12 Endeavour Square
London
E20 1JN

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

DECISION NOTICE

To:	**HSBC Bank plc**
Firm Reference Number:	**114216**
Address:	**8 Canada Square, London, E14 5HQ**
Date:	**14 December 2021**

1. ACTION

1.1. For the reasons given in this Notice the Authority has decided to impose on HSBC Bank plc ("HSBC") a civil penalty of £63,946,800.

1.2. HSBC 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 £91,352,600.

2. SUMMARY OF REASONS

2.1. All authorised firms are required to have systems and controls in place to mitigate the risk that they might be used to commit financial crime. Firms must satisfy the Authority that they have adequate internal control mechanisms to manage their financial crime risk. Firms can detect, prevent and deter financial crime by using effective systems and controls.

2.2. A firm must carry out ongoing monitoring of its business relationships. This includes scrutiny of transactions undertaken throughout the course of a relationship to ensure that transactions are consistent with a firm's knowledge of the customer, business and risk profile.

2.3. The Money Laundering Regulations 2007 (the "ML Regulations"), which were in force during the relevant period, required firms to establish and maintain appropriate and risk-sensitive policies and procedures relating to that ongoing monitoring of business relationships in order to prevent money laundering and terrorist financing. Firms were also required to establish and maintain appropriate and risk-sensitive policies and procedures for the monitoring and management of compliance with, and internal communication of, those policies and procedures. The purpose of monitoring is to identify unusual or uncharacteristic behaviour by customers and patterns of behaviour which are characteristic of money laundering or terrorist financing, which after analysis may lead to a suspicion of money laundering or terrorist financing. It can also help firms to know their customers, assist in assessing risk and provide assurance that the firm is not being used for the purposes of financial crime.

2.4. HSBC is part of HSBC Group, which is one of the largest banking and financial services institutions in the world. At the end of the relevant period HSBC had 13.6 million active customers and during the relevant period 2 of its key transaction monitoring systems monitored around 284.8m transactions per month. With