism.

1.15 The JMLSG Guidance is periodically updated. Changes to the following relevant provisions during the Relevant Period are indicated below.

Relevant extracts from the JMLSG Guidance

Part I - Chapter 4 – Risk-based Approach

1.16 Paragraph 4.13 stated (until 13 December 2017):

"Whatever approach is considered most appropriate to the firm's money laundering/terrorist financing risk, the broad objective is that the firm should know at the outset of the relationship who their customers are, where they operate, what they do, their expected level of activity with the firm and whether or not they are likely to be engaged in criminal activity. The firm then should consider how the profile of the customer's financial behaviour builds up over time, thus allowing the firm to identify transactions or activity that may be suspicious."

1.17 Paragraph 4.2 stated (from 13 December 2017 onwards):

"*Whatever approach is considered most appropriate to the firm's money laundering/terrorist financing risk, the broad objective is that the firm should know at the outset of the relationship who its customers (and, where relevant, beneficial owners) are, where they operate, what they do, their expected level of activity with the firm. The firm then should consider how the profile of the customer's financial behaviour builds up over time, thus allowing the firm to identify transactions or activity that may be suspicious.*"

1.18 Paragraph 4.51 stated (until 13 December 2017):

"*Where the risks of ML/TF are higher, firms must conduct enhanced due diligence measures consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether these transactions or activities appear unusual or suspicious. Examples of EDD measures that could be applied for higher risk business relationships include:*

- *Obtaining, and where appropriate verifying, additional information on the customer and updating more regularly the identification of the customer and any beneficial owner*
- *Obtaining additional information on the intended nature of the business relationship*
- *Obtaining information on the source of funds or source of wealth of the customer*
- *Obtaining information on the reasons for intended or performed transactions*
- *Obtaining the approval of senior management to commence or continue the business relationship*
- *Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination*

1.19 Paragraph 4.62 stated (from 13 December 2017 onwards):

"Where the risks of ML/TF are higher, firms must conduct enhanced due diligence measures consistent with the risks identified.

(a) In particular, they must:

- *as far as reasonably possible, examine the background and purpose of the transaction; and*

- *increase the degree and nature of monitoring of the business relationship, in order to determine whether these transactions or activities appear unusual or suspicious.*

(b) Examples of other EDD measures that, depending on the requirements of the case, could be applied for higher risk business relationships include:

- *Obtaining, and where appropriate verifying, additional information on the customer and updating more regularly the identification of the customer and any beneficial owner*
- *Obtaining additional information on the intended nature of the business relationship*
- *Obtaining information on the source of funds or source of wealth of the customer*
- *Obtaining information on the reasons for intended or performed transactions*
- *Obtaining the approval of senior management to commence or continue the business relationship*
- *Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination*
- *Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards".*

Part I - Chapter 5 - Customer Due Diligence

Application of CDD measures

1.20 Paragraph 5.3.15 (until 13 December 2017) / 5.3.18 (from December 2017 onwards) stated:

"As risk dictates […] *firms must take steps to ensure that they hold appropriate information to demonstrate that they are satisfied that they know all their customers. Where the identity of an existing customer has already been verified to a previously applicable standard then, in the absence of circumstances indicating the contrary, the risk is likely to be low. A range of trigger events, such as an existing customer applying to open a new account or establish a new relationship, might prompt a firm to seek appropriate evidence."*

Enhanced Due Diligence

1.21 Paragraph 5.5.1 stated:

"A firm must apply EDD measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. As part of this, a firm may conclude, under its risk-based approach, that the information it has collected as part of the customer due diligence process […] *is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer, the customer's beneficial owner, where applicable, and the purpose and intended nature of the business relationship."*

1.22 Paragraph 5.5.2 stated:

"As a part of a risk-based approach, therefore, firms should hold sufficient information about the circumstances and business of their customers and, where applicable, their customers' beneficial owners, for two principal reasons:

- *to inform its risk assessment process, and thus manage its money laundering/terrorist financing risks effectively; and*
- *to provide a basis for monitoring customer activity and transactions, thus increasing the likelihood that they will detect the use of their products and services for money laundering and terrorist financing."*

1.23 Paragraph 5.5.6 stated:

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

1.24 Paragraph 5.5.7 stated:

"The availability and use of other financial information held is important for reducing the additional costs of collecting customer due diligence information and can help increase a firm's understanding of the risk associated with the business relationship. Where appropriate and practical, therefore, and where there are no data protection restrictions, firms should take reasonable steps to ensure that where they have customer due diligence information in one part of the business, they are able to link it to information in another."