FINAL NOTICE

To: Metro Bank Plc

Reference
Number: 488982

Address: 1 Southampton Row, London, WC1B 5HA

Date: 12 November 2024

1. ACTION

1.1. For the reasons given in this Final Notice, the Authority hereby imposes on Metro Bank Plc ("Metro" or the "Bank") a financial penalty of £16,675,200 pursuant to section 206 of the Act.

1.2 Metro 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 £23,821,700 on Metro.

2. SUMMARY OF REASONS

2.1. Metro is an authorised firm that is regulated by the Authority and the Prudential Regulation Authority ("PRA"). Metro was established in 2010. It offers retail, business, commercial and private banking services.

2.2. The Authority has the operational objective of protecting and enhancing the integrity of the UK financial system. Money laundering through UK financial institutions undermines the integrity of the UK financial system.

2.3. Under the Authority's rules, financial institutions operating in the UK are responsible for minimising their risk of being used for criminal purposes, including the risk of being used to facilitate money laundering or terrorist financing. 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. They must also comply with the applicable Money Laundering Regulations.

2.4. The Money Laundering Regulations 2007 (the "Regulations") were in effect during the Relevant Period, namely from 6 June 2016 to 17 December 2020. The Regulations required firms, amongst other things, to conduct ongoing monitoring of business relationships and to establish and maintain appropriate and risk-sensitive policies and procedures relating to ongoing monitoring. The purpose of conducting ongoing monitoring is to scrutinise transactions in order to ensure that they are consistent with the firm's knowledge of the customer and to identify patterns of behaviour which appear characteristic of either money laundering or terrorist financing and which, after analysis, may lead to suspicions of money laundering or terrorist financing. Ongoing monitoring can also assist firms in knowing their customers, the assessment of risk and provide assurance that the firm is not being used to facilitate financial crime.

2.5. On 6 June 2016 (the start of the Relevant Period), Metro implemented an Automated Transaction Monitoring System ("ATMS") to monitor customer transactions. As it transpired, there were serious deficiencies in relation to the set-up, operation and oversight of the ATMS which were not identified and/or remedied by Metro within an acceptable period of time. Over the Relevant Period, as a result of the failings set out in this Notice, Metro failed to monitor over 60 million transactions (circa 6.0% of the total transaction volume) with a value of over £51 billion (circa 7.6% of the total transaction value).

2.6. Although the Authority acknowledges that many of these transactions were subsequently reviewed as part of a remediation exercise, the Lookback Review, this process was only completed a number of years after the event in 2022. The remediation resulted in Metro submitting 153 suspicious activity reports and 43 notices to customers closing their accounts. This was in addition to the 1,403 suspicious activity reports in respect of customers included in the Lookback Review and which were submitted prior to the Lookback Review.

2.7. Data for the ATMS originated from Metro's Data Store ("DS"), which was a separate database within the Bank that contained a near real-time view of the data within Metro's core banking records system. Metro decided that the data feed process to the ATMS should occur from the DS for a number of reasons, including operational resilience. In order for monitoring to take place, the DS needed to feed Customer Records (comprising details about the customer), Account Records (comprising details of the customer's account(s)) and Transaction Records (comprising details about the customer's account transaction(s)) into the ATMS.

The Time Stamp Code Logic Error

2.8. Almost three years later, on 17 April 2019, during testing of an upgrade to Metro's core banking records system, an issue referred to in this Notice as the "Time Stamp Code Logic Error" was identified by the Bank. The Bank notified the Authority about this issue on 29 May 2019.

2.9. In essence, the Time Stamp Code Logic Error meant that a large number of transactions had not been fed into the ATMS for ongoing monitoring, since its implementation on 6 June 2016. This issue was caused by an error in the data extraction methodology from the Bank's DS for loading into the ATMS, which caused certain Transaction Records to be rejected by the ATMS. Specifically, where a customer had opened an account and transacted on the same day, the associated Account Record was not included in the data feed, and therefore those Transaction Records and ensuing Transaction Records were rejected by the ATMS until there was an update to the Account Record, whereupon the ATMS could reconfigure. Over an approximately three-year period from Metro's implementation of the ATMS, the Time Stamp Code Logic Error impacted in the region of 166,000 accounts, meaning that over 46.5 million transactions related to those accounts with an associated value of over £31.5 billion had not been monitored.

2.10. A tactical fix to remedy the Time Stamp Code Logic Error was implemented on 21 July 2019. Following application of the fix, for transactions intended for monitoring by the ATMS, at least 99.7% of Transaction Records were consistently fed into the ATMS, however Metro was not aware of this (for the reasons summarised in paragraphs 2.12 and 2.14) until after the Relevant Period.

2.11. The failure by Metro to identify the Time Stamp Code Logic Error in a timely manner arose, in part, as a result of the fact that, before the Lookback Review in July 2019,Metro did not check the completeness of data fed into the ATMS. Metro performed a number of ad hoc reconciliations over the course of 2020, however these did not relate to Transaction Records. These reconciliations were inadequate in the absence of a formal procedure for checking the completeness of the data (including Customer, Account and Transaction Records) in the ATMS on an ongoing basis. Prior to 17 December 2020, Metro failed put in place an effective reconciliation process between the DS and the destination ATMS in order to ensure that all Customer, Account and Transaction Records were loading correctly. This failure to check the completeness of data fed into the ATMS during the Relevant Period significantly impacted Metro's ability, on an ongoing basis, to identify which Customer, Account and Transaction Records were sent, or not sent, to the ATMS and consequently its ability to ensure that all of these records were monitored appropriately.

2.12. On 17 December 2020 (the end of the Relevant Period), the DS commenced sending daily "count files" to the ATMS. The count files included figures for all Customer, Account and Transaction Records, and enabled Metro to compare the total number of records received by the ATMS, plus the records rejected by the ATMS and placed into Bad Data folders, to the total number of records sent to the ATMS from the DS, on an ongoing basis. Where the totals did not match, emails were generated and sent to Financial Crime Operations in order to alert them to the disparity. Prior to this control being implemented, Metro had no mechanism for checking on an ongoing basis whether all records that were intended to be monitored by the ATMS were successfully received by the ATMS from the DS.

Bad Data

2.13. Metro also failed to put in place adequate systems and controls for managing an issue which was referred to internally as "Bad Data" and its "exceptions process" which was meant to deal with Bad Data was inadequate. In this regard, there were rules within the ATMS to prevent data loading where there were data quality issues, such as missing or incomplete data or a failure to meet prescribed criteria. Where a mandatory field was missing, the whole data record would be rejected by the ATMS and where a non-mandatory field was missing, the record might be rejected in part. "Bad Data" (as referred to within Metro) was the term used for any Customer, Account and Transaction Records that had been rejected from the ATMS. For Customer Records, these could be new records or updates to existing records.

2.14. The records which were rejected from the ATMS as Bad Data were placed into Bad Data folders, however Metro failed to put into place a regular review process for the Account and Transaction Records in the Bad Data folders, which were only intermittently reviewed as part of wider work to understand the Bad Data issues. In addition, it was only on 14 December 2020, when Metro implemented a fix to remove internal transactions, in respect of which monitoring was not required, from the data feed from the DS into the ATMS, that the Bank had clear visibility of the true volume of customer transactions (as opposed to internal transactions) being rejected by the ATMS for the first time since the ATMS went live in June 2016.

2.15. Whilst there was an "exceptions process" within Metro which was meant to deal with one aspect of Bad Data, namely rejected Customer Records, a lack of adequate systems and controls for managing Bad Data and deficiencies in relation to the exceptions process meant that Customer, Account and Transaction Records that should have been routinely loaded into the ATMS but had been rejected, were not subject to ongoing monitoring either in a timely fashion or at all. Therefore, this impacted the generation of alerts in respect of suspicious or uncharacteristic account activity and exposed Metro to financial crime risk.

Oversight and Governance

2.16. Bad Data was recognised as a risk and a serious issue at comparatively less senior grades within Metro and individual staff members investigated and attempted to escalate this issue to more senior staff and Committees in 2017 and 2018. In particular, the issue was raised at Metro's Financial Crime Steering Group, which was responsible for overseeing financial crime issues, in January 2018 when it agreed to undertake a review of the issue. However, this decision was subsequently removed from the final minutes of the Financial Crime Steering Group's meeting with the intention of revisiting the issue once it was better understood, and it was not discussed again until April 2019 when the Time Stamp Code Logic Error was identified.

2.17. Members of Metro's Financial Crime Working Group ("Working Group"), which reported into the Financial Crime Steering Group, and the Financial Crime Operations Risk Board ("Operations Risk Board"), escalated the issue of Bad Data to senior staff in Metro in 2018. The risk in relation to this issue was passed to a more junior member of staff to liaise with a senior member of staff, although the Authority understands that Metro has no formal records to demonstrate that such an escalation took place. In any event, no substantive action was taken.

2.18. Metro instructed two external compliance firms, one at the end of 2018, and a second at the end of 2019. These external reviews enabled Metro better to understand the issues with its ATMS and to implement a remediation programme to improve the applicable controls. Metro subsequently made significant enhancements to the Bank's end-to-end architecture and data controls to ensure that the data fed into the ATMS is complete and accurate.

2.19. Metro was required, pursuant to Principle 3 of the Authority's Principles for Businesses, to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. Under the Authority's rules, Metro was also required to:

2.19.1. establish, implement and maintain adequate policies and procedures sufficient for ensuring the compliance of the firm with its obligations under the regulatory system and for countering the risk that it might be used to further financial crime;

2.19.2. ensure that those policies and procedures included systems and controls that (1) enabled it to identify, assess, monitor and manage money laundering risk and (2) were comprehensive and proportionate to the nature, scale and complexity of its activities; and

2.19.3. carry out a regular assessment of the adequacy of those systems and controls to ensure that they remained compliant.

2.20. During the Relevant Period, Metro failed to meet these requirements and, in doing so, breached Principle 3. In particular:

2.20.1. From the implementation of the ATMS on 6 June 2016, Metro failed to take any steps to check the completeness of data feeding into the ATMS, prior to identifying the Time Stamp Code Logic Error on 17 April 2019. Throughout the Relevant Period, Metro did not have controls in place to check, on an ongoing basis, that transactions that should have been monitored by the ATMS were being received by the ATMS and this contributed to the situation whereby the Time Stamp Code Logic Error continued for nearly three years before it was identified.

2.20.2. There was no adequate process in place to deal with Bad Data rejected from the ATMS: Metro did not take sufficient steps to ensure that the exceptions process for dealing with rejected Customer Records was adequate and there were no processes in place to deal with rejected Account Records and Transaction Records.

2.20.3. Bad Data was recognised as a risk and a serious issue at comparatively less senior grades within Metro and individual staff members investigated and attempted to escalate this issue to more senior staff and Committees in 2017 and 2018. However, reference to Bad Data was removed from the Financial Crime Steering Group's January 2018 minutes, on the basis that the Bad Data issue did not appear to be substantiated, which meant there was no action to track and monitor this risk. Members of the Working Group and the Operations Risk Board also escalated the issue of Bad Data to senior staff in 2018. Although the risk was passed to a more junior member of staff to liaise with a senior member of staff, no substantive action took place.

2.20.4. During the Relevant Period Metro did not have a sufficient understanding of the level of AML risk associated with unmonitored transactions. This was, in part, due to the fact that the true picture of the volume of transactions rejected by the ATMS (and which therefore went unmonitored) was obscured by the presence of internal transactions which did not need to be monitored. This issue took Metro over four years to resolve and it was only on 14 December 2020, shortly before the end of the Relevant Period, that Metro implemented a fix to remove internal transactions from the data feed into the ATMS.

2.21. These transaction monitoring failings resulted in over 60 million transactions with a value of over £51 billion not being monitored during the Relevant Period. Whilst many of these transactions were subsequently reviewed as part of a remediation exercise, there was a lengthy delay in the identification of suspicious activity and this increased the risk of Metro inadvertently being used for the purposes of financial crime.

2.22. The Authority acknowledges the historic nature of the failings identified in this Notice, and Metro has remediated these issues. The Authority also acknowledges that Metro has invested extensively in remediating and enhancing its financial crime framework since the events in question.

2.23. The Authority hereby imposes on Metro a financial penalty of £16,675,200 pursuant to section 206 of the Act.

3. DEFINITIONS

3.1. The definitions below are used in this Notice:

"Account Record(s)" comprise details about the account including the account number.

The "Act" means the Financial Services and Markets Act 2000.

"AML" means Anti-Money Laundering.

The "ATMS" means the Automated Transaction Monitoring System in operation at Metro.

The "Authority" means the Financial Conduct Authority.

"Bad Data" means any records that were rejected from the ATMS.

The "Bad Data Report" means the internal Metro report dealing with Bad Data in more detail than the later Working Group Paper (see below).

The "Business and Commercial Support Team" means the team within Metro responsible for reviewing Customer Records rejected from the ATMS which was known as the "Account Servicing Team" until Q4 2018.

"Compliance Firm 1" was engaged by Metro in December 2018 to undertake a review of the Bank's financial crime technology to understand whether it was aligned with standard industry practice.

"Compliance Firm 2" was engaged by Metro in December 2019 to review the end-to-end architecture of the AML / transaction monitoring features of the ATMS.

"Compliance Report 1" means the compliance report produced by Compliance Firm 1.

"Compliance Report 2" means the compliance report produced by Compliance Firm 2.

"Customer Record(s)" comprise details about the customer including, for example, address and country of residence.

“DS” means Data Store, a separate database which contained a near real-time view of the data within Metro’s core banking records system. The data feed for the ATMS originated from the DS.

The “FCIP” means the Financial Crime Improvement Programme implemented by Metro post-Compliance Report 2.

The “JMLSG” means the Joint Money Laundering Steering Group. The JMLSG produces guidance for the financial services sector relating to compliance with AML and counter terrorist financing legislation and the associated regulations.

The “Lookback Audit” means the audit of the Lookback Review performed by Metro in Q4 2020.

The “Lookback Review” means a transaction monitoring lookback review initiated by Metro, which involved identifying all accounts missing from the ATMS as of 1 July 2019.

“Metro” or the “Bank” means Metro Bank Plc.

The “Operations Risk Board” means the Financial Crime Operations Risk Board at Metro.

The “PRA” means the Prudential Regulation Authority.

“Referential Integrity” means the requirement for the ATMS to have the associated Customer Record (including details about the customer) and Account Record (including the account number) in order to successfully acquire a Transaction Record and monitor that transaction. If Referential Integrity did not exist in Customer, Account and Transaction Records, the ATMS rejected the acquisition of the associated record(s).

The “Regulations” means the Money Laundering Regulations 2007.

The “Relevant Period” is 6 June 2016 to 17 December 2020.

The “Reports” means the Bad Data Report and the Working Group Paper (see below).

The “Technology Steering Committee” means the Financial Crime Technology (ATMS) Steering Committee at Metro.

The "Time Stamp Code Logic Error" refers to an issue which was caused by an error in the data extraction methodology from the Bank's DS for loading into the ATMS. This affected Account Records, and because of Referential Integrity it caused associated Transaction Records to be rejected by the ATMS where a customer had opened an account and transacted on the same day.

"Transaction Record(s)" comprise details about individual transactions.

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

The "Working Group" means the Financial Crime Working Group at Metro.

The "Working Group Paper" means the Financial Crime Working Group paper summarising the issues in relation to Bad Data as understood at the time within Metro dated 19 April 2018.

4. FACTS AND MATTERS

Background

Metro Bank Plc

4.1. Metro is an authorised firm that is regulated by the Authority and the PRA. It is 100% owned by Metro Bank Holdings Plc, which is listed on the main market of the London Stock Exchange.

4.2. Metro was established in 2010 and offers retail, business, commercial and private banking services.

Overview of legal and regulatory obligations

Principles for Businesses / Senior Management Arrangements, Systems and Controls

4.3. Metro was required, pursuant to Principle 3 of the Authority's Principles for Businesses, to take reasonable care to organise its affairs responsibly and effectively, with adequate risk management systems.

4.4. Under the chapter of the Authority's Handbook entitled Senior Management Arrangements, Systems and Controls ("SYSC"), Metro was also required to:

4.4.1 establish, implement and maintain adequate policies and procedures sufficient for ensuring the compliance of the firm with its obligations under the regulatory system and for countering the risk that it might be used to further financial crime (SYSC 6.1.1R);

4.4.2 ensure that those policies and procedures include systems and controls that enable it to identify, assess, monitor and manage money laundering risk and were comprehensive and proportionate to the nature, scale and complexity of its activities (SYSC 6.3.1R); and

4.4.3 carry out a regular assessment of the adequacy of those systems and controls to ensure that they continue to comply with SYSC 6.3.1R (SYSC 6.3.3R).

Money Laundering Regulations 2007

4.5. Metro had a separate obligation to comply with relevant legal requirements under the Money Laundering Regulations 2007 (the "Regulations").

Requirement to carry on ongoing monitoring

4.6. The Regulations required firms to carry out ongoing monitoring of a business relationship on a risk-sensitive basis (Regulation 8). The purpose of conducting ongoing monitoring is to scrutinise transactions to ensure they are consistent with the firm's knowledge of the customer and to identify patterns of behaviour that appear characteristic of either money laundering or terrorist financing and which, after analysis, may lead to suspicions of money laundering or terrorist financing. Ongoing monitoring can also help firms to know their customers, assess risk and provide assurance that the firm is not being used for the purposes of financial crime.

Requirement to have appropriate and risk-sensitive policies and procedures

4.7. In order to prevent activities related to money laundering and terrorist financing, the Regulations further required firms to establish and maintain appropriate and risk-sensitive policies and procedures relating to, amongst other things, the ongoing monitoring of business relationships (Regulation 20(1)(a)). In addition, firms were required to establish and maintain appropriate and risk-sensitive policies and procedures relating to the monitoring and management of compliance with, and internal communication of, those policies and procedures (Regulations 20(1)(f)).

4.8. Those policies and procedures referred to above had to provide for the identification and scrutiny of:

4.8.1. complex or unusually large transactions;

4.8.2. unusual patterns of transactions with no apparent economic or visible lawful purpose; and

4.8.3. any other activity which the firm regarded as particularly likely by its nature to be related to money laundering or terrorist financing.

Joint Money Laundering Steering Group Guidance

4.9. SYSC 6.3.5G provides that the Authority, 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 ("JMLSG"). Guidance concerning monitoring customer activity is set out below and reflects the JMLSG Guidance 2014 and JMLSG Guidance 2017.

4.10. Essential to a monitoring system is that it flags up transactions and / or activities for further examination, ensures the reports (referred to in this Notice as "alerts") are reviewed promptly by the right person and appropriate action is taken on the findings of any further examination (paragraph 5.7.3, Chapter 5, Part 1).

4.11. The scope and complexity of the monitoring process will be influenced by a firm's business activities and whether the firm is large or small (paragraph 5.7.8, Part 1, Chapter 5). A monitoring system may be manual or automated but for firms where there are major issues of volume, a more sophisticated automated system may be necessary (paragraph 5.7.13, Part 1, Chapter 5). The greater the volume of transactions, the less easy it will be for a firm to monitor them without the aid of some form of automation (paragraph 5.7.16, Part 1, Chapter 5). Firms should understand the workings and rationale of an automated system, and should understand the reasons for its output of alerts (paragraph 5.7.15, Part 1, Chapter 5).

The implementation of the ATMS

4.12. Having committed to implementing an ATMS, at the planning stage, Metro defined the high-level business requirements for the ATMS. In terms of "core functionality", Metro stated that the system(s) had to be capable of performing and supporting Metro's processes, to a standard which complied with all legal and regulatory requirements and the Bank's own risk appetite. Consequently, the transaction monitoring requirements that were stipulated by Metro as "must haves" for the ATMS included the ability to perform real-time monitoring of all retail and commercial transactions, and the ability to monitor all current and future transaction types across all current and future Metro products.

4.13. In order for monitoring to take place, Customer Records, Account Records and Transaction Records needed to be fed into the ATMS. As a means of feeding the Customer, Account and Transaction Records held in Metro's core banking system into the ATMS, Metro opted to use the DS, which was a separate database within the Bank which contained a near real-time view of the data within Metro's core banking records system. Metro decided to use the DS to feed data into the ATMS for a variety of reasons, including operational resilience.

4.14. The data feed from the DS to the ATMS comprised "batch files" which contained the Customer Records, Account Records and Transaction Records. In this regard:

4.14.1 Customer Records comprised details about the customer including, for example, address and country of residence. Customer Records were sent to the ATMS when a customer record was created for new customers or when an existing customer record was updated, for example, if an existing customer updated their address.

4.14.2 Account Records comprised details about the account including the account number.

4.14.3 Transaction Records comprised details about individual transactions.

4.15. Each of these three sets of records were required in order for the ATMS to effectively monitor customer transactions, as follows: For the ATMS to successfully acquire Transaction Records, the associated Account Records had to be present in the ATMS; for the ATMS to successfully acquire Account Records, the associated Customer Record had to be present in the ATMS. Requiring the associated Customer Record and Account Record for each Transaction Record was known as "Referential Integrity". If Referential Integrity did not exist in Customer, Account and Transaction Records, the ATMS would reject the acquisition of an Account Record where a Customer Record was not present and reject the acquisition of a Transaction Record where an Account Record was not present.

4.16. Where records were acquired by the ATMS (as opposed to being rejected), they would be subject to ongoing monitoring. Records rejected by the ATMS, which were described within Metro as "Bad Data", would be put into Bad Data folders (see paragraphs 4.55 to 4.56). In circumstances where a record in the Bad Data folder comprised a failed update to an existing record (for example, the Customer Record was already in the ATMS but a change to this Customer Record was rejected because an updated address did not include a postcode), transactions on the Account Records attached to the existing Customer Record were still monitored.

4.17. The ATMS went live on 6 June 2016.

The Time Stamp Code Logic Error

4.18. On 17 April 2019, during testing of an upgrade to Metro's core banking records system, Metro identified the Time Stamp Code Logic Error. This issue was caused by an error in the data extraction methodology from the Bank's DS for loading into the ATMS, which caused certain transactions to be rejected by the ATMS. This issue had been present since the introduction of the ATMS by Metro in June 2016 and, as such, it had not been identified for a period of almost three years, despite the fact that it resulted in large numbers of transactions not being monitored (see paragraphs 4.74 to 4.76).

4.19. Metro discovered that, in circumstances where (a) a customer had opened an account and (b) made transactions on the same day, the Customer Records and Transaction Records were extracted from the source data and included in the data feed from the DS to the ATMS in the correct way, but the Account Records were not being included in the data feed from the DS to the ATMS. This was due to a technical flaw whereby the timestamp on the Account Records was "processing day +1", whereas the logic used to populate the ATMS batch file looked for a timestamp of "processing day -1". Because of this incompatibility, the Account Records were not extracted from the DS.

4.20. Due to Referential Integrity, where there was an absence of an Account Record in the ATMS, all Transaction Records related to that account would be rejected. Thus the Time Stamp Code Logic Error caused all transactions on the affected accounts to be rejected from the ATMS. At the time of the Lookback Review, Metro understood this issue to occur from the opening of the account until there was a day on which there were no transactions on the account, and the ATMS could reconfigure. Following the end of the Relevant Period, Metro established that the issue occurred if and until there was an update to the Account Record, and the ATMS could reconfigure.

4.21. In addition, it was not possible to load transactions into the ATMS retrospectively as each Transaction Record had a date-stamp on it and, once the system date had moved beyond this date-stamp, the transaction could not be loaded into the ATMS.

4.22. Metro notified the Authority about the Time Stamp Code Logic Error on 29 May 2019 and a tactical fix to remedy the Time Stamp Code Logic Error was implemented on 21 July 2019.

4.23. However, by this time, the Time Stamp Code Logic Error had impacted in the region of 166,000 accounts, meaning that over 46.5 million transactions related to those accounts with an associated value of over £31.5 billion had not been monitored.

4.24. The Authority considers it a serious failure in the operation and oversight of the ATMS that the Time Stamp Code Logic Error was allowed to persist for over three years, since the implementation of the ATMS, before being identified and rectified. During the intervening period, large numbers of transactions which should have been monitored for AML purposes were not, meaning that there was an enhanced risk of Metro being used to facilitate money laundering during the Relevant Period.

The Time Stamp Code Logic Error and lack of an effective reconciliation process

4.25. The failure by Metro to identify the Time Stamp Code Logic Error in a timely manner arose, in part, as a result of the fact that, before the Lookback Review in July 2019, Metro took no steps to check the completeness of data fed into the ATMS. Throughout 2020, Metro performed a number of ad-hoc reconciliations to check the completeness of the data feed, but these only related to Customer Records and Account Records and did not cover Transaction Records. Prior to 17 December 2020, Metro failed to put in place an effective reconciliation process between the DS and the destination ATMS in order to ensure that all Customer, Account and Transaction Records were loading correctly.

4.26. Data reconciliation in this context is the process of validating data that is fed from a firm's source systems to the transaction monitoring system to confirm it is complete. If the data differs between the source systems and the ATMS, then this suggests that transactions are not being loaded into the ATMS and as a result not being monitored by the ATMS, which would therefore not generate alerts where appropriate.

4.27. In this way, the Authority considers that an effective reconciliation process between the DS and the ATMS was a key part of the Bank's transaction monitoring system which should have been in place from the inception of the ATMS in June 2016. However, prior to the Lookback Review in July 2019 (see paragraphs 4.33 to 4.45) there was no reconciliation between the DS and the ATMS. Further, there was no set procedure for undertaking regular reconciliations between the DS and the ATMS, so as to ensure that all Customer, Account and Transaction Records were being correctly received by the ATMS on an ongoing basis, from the ATMS going live on 6 June 2016 until the implementation of a count check control in December 2020.

4.28. Metro performed a number of ad hoc reconciliations over the course of 2020, relating to Account Records and Customer Records, but not Transaction Records:

4.28.1. In March 2020, Metro performed a reconciliation of Account Records present in the DS and Account Records present in the ATMS. This identified that 125 accounts of the 374,593 accounts opened in the period to 31 March 2020 ought to have fed into the ATMS but had failed to do so and, of these, 106 accounts had failed to load due to data validation issues.

4.28.2. In July 2020, Metro compared the volume of customers in the DS against the volume of customers in the ATMS. The exercise found that there was a discrepancy of 3,135 between active Customer Records for transaction monitoring in the ATMS (1,138,196) and the expected figure from the DS (1,141,331).

4.28.3. In September 2020, Metro checked the number of Customer Records that were not updated successfully in the ATMS against the overall population of Customer Records in the DS. This established that 3,282 Customer Records had been rejected due to data validation issues however, of these, 955

Customer Records were inactive. Of the remaining population of 2,327 active records, only 30 customer records that could not be updated were in scope for transaction monitoring.

4.29. These reconciliations provided Metro with assurance, at the point they were completed, of the coverage of the Customer and Account Records in the ATMS. Following each of these exercises, Metro took steps to remediate the records identified as missing and manually load these into the system.

4.30. However, the performance of these ad hoc reconciliations was inadequate, in the absence of a formal procedure for checking the completeness of the data (including Customer, Account and Transaction Records) in the ATMS on an ongoing basis.

4.31. On 17 December 2020, the DS commenced sending daily “count files” along with each of the batch files to the ATMS. The count files included figures for all Customer, Account and Transaction Records and enabled Metro to compare the total number of records received by the ATMS, plus the records rejected from the ATMS and placed into Bad Data folders, to the total number of records sent to the ATMS from the DS on an ongoing basis. Where the totals did not match, emails were generated and sent to Financial Crime Operations in order to alert them to the disparity. Prior to this control being implemented, Metro had no mechanism for checking on an ongoing basis whether all records that were intended to be monitored by the ATMS were successfully received by the ATMS from the DS. As such, the Authority considers that Metro only put into place an effective reconciliation process as part of its monitoring system on 17 December 2020 (marking the end of the Relevant Period).

4.32. The Authority considers that it was a serious failure on the part of Metro not to ensure that there was an effective reconciliation process in relation to the data received by the ATMS at the time it was implemented. The Authority further considers that, if an effective reconciliation process had been put in place in June 2016, then the Time Stamp Code Logic Error could have been identified and rectified sooner, and the missing transactions could have been monitored for potentially suspicious activity well before Metro commenced its remediation project in July 2019.

Time Stamp Code Logic Error Remediation Project - the Lookback Review and the Lookback Audit

4.33. A remediation project, the transaction monitoring lookback review (the "Lookback Review"), was initiated by Metro in July 2019 after it identified the Time Stamp Code Logic Error.

4.34. As part of the Lookback Review, Metro undertook a reconciliation exercise comparing a full list of the accounts in the DS with the accounts in the ATMS as of 1 July 2019, with a view to identifying and remediating all accounts missing from the ATMS. Metro identified that approximately 238,000 accounts were missing from the ATMS. Of these, 166,358 accounts were missing because of the Time Stamp Code Logic Error.

4.35. The remaining 71,627 accounts were not affected by the Time Stamp Code Logic Error and were missing from the ATMS for other reasons. There had been no transactions on 71,378 of these accounts and the remaining 249 accounts had been opened prior to the implementation of the ATMS. Metro did not undertake a targeted root cause analysis to understand why the 71,627 accounts were missing from the ATMS at that time as it instructed a third-party, Compliance Firm 2, to undertake a review of the end-to-end architecture of the AML / transaction monitoring features of the ATMS in December 2019.

4.36. At the time of the Lookback Review, the 238,000 accounts that were identified as missing from the ATMS were incorrectly thought to be associated with 152,225 customers (see paragraph 4.40 below for further details of how this was confirmed to be an underestimation of the number of customers, during the Lookback Audit). At this time, Metro understood that these customers had a further 143,823 associated accounts, which had previously been fed into the ATMS and had been subject to ongoing monitoring. However, these associated accounts were included within the scope of the Lookback Review *"in order to ensure that the customer focused detection scenarios operated correctly"*, on the basis that the behaviour of each customer would not have been evaluated correctly had a full set of their accounts not been included in the review. As a result, there were over 381,000 accounts within the scope of the Lookback Review.

4.37. Once the number of accounts missing from the ATMS had been identified, in effect, the Lookback Review replicated the ATMS transaction monitoring scenarios over the accounts which were missing from the ATMS and the associated accounts of those customers. This resulted in the generation of 10,162 alerts indicating that unusual or uncharacteristic transactional activity had taken place on those customers' accounts, which the Bank's alert review team then reviewed (see paragraph 4.43).

4.38. In Q4 2020, Metro performed an audit of the Lookback Review (the "Lookback Audit"). The Lookback Audit identified that a coding error had occurred which had led to a material reduction in the scope of customers that had been included in the Lookback Review. The Lookback Audit report, which was finalised in May 2021, concluded that, as a result of this error, a potentially significant number of customers (over 1,400) and over 4,000 alerts had been excluded from the Lookback Review.

4.39. After the Lookback Audit, an additional alert file was generated, containing an additional 4,946 alerts across 1,742 customers.

4.40. Following the Lookback Audit, it was confirmed that the circa 238,000 accounts that were identified as missing from the ATMS were, in fact, associated with 212,205 customers (as opposed to 152,225 customers as incorrectly identified by the Lookback Review) and that these customers had 290,011 associated accounts (as opposed to 143,823 associated accounts) that had previously been subject to transaction monitoring. The additional 146,188 accounts were also included in the review to enable a more comprehensive assessment, once again, on the basis that the behaviour of each customer would not have been evaluated correctly had a full set of their accounts not been included in the review.

4.41. Overall, the Lookback Review and the Lookback Audit considered approximately 112.7 million transactions of approximately 212,000 customers across approximately 528,000 accounts and generated 15,108 alerts.

4.42. In total, 46,662,134 previously unmonitored transactions were included in the scope of the Lookback Review. The value of these transactions was £31,637,046,957.

4.43. These unmonitored transactions were only reviewed after the event, during the periods April 2020 to October 2020 (as part of the Lookback Review) and January 2022 to March 2022 (following the Lookback Audit of the Lookback Review). Following each of these reviews, the Bank submitted a number of additional suspicious activity reports (124 and 29, respectively). Metro also issued notices to customers closing their accounts (36 and 7, respectively). Prior to the Lookback Review, Metro had made 1,403 suspicious activity reports in respect of customers included in the Lookback Review.

4.44. The Authority considers that there was a lengthy delay in the identification of certain suspicious activity and, therefore, an increased risk that money laundering and/or terrorist financing had gone undetected for a significant period of time.

4.45. The Lookback Audit concluded in March 2022, almost three years after the Lookback Review first commenced and almost six years after the ATMS had been implemented.

The Time Stamp Code Logic Error and Bad Data

4.46. As explained above, the Time Stamp Code Logic Error occurred due to an error in the data feed methodology whereby, in circumstances where a customer account was opened and a transaction on that account took place on the same day, the Account Records were not included in the data feed from the DS to the ATMS. This, in turn, meant that transactions on customer accounts affected by the Time Stamp Code Logic Error were then rejected by the ATMS as Bad Data, as Referential Integrity required that Transaction Records had to have the associated Customer and Account Records in the ATMS in order for the Transaction Records to be accepted by the ATMS. Aside from the Time Stamp Code Logic Error, the ATMS also rejected Customer, Account and Transaction Records as Bad Data for other reasons. The Authority's findings in relation to Bad Data and the inadequate manner in which Metro dealt with this issue are set out in paragraphs 4.47 to 4.73 below.

Bad Data

4.47. "Bad Data" (as referred to within Metro) was a term used for any Customer, Account and Transaction Record that had been rejected from the ATMS. These rejected records were placed into Bad Data folders.

4.48. There were rules within the ATMS to prevent data loading where there were data quality issues, such as missing or incomplete data or a failure to meet prescribed criteria. Where a mandatory field was missing, the whole record would be rejected. Where a non-mandatory field was missing, the record might be rejected in part.

4.49. As referred to above at paragraph 4.15, for the ATMS to successfully acquire Transaction Records, the associated Account Records had to be in the ATMS. Likewise, for the ATMS to successfully acquire Account Records, the associated Customer Records had to be in the ATMS. This requirement was referred to as Referential Integrity and, if Referential

Integrity did not exist in respect of each of those records, the ATMS would reject their acquisition.

4.50. The main reasons that Customer Records were rejected by the ATMS during the Relevant Period related to issues with the address, the postcode and the country of residence of the customer (as a result of the fact that the relevant fields were either blank, incorrect or did not conform to specifications).

4.51. The singular reason that Account Records were rejected by the ATMS during the Relevant Period was because they were "*Missing Primary Customer Record*" on the basis that, where the Customer Record was not in the ATMS (as described in the previous paragraph), the associated Account Record was rejected because of the requirement for Referential Integrity. As set out in paragraph 4.19 above, the Time Stamp Code Logic Error resulted in Account Records being excluded from the ATMS data feed, rather than being rejected by the ATMS.

4.52. The main reason that Transaction Records were rejected by the ATMS was "*Account Number not known to* [the ATMS]" on the basis that, where the Account Record was not in the ATMS (as described in the previous paragraph), the associated Transaction Records were rejected because of the requirement for Referential Integrity. During the Relevant Period, the primary reason that *"Account Number [was] not known to* [the ATMS]*"* was because of the Time Stamp Code Logic Error.

4.53. In this way, if the Customer Record was not acquired into the ATMS, for whatever reason, then there could be no Account Record in the ATMS. With no Account Record in the ATMS, no transactions could be monitored on the account until the Customer Record, and following this the Account Record, were successfully acquired into the ATMS.

4.54. Furthermore, even if the Account Record was successfully accepted into the ATMS at some point in the future, there was no facility to "replay" the transactions that had been missed in the ATMS, as the ATMS did not have the functionality to process transaction data retrospectively (see paragraph 4.21). In this way, the ATMS could not remediate unmonitored transactions automatically and any transactions that had been made by the customer up to that point could not be monitored by the ATMS. However, the Authority acknowledges that Metro took steps to remediate certain transactions within the Bad Data folders through the Lookback Review.

Bad Data folders

4.55. Records rejected by the ATMS (i.e. Bad Data) were put into Bad Data folders. Upon this occurrence, the ATMS would also generate a file which provided details of the reasons why the ATMS could not acquire the records, for example because a mandatory field was not present.

4.56. However, despite some members of staff being aware that large amounts of Bad Data, particularly in relation to Transaction Records, were being deposited into the Bad Data folders, Metro failed to put in place a process for dealing with the rejected Account and Transaction Records in the Bad Data folders, which were only intermittently reviewed as part of work by these individuals to understand the Bad Data issues. As regards the rejected Customer Records in the Bad Data folders, these were meant to be dealt with by Metro's "exceptions process" however this was inadequate for the reasons set out below in paragraphs 4.57 to 4.73.

The exceptions process for Bad Data

4.57. There was an exceptions process within Metro which was meant to deal with Customer Records (as opposed to Account Records and Transaction Records) which had been rejected from the ATMS as Bad Data during the Relevant Period. The exceptions process was managed by Metro's Business and Commercial Support Team (formerly the Account Servicing Team until Q4 2018).

4.58. Initially, IT Operations within Metro produced daily reports in the form of a spreadsheet, which set out details of the Customer Records that required remediation (in order to correct the issues that were causing them to be treated as Bad Data). The Business and Commercial Support Team was then responsible for remediating the Customer Records which were referred to in the daily reports, where they were able to do so (for example, by correcting data which was in the wrong format or inserting missing data). However, the Business and Commercial Support Team did not have the necessary permissions to remediate all types of Customer Records (see paragraphs 4.61 to 4.64) and, furthermore, there were occasions when the daily reports were not emailed to the Business and Commercial Support Team for processing, such that a backlog of remediation work built up between September 2016 and March 2017.

4.59. To address the issue of the daily reports not being emailed to the Business and Commercial Support Team in a timely manner, the process of generating the daily reports was automated by IT Operations in April 2017. From this time, the daily reports were automatically placed in a shared folder within Metro which the Business and Commercial Support Team could access. As before, the Business and Commercial Support Team was then responsible for remediating the Customer Records in the daily reports, however it remained the case that they were not able to do so where they did not have the necessary permissions.

4.60. Further, there was no escalation process in place if the Business and Commercial Support Team could not correct a Customer Record. In effect, this meant that there was no designated procedure for correcting certain types of Customer Records, such that those Customer Records and the associated Account and Transaction Records would continue to be rejected by the ATMS and would go unmonitored.

4.61. One type of Customer Record that the Business and Commercial Support Team was not able to correct was Partnership records. The Partnerships service from Metro offered a range of banking services for a variety of approved intermediaries including pension providers, Independent Financial Advisers, wealth managers and accountants.

4.62. The Bad Data Report (see paragraphs 4.90 to 4.93), completed by April 2018, stated that 62% (2,772 of 4,448) of the Customer Records rejected from the ATMS were from the Partnerships area within Metro. The Bad Data Report also stated that there was a spike of Bad Data which, in all likelihood, was related to Partnerships in December 2017 when 74% of Bad Data related to customers was believed to have originated from that part of the business.

4.63. The Business and Commercial Support Team was not responsible for Partnerships Customer Records and they did not have access to those records in Metro's core banking system, meaning that they were unable to view and amend them. As a result, as of May 2018, the Business and Commercial Support Team could only rectify approximately a third of the Customer Records that were detailed in the daily reports that were produced as part of the exceptions process.

4.64. In this way, at the time the Bad Data Report was written, no steps were being taken by Metro to review or rectify the necessary Partnerships Customer Records relevant for the ATMS as part of the exceptions process.

4.65. Where it was possible for the Business and Commercial Support Team to remediate Customer Records as envisaged under the exceptions process, this entailed updating the Customer Record in Metro's core banking records system and contacting the relevant relationship manager for further information where necessary.

4.66. However, there was an absence of defined procedures in relation to how the Business and Commercial Support Team should go about correcting all types of Customer Records which, coupled with inadequate oversight of the exceptions process, meant that Metro had inadequate controls around ensuring that the remediation of the rejected Customer Records was undertaken properly and seen through to completion in an appropriate timeframe. The potential risk associated with the lack of defined process for remediating Customer Records was articulated by more junior Metro staff prior to the ATMS going live in March 2016 and yet it was still being referenced as an ongoing concern in the Bad Data Report which was finalised over two years later. In this way, the exceptions process was insufficiently defined and had inadequate oversight, despite more junior staff at Metro recognising this as a risk area.

4.67. If a Customer Record could be corrected, it was automatically fed into the ATMS the following day in the normal "business as usual" processes that picked up new and changed Customer Records. Once a Customer Record had been remediated in this way, in circumstances where the associated Account Record had been rejected by the ATMS because of Referential Integrity, it was possible for the ATMS to acquire the Account Record without the need for remediation of the Account Record itself (although this did not occur automatically).

4.68. However, there was no process for ensuring that Account Records associated with rejected Customer Records were acquired into the ATMS, once the Customer Records had been corrected. The Authority acknowledges that Metro undertook some reconciliations in 2020 (see paragraphs 4.28 to 4.30), following which it remediated certain missing records and manually loaded these into the system.

4.69. Likewise, there was no process to deal with Transaction Records which were rejected by the ATMS and put into Bad Data folders, although the Lookback Review which took place in July 2019 following Metro's identification of the Time Stamp Code Logic Error did involve the review of Transaction Records associated with the Account Records that were identified as missing from the ATMS as at 1 July 2019 (see paragraphs 4.33 to 4.45 above). Further, as referred to above, there was no facility to "replay" the transactions that had been missed in the ATMS as the ATMS did not have the functionality to process transaction data retrospectively (see paragraphs 4.21 and 4.54).

4.70. Moreover, in terms of governance, no management information was generated in relation to the exceptions process and no periodic reporting on Bad Data to any individuals, teams or committees took place during the Relevant Period.

4.71. The Authority therefore considers that Metro failed to put in place adequate systems and controls for managing Bad Data and in relation to the exceptions process which meant that Customer, Account and Transaction Records that should have been routinely loaded into the ATMS were not being so loaded, either in a timely fashion or at all.

4.72. As a result, every time a Bad Data record was created for a new Customer Record, an Account Record or a Transaction Record, the ongoing monitoring ordinarily performed by the ATMS, which in turn would have generated alerts for Metro's AML teams, was not performed for these records. Consequently, unusual or uncharacteristic transactional activity was not highlighted to the Metro AML teams who would ordinarily use this information to identify suspicious activity. As such, in respect of Bad Data, there was a risk of Metro missing suspicious activity and thereby inadvertently being used to further financial crime.

4.73. The Authority considers that an effective process for managing Bad Data so as to ensure that the associated records were subject to ongoing monitoring was a key part of Metro's AML control framework and should have been in place since the inception of the ATMS in 2016. Further, in the absence of this, substantive remedial action should have taken place when the risks in relation to Bad Data and the exceptions process were being discussed within Metro throughout 2018 (see paragraphs 4.78 to 4.103).

Impact of Bad Data

4.74. Of the total number of transactions not monitored by Metro in the period 6 June 2016 to 21 July 2019, at least 46,662,134 transactions (£31,637,046,957 in value) are attributable to the Time Stamp Code Logic Error, and Metro is not able to precisely attribute 13,807,299 (£19,686,082,418 in value) between the Time Stamp Code Logic Error and other Bad Data issues.

4.75. However, through work undertaken following the end of the Relevant Period, Metro determined that, for transactions intended for monitoring by the ATMS, at least 99.7%

of Transaction Records were consistently fed into the ATMS from 21 July 2019, the point Metro implemented the fix for the Time Stamp Code Logic Error (see paragraph 4.22). This indicates that the Time Stamp Code Logic Error is likely to have been the single material failure resulting in Bad Data Transaction Records during the Relevant Period. Following the application of the fix for the Time Stamp Code Logic Error, the number of rejected Transaction Records significantly decreased from 1,352,665 for July 2019 to 438 in August 2019.

4.76. During the entirety of the Relevant Period, the total number of transactions entered into the ATMS was at least 1,008,426,668, with at least 60,483,951 (circa 6.0%) being rejected due to the Time Stamp Code Logic Error or other issues with Bad Data. The total value of the transactions entered into the ATMS during this period was at least £675,818,015,000, with the total value of rejected transactions as a result of the failings described in this Notice being at least £51,250,294,000 (circa 7.6%). This equated to a high volume and high value of transactions that were not monitored, with Metro having insufficient understanding as to why, during the Relevant Period.

4.77. Further, the failure to put in place an effective reconciliation process between the DS and the ATMS until 17 December 2020 meant that, during the Relevant Period, Metro was not appropriately monitoring the quantity of rejected Transaction Records.

Lack of effective oversight and governance

Lack of overall oversight in relation to the ATMS, Bad Data and the exceptions process

4.78. Metro has informed the Authority that there has been a loss of institutional knowledge from within Metro due to key stakeholders involved with the ATMS leaving over time. Metro was only able to identify limited documentation which clarified the roles and responsibilities associated with the effective ongoing management of the ATMS prior to January 2020. Metro has also been unable to identify who was responsible for ensuring that the data ingested into the ATMS was complete in the period from the start of the Relevant Period to January 2020. Further, no management information was generated in relation to the exceptions process and no periodic reporting on Bad Data to any individuals, teams or committees took place during the Relevant Period.

Awareness of Bad Data amongst operational staff

4.79. As of 29 March 2016, prior to the go-live date for the ATMS, there was a recognition within Metro's Information Technology staff of the potential for Bad Data to be an issue and that processes needed to be put in place to deal with this issue effectively.

The Customer Monitoring Steering Group

4.80. The Customer Monitoring Steering Group had oversight of the implementation of the ATMS. It was aware of the potential for Bad Data to arise prior to the implementation of the ATMS and was involved in defining the exceptions process. The Customer Monitoring Steering Group was disbanded in November 2016 however it appears to have taken no substantive action to address the Bad Data issues before being disbanded.

The Financial Crime Steering Group

4.81. The Financial Crime Steering Group had an oversight role in relation to financial crime issues that arose within Metro and included senior individuals within Metro.

4.82. At a meeting of the Financial Crime Steering Group on 13 April 2016, Bad Data was discussed, demonstrating an awareness of the issues associated with Bad Data prior to the ATMS going live. In particular, it was noted that concerns had been raised about "*the system picking up Bad Data and not being able to process alerts until this has been cleared*" and, further, that there was a need to "*analyse how much can we ignore/remediate before we agree next actions. A process is being drawn up for Bad Data….*".

4.83. Whilst an exceptions process was put in place within Metro which purported to deal with Customer Records rejected from the ATMS since it went live on 6 June 2016, this was inadequate for the reasons set out at paragraphs 4.57 to 4.73. Further, Metro took no steps to implement a process to ensure that Account Records associated with rejected Customer Records were acquired into the ATMS, or to deal with Transaction Records rejected from the ATMS (although the Lookback Review which took place in July 2019 following Metro's identification of the Time Stamp Code Logic Error did involve the review of Transaction Records associated with the Account Records that were identified as missing from the ATMS as at 1 July 2019 (see paragraphs 4.33 to 4.45 above)).

4.84. In mid to late 2017, staff at Metro raised concerns about Bad Data and the fact that these records were not being remediated with a senior member of the Financial Crime Steering Group. However, it remained the case that the issue of Bad Data was not given adequate consideration: Although Bad Data was discussed at a meeting of the Financial Crime Steering Group on 18 January 2018, the final minutes of the meeting do not record any discussion of Bad Data. In fact, the issue was raised at the meeting, and an action was agreed to undertake a review and present back to the Financial Crime Steering Group in February 2018. However, this action was subsequently removed from the final minutes of the meeting on the basis that there was "*no context*" and "*the concern that had been raised had not yet been substantiated*". Although the issue of Bad Data had already persisted since the implementation of the ATMS, it was agreed that this issue could be revisited by the Financial Crime Steering Group once it was better understood. Removing reference to Bad Data from the minutes of the meeting meant that the Financial Crime Steering Group had no related action to track and monitor going forward. It therefore had no reminder to seek the "*context*" or substantiation that was said to be needed, or to discuss Bad Data again at its future meetings. Indeed, despite the issue not having been resolved, Bad Data did not appear in Financial Crime Steering Group governance materials again for well over a year, until after the Time Stamp Code Logic Error had been identified in April 2019.

4.85. Internal Metro communications demonstrate that there was significant concern in relation to Bad Data amongst less senior staff at the Bank who recognised this as a serious risk area, for example, acknowledging that the Business and Commercial Support Team "*can only rectify about 1/3 of the bad data, the rest sits with Partnerships so is never corrected and historic transactions are never screened"*. These less senior staff were clear that this issue was not getting the exposure it needed at senior levels within Metro and required continued escalation. Given the volume of transactions that were not being monitored during this period of time, Bad Data represented an ongoing risk to the Bank that was not adequately addressed despite the fact that less senior staff recognised it as a serious issue.

The Financial Crime Working Group

4.86. The Financial Crime Working Group (the "Working Group") was established in March 2018 in order to provide oversight of the monitoring of financial crime risk within the Bank. Its responsibilities included optimising the performance of the ATMS. The Working Group reported into the Financial Crime Steering Group and was responsible for providing regular updates to the Financial Crime Steering Group. Many of the less senior members of Metro staff who had concerns about Bad Data (see paragraph 4.85) were members of the Working Group.

4.87. The inaugural meeting of the Working Group took place on 15 March 2018. The minutes of the meeting record an action to produce a summary paper in relation to Bad Data for discussion at the next meeting covering the following areas:

> "*What is bad data?*
> *What is the current process for managing/repairing bad data?*
> *What is the impact of not fixing bad data?*
> *What are the current issues with bad data?*
> *What action is required to address?"*

4.88. On 19 April 2018, an internal paper was produced for the Working Group summarising the issues in relation to Bad Data as understood within Metro at the time (the "Working Group Paper"). This appears to have been a summary of a separate report which dealt with issues in relation to Bad Data in more detail (the "Bad Data Report"). Collectively these two documents are referred to as "the Reports" in this Notice.

4.89. The Authority acknowledges that the Reports were not intended to be conclusive and were primarily intended to raise awareness of the issues addressed therein. The Authority also acknowledges that the Reports reflected what Metro understood at the time of their creation and that further analysis was required by Metro in order to investigate the issues raised and identify the root cause(s). Nonetheless the Authority considers that the Reports demonstrate that there was a clear understanding within the Working Group that Bad Data constituted a significant AML risk which needed to be addressed.

Detail of the Bad Data Report

4.90. The purpose of the Bad Data Report was to put some context around the Bad Data issues with a view to then escalating the issues further within Metro. The Bad Data Report also set out why Bad Data was problematic from an AML perspective. It stated:

> "*Every time a bad data record is created, for a customer, account or transaction it is a signal that this information is not made visible to the AML teams, as they are relying on screening rules maintained within [the ATMS] to catch criminal/illegal activity. This means that the screening performed by [the ATMS], which generates alerts for*

our AML teams; is not performed for every customer/account/transaction. As such there is a risk of not screening the full data and missing out suspicious activity indicators.

Due to the nature of entity relations within [the ATMS], a customer load failure due to bad data is guaranteed to cause associated account load failures even if the account information succeeds all other validations. This in turn can cause all associated transaction loads to fail for said customers' accounts, which means that none of that customer's activity is subject to screening."

4.91. The consequence of the above was that unusual or uncharacteristic transactional activity would not be highlighted to Metro's AML team who would ordinarily use this information to identify suspicious activity. As such, there was a risk of Metro missing suspicious activity and thereby inadvertently being used to further financial crime. Due to Referential Integrity, none of the affected customers' Transaction Records would be subject to ongoing monitoring until the errors in the associated Customer and Account Records had been corrected.

4.92. The Bad Data Report also made reference to various other matters of concern regarding Bad Data and Metro's AML control framework, including the following:

4.92.1. The Bad Data Report acknowledged that Metro had failed to put in place an effective reconciliation process in order to ensure that all Customer, Account and Transaction Records were loading into the ATMS correctly, stating "*there is no absolute reconciliation for all bad data, i.e. list of customers/accounts/transactions present in source systems (*[Metro's core banking records system/DS]*) is not compared to the destination system (ATMS). This means if something fails without warning / error – it is not picked up or reported on. Theoretically, if a record fails to extract, it may fail silently*".

4.92.2. The Bad Data Report set out details of the number of customers/transactions which were not subject to ongoing monitoring as a result of Bad Data. From August 2016 to March 2018, the number of customers that were not, at that time, subject to ongoing monitoring was 5,849 out of 1,213,370 unique customer records in the ATMS, which was a comparatively small number with a failure rate of 0.48%. However, the number and relative proportion of transactions not being monitored was much higher, *"10.8%/1.6M of all* *transactions in March 2018",* down slightly from *"a peak of 1.843M transaction records in Jan 2018 which was 12%"*. In this regard, the Authority acknowledges that these transaction figures included internal Metro transactions which did not need to be monitored in the same way as customer transactions (see paragraph 4.113 to 4.116 below). However, the Authority also notes that the presence of these internal transactions meant that Metro was unable to understand the actual number of customer transactions that were not subject to monitoring and should have been, and hence was unable to quantify the corresponding AML risk associated with Bad Data.

4.92.3. The Bad Data Report stated that 62% of Customer Records rejected from the ATMS were from the Partnerships area within Metro and that there was a spike of rejected Customer Records in December 2017, 74% of which related to the Partnerships area. The Bad Data Report further noted that these Customer Records relating to Partnerships could not be rectified by the Business and Commercial Support Team as part of the exceptions process (see paragraphs 4.61 to 4.64 above).

4.93. In this way, a significant number of the failings identified in this Notice were also discussed in the Bad Data Report as at early 2018. In summary, these related to the lack of an effective reconciliation process, the Business and Commercial Support Team not having full access to all Customer Records, the lack of an escalation process for rejected Customer Records that could not be remediated and a lack of oversight generally within the exceptions process.

Detail of the Working Group Paper

4.94. The Working Group Paper was drafted by members of the Working Group in April 2018. The intention of the Working Group Paper was to simplify and summarise the issues raised in the Bad Data Report so that senior staff within Metro could understand them. Accordingly, the Working Group Paper highlighted several risks in relation to Bad Data including the fact that approximately 26% of transactions were not feeding into the ATMS as, on a daily basis, this percentage of the batch file was being rejected. Consequently, the Working Group Paper acknowledged that "*we are not adequately screening and monitoring our customers*".

4.95. The ‘next steps’ set out in the Working Group Paper included raising this ongoing issue at the Financial Crime Steering Group and relevant risk boards / committees within Metro, and reporting any findings and developments to the Working Group and the Financial Crime Steering Group. However, as referred to above, Bad Data did not appear in Financial Crime Steering Group governance materials until approximately a year later, in April 2019.

4.96. The Reports were considered at Working Group meetings on 19 April 2018 and 17 May 2018, with the Working Group determining that Bad Data should be added as an agenda item going forward.

4.97. Thereafter, minutes of a Working Group meeting dated 19 July 2018 noted an intention to raise issues around the volume of Bad Data being seen with senior management. Although minutes of a Working Group meeting dated 16 August 2018 noted an intention for the Working Group to receive an update on this in September 2018, no such update was received.

4.98. In summary, the Working Group sought to ensure that the risks associated with Bad Data were articulated in the Reports and escalated the issue to senior staff at Metro in 2018. The Authority is not aware of evidence that the issue was effectively escalated further to key decision makers for resolution. Despite the fact that the issue of Bad Data had not been resolved and remained an ongoing AML risk, Bad Data was removed from the Working Group agendas as an item after this point.

The Financial Crime Operations Risk Board

4.99. The Financial Crime Operations Risk Board (the “Operations Risk Board”) was established to provide a review of key risk indicators across Financial Crime Operations, implement an operational risk framework, review risk related events to understand preventative controls and report all risk activity taking place in each team.

4.100. Whilst the Reports were also discussed at the Operations Risk Board, it appears that copies of these documents were not themselves provided to the forum.

4.101. Bad Data was first raised as a risk at the Operations Risk Board at a meeting on 17 May 2018. The minutes of the meeting record that Bad Data was one of two new risks raised and was ranked as the number 5 risk in the “top 5” risks. Moreover, in the risk dashboard circulated prior to this meeting, it was recognised as “*possibly a bank wide risk*”. Bad

Data had risen to number 4 in the top 5 risks by the time of the Operations Risk Board meeting on 19 July 2018, following which a more junior member of the Operations Risk Board was tasked with the action to "*liaise with [a senior member of staff] to understand 'Bad Data' risks and who should be managing the risk*".

4.102. Minutes of an Operations Risk Board meeting dated 16 August 2018 record that it was discussed and agreed that subsequent Bad Data actions sat with this more junior member of staff who was moving to the Policy team at Metro, therefore the actions were no longer required to be tracked as part of the Operations Risk Board meetings. Bad Data was not an agenda item for the Operations Risk Board meeting on 20 September 2018, and it no longer featured as one of the top 5 risks either. Bad Data was not discussed at the Operations Risk Board after the meeting on 16 August 2018.

4.103. In light of the above, the Authority considers that Metro failed to ensure that there were appropriate governance arrangements in relation to Bad Data and, further, failed to take adequate steps to address the issue of Bad Data in a timely manner:

4.103.1. Metro knew of the potential for Bad Data to exist prior to the implementation of the ATMS on 6 June 2016 but did not take steps to ensure that processes were in place to deal with the issue effectively.

4.103.2. Bad Data was recognised as a risk and a serious issue at comparatively less senior grades within Metro and individual staff members investigated and attempted to escalate this to more senior staff and Committees in 2017 and 2018. However, the Financial Crime Steering Group removed reference to Bad Data from its January 2018 meeting minutes on the basis that the Bad Data issue did not appear to be substantiated and would be re-visited when the issue was understood. Despite the issue not having been resolved, the Financial Crime Steering Group did not discuss the issue again until after the Time Stamp Code Logic Error had been identified in April 2019.

4.103.3. Members of the Working Group prepared the Reports which sought to articulate the AML risks associated with Bad Data. The Working Group and Operations Risk Board escalated the issue of Bad Data to senior staff in Metro in 2018. Eventually the risk was passed over to Policy with the more junior member of staff to liaise with a senior member of staff. The Authority understands that Metro has no formal records to demonstrate that such escalation took place. Despite the fact that the issue of Bad Data had not been resolved and remained an ongoing AML risk, Bad Data disappeared from the Working Group and Operations Risk Board agendas.

4.103.4. Despite there being an awareness of the issue of Bad Data within Metro from early 2016 onwards, Metro did not take any substantive action to try to address the issue of Bad Data until it engaged Compliance Firm 1 in December 2018, see paragraphs 4.104 to 4.108 below.

4.103.5. Thus, Metro's failure to take any meaningful steps towards addressing the issue of Bad Data persisted for a period of well over two years.

4.103.6. During this time and throughout the Relevant Period, no management information was generated in relation to the exceptions process and no periodic reporting on Bad Data to any individuals, teams or committees took place.

External Compliance Firms

4.104. Compliance Firm 1 was engaged by Metro in December 2018 to undertake a review of the Bank's financial crime technology to understand whether it was aligned with standard industry practice. Following its review, Compliance Firm 1 produced a report dated March 2019 ("Compliance Report 1").

4.105. Compliance Report 1 identified that although the primary financial crime controls were in place within Metro, their configuration was not aligned with standard industry practice. Compliance Report 1 acknowledged that this was likely to mean that current controls were insufficient to mitigate Metro's key financial crime risks and to meet some regulatory obligations. With specific reference to transaction monitoring, Compliance Report 1 stated that this may overlook customer behaviour which was indicative of money laundering or terrorist financing.

4.106. Compliance Report 1 raised the issue of Partnerships data within Metro (see paragraphs 4.61 to 4.64), observing that circa 20% of Transaction Records, primarily in relation to Partnerships data, were being rejected by the ATMS. Compliance Report 1 went on to state that it was important for Metro to have a mechanism in place to review rejected records and ensure these were corrected.

4.107. Compliance Report 1 also stated that there did not appear to have been a review of the data feed into the ATMS to confirm that all Customer Records, Account Records and Transaction Records were complete and accurately captured by the ATMS. Compliance Report 1 further stated that, without undertaking this step, it was not possible to have confidence that financial crime risk was being appropriately managed within Metro. This issue was characterised as a Medium Priority Finding (on a scale of Low, Medium, High, Very High Priority Findings), which meant that "*Action* [was] *required to strengthen these controls"*.

4.108. In response to Compliance Report 1, Metro established the Financial Crime Technology (ATMS) Steering Committee (the "Technology Steering Committee") in April 2019. The Technology Steering Committee, amongst other areas, was responsible for overseeing improvements to Metro's transaction monitoring systems and controls. The Technology Steering Committee also had oversight of the remediation of the Time Code Stamp Logic Error.

4.109. Compliance Firm 2 was engaged by Metro to review the end-to-end architecture of the AML / transaction monitoring features of the ATMS. The review took place between December 2019 and January 2020. Compliance Firm 2 then produced a report ("Compliance Report 2") detailing their findings.

4.110. Compliance Report 2 also raised the issue of Partnerships data within Metro and the exceptions process (see paragraphs 4.57 to 4.73). In particular, Compliance Report 2 noted that there was no escalation process in place for the Business and Commercial Support team to follow in circumstances where it had been unable to remediate rejected Customer Records. In addition, it was noted that the team was unable to effect changes to Partnership Customer Records, that there was no Service Level Agreement in place for re-processing exceptions (i.e. agreed timeframes in place for amending rejected Customer Records via the exceptions process) and, further, that there was no process in place at all to manage Account Records or Transaction Records that had been rejected from the ATMS.

4.111. Compliance Report 2 also addressed the issue of internal transactions, which did not need to be monitored (see paragraphs 4.113 to 4.116). In this regard, internal accounts were excluded from the Account Records that were sent to the ATMS, however their associated Transaction Records (such as double entries for the general ledger) were not excluded. This meant that these Transaction Records were rejected as Bad Data by the ATMS, due to Referential Integrity. This specific issue caused the generation of thousands of Bad Data records each day which, in turn, meant that there was a lack of clear visibility of the true volume of customer transactions being rejected by the ATMS and made the identification of “true” exceptions (i.e. where genuine data quality issues had occurred and needed to be remediated) more difficult to identify, such that Metro was unable to quantify the corresponding AML risk.

4.112. In this way, both Compliance Firm 1 and Compliance Firm 2 identified risks in relation to (amongst other things) managing Bad Data, the inability of the Business and Commercial Support Team to remediate Partnerships data and the exceptions process, which broadly reflect the Authority’s concerns that are summarised at paragraphs 4.57 to 4.73 above. Some of these risks had also been identified in the Reports prepared in 2018 yet Metro did not take steps to address these risk areas until Compliance Firm 1 and Compliance Firm 2 had submitted their reports, in March 2019 and January 2020 respectively.

Internal transactions at Metro and the ATMS

4.113. As mentioned above, internal Metro transactions did not require monitoring in the same way as external transactions, as these transactions were executed within Metro itself. Despite this, internal transactions were included in the data feed from the DS into the ATMS. These internal transactions were rejected as Bad Data on the grounds of Referential Integrity as there was no corresponding Account Record in the ATMS (see also paragraph 4.111).

4.114. On 14 December 2020, Metro implemented a fix to remove internal transactions from the data feed from the DS into the ATMS. This enabled the Bank to have clear visibility of the true volume of customer transactions being rejected by the ATMS on an ongoing basis for the first time since the ATMS went live in June 2016.

4.115. This fix took Metro four and half years to implement, and during this time the ongoing picture of the volume of customer transactions rejected by the ATMS was obscured by the internal transactions which did not need to be monitored in the first place. The Authority acknowledges that Metro approximately quantified the number of internal transactions in the Bad Data folders during the Lookback Review as at a singular point in time prior to December 2019.

4.116. In combination with the lack of an effective reconciliation process to confirm that all data from the DS was being loaded into the ATMS, the inclusion of internal transactions in the data feed from the DS to the ATMS meant that Metro was unable to properly quantify the extent to which its customer transactions were subject to ongoing monitoring (or otherwise) and, therefore, the level of AML risk in relation to unmonitored transactions during the Relevant Period.

Remediation by Metro

4.117. Metro has taken recommendations from both Compliance Report 1 and Compliance Report 2 and implemented these, either in whole or in part, in an overarching Financial Crime Improvement Programme ("FCIP"). Further, Metro has advised the Authority that remediation activity to address the issues identified in Compliance Report 2 has been included within the scope of either the Bank's FCIP or the programme of work overseen by the Bank's Executive Data Governance Working Group.

4.118. In particular, with reference to the issues identified in this Notice, Metro has made:

4.118.1. significant enhancements to the Bank's end-to-end architecture and data controls to ensure that the data that is fed into the ATMS is complete and accurate: Metro has achieved a reconciliation rate of Transaction Records fed into the ATMS of at least 99.7% by volume since 22 July 2019;

4.118.2. material improvements to the controls for the oversight of Bad Data; and

4.118.3. a significant investment in additional resource and capability to manage the Bank's ATMS, to review and assess the quality and effectiveness of the ATMS and to review and investigate possible suspicious activity.

5. FAILINGS

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

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

5.3. SYSC 6.1.1R required Metro to establish, implement and maintain adequate policies and procedures sufficient to ensure Metro's compliance with its obligations under the regulatory system and for countering the risk that it might be used to further financial crime.

5.4. SYSC 6.3.1R required Metro to ensure that those policies and procedures included systems and controls that (1) enabled it to identify, assess, monitor and manage money laundering risk, and (2) were comprehensive and proportionate to the nature, scale and complexity of its activities.

5.5. SYSC 6.3.3R required Metro to carry out a regular assessment of the adequacy of those systems and controls to ensure that they remained compliant.

5.6. During the Relevant Period, Metro failed to meet these requirements and, in doing so, breached Principle 3. In particular:

5.6.1. From the implementation of the ATMS on 6 June 2016, Metro failed to take any steps to check the completeness of data feeding into the ATMS, prior to identifying the Time Stamp Code Logic Error on 17 April 2019. Throughout the Relevant Period, Metro did not have controls in place to check, on an ongoing basis, that transactions that should have been monitored by the ATMS were being received by the ATMS and this contributed to the situation whereby the Time Stamp Code Logic Error continued for nearly three years before it was identified.

5.6.2. There was no adequate process in place to deal with Bad Data rejected from the ATMS: Metro did not take sufficient steps to ensure that the exceptions process for dealing with rejected Customer Records was adequate and there were no processes in place to deal with rejected Account Records and Transaction Records.

5.6.3. Bad Data was recognised as a risk and a serious issue at comparatively less senior grades within Metro and individual staff members investigated and attempted to escalate this to more senior staff and Committees in 2017 and 2018. However, reference to Bad Data was removed from the Financial Crime Steering Group’s January 2018 minutes, on the basis that the Bad Data issue did not appear to be substantiated, which meant there was no action to track and monitor this risk. Despite the issue not having been resolved, the Financial Crime Steering Group did not discuss Bad Data again until after the Time Stamp Code Logic Error had been identified in April 2019. Likewise, the Working Group and the Operations Risk Board escalated Bad

Data to senior staff within Metro in 2018, but no substantive action took place.

5.6.4. During the Relevant Period, Metro did not have a sufficient understanding of the level of AML risk associated with unmonitored transactions. This was, in part, due to the fact that the true picture of the volume of transactions rejected by the ATMS (and which therefore went unmonitored) was obscured by the presence of internal transactions which did not need to be monitored. This issue took Metro over four years to resolve and it was only on 14 December 2020, shortly before the end of the Relevant Period, that Metro implemented a fix to remove internal transactions from the data feed into the ATMS.

5.7. These transaction monitoring failings resulted in over 60 million transactions with a value of over £51 billion not being monitored during the Relevant Period. Whilst many of these transactions were subsequently reviewed as part of a remediation exercise, there was a lengthy delay in the identification of suspicious activity and this increased the risk of Metro inadvertently being used for the purposes of financial crime.

6. SANCTION

Financial penalty

6.1. The Authority's policy for imposing a financial penalty is set out in Chapter 6 of the Decision Procedure and Penalties manual ("DEPP"). In respect of conduct occurring on or after 6 March 2010, the Authority applies a five-step framework to determine the appropriate level of financial penalty. DEPP 6.5A sets out the details of the five-step framework that applies in respect of financial penalties imposed on firms.

Step 1: disgorgement

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

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

6.4. Step 1 is therefore £0.

Step 2: the seriousness of the breach

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

6.6. The Authority considers that the revenue generated by Metro is indicative of the harm or potential harm caused by its breach. The Authority has therefore determined a figure based on a percentage of Metro's relevant revenue. Metro's relevant revenue is the total revenue derived by Metro from its customers during the period of the breach. The period of Metro's breach was from 6 June 2016 to 17 December 2020 inclusive. The Authority considers Metro's relevant revenue for this period to be £2,117,492,472.

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:

6.8.1. The breach revealed serious or systematic weaknesses in the firm's procedures or in the management systems or internal controls relating to all or part of the firm's business; and

6.8.2. 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:

6.9.1. There was no or little loss or risk of loss to consumers, investors or other market users individually and in general.

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 £2,117,492,472.

6.11. Step 2 is therefore £317,623,870.

6.12. Pursuant to DEPP 6.5.3G(3), 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 figure that (at Step 2) is proportionate to the breach, and having taken into account previous cases, the Step 2 figure is reduced to £23,821,790.

Step 3: mitigating and aggravating 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 that the following factors aggravate the breach:

6.15.1. Since 1990, JMLSG has published detailed written guidance on AML controls. During the Relevant Period, JMLSG provided guidance on compliance with the legal requirements of the Money Laundering Regulations, regulatory requirements in the Handbook and evolving practice in the financial services industry.

6.15.2. Before the Relevant Period, the Authority published the following guidance in relation to AML controls:

6.15.2.1. In March 2008, the Authority issued its findings of a thematic review of firms' anti-money laundering processes in a report titled *'Review of firms' implementation of a risk-based approach to anti-money laundering'*. The report included examples of good industry practice, such as large firms using automated transaction monitoring, and reminded firms that their approach to AML should be aligned with JMLSG guidance;

6.15.2.2. In June 2011, the Authority issued a report titled *'Banks' management of high money-laundering risk situations: How banks deal with high-risk customers (including politically exposed persons), correspondent banking relationships and wire transfers'*. The report notes that *"Banks must be able to identify and scrutinise unusual transactions, or patterns of transactions which have no apparent economic or visible lawful purpose, complex or unusually large transactions and any other activity which is regarded as particularly likely to be related to money laundering"*; and

6.15.2.3. In December 2011, the Authority published *'Financial Crime: A Guide for Firms'*. This included guidance on the requirements of automated transaction monitoring and good and poor practices.

6.15.3. The Authority has also published a number of notices against firms for AML weaknesses both before and during the Relevant Period, including in respect of 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.

6.15.4. Metro was accordingly aware, or ought to have been aware, of the importance of establishing, implementing and maintaining adequate AML systems and controls.

6.15.5. Metro was previously fined £10,002,300 by the Authority for its contravention of Listing Rule 1.3.3R (misleading information not to be published) as it published inaccurate information concerning the figure for Risk Weighted Assets in its Q3 trading update on 24 October 2018.

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

6.16.1. Metro's cooperation during the investigation of the breach was materially above the Authority's expectations.

6.16.2. The Bank has taken substantial remedial steps in respect of its financial crime framework and has implemented a Financial Crime Improvement Programme. Metro has made significant investment in additional resource and capability to manage the Bank's financial crime risk.

6.17. Having taken into account these aggravating and mitigating factors, the Authority considers that the Step 2 figure should not be increased or decreased.

6.18. Step 3 is therefore £23,821,790.

Step 4: adjustment for deterrence

6.19. 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.

6.20. The Authority considers that the Step 3 figure of £23,821,790 represents a sufficient deterrent to Metro and others, and so has not increased the penalty at Step 4.

6.21. Step 4 is therefore £23,821,790.

Step 5: settlement discount

6.22. 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.

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

6.24. Step 5 is therefore £16,675,253.

Proposed penalty

6.25. The Authority hereby imposes a total financial penalty of £16,675,200 on Metro for breaching Principle 3.

7. PROCEDURAL MATTERS

7.1. This Notice is given to Metro under and in accordance with section 390 of the Act. The following statutory rights are important.

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 Metro to the Authority no later than 26 November 2024.

If the financial penalty is not paid

7.4. If all or any of the financial penalty is outstanding on 26 November 2024, the Authority may recover the outstanding amount as a debt owed by Metro 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 you 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 Richard Topham at the Authority (email: Richard.Topham@fca.org.uk / phone number: 0207 066 1180).

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

ANNEX A

RELEVANT STATUTORY AND REGULATORY PROVISIONS

RELEVANT STATUTORY PROVISIONS

1.1. 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).

1.2. 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

Principles for Businesses

2.1. 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.

2.2. Principle 3 provides:

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

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

2.3. 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".

2.4. SYSC 6.3.1R states:

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

(1) enable it to identify, assess, monitor and manage money laundering risk; and
(2) are comprehensive and proportionate to the nature, scale and complexity of its activities".

2.5. SYSC 6.3.3R states:

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

2.6. 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."

2.7. 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

2.8. 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

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

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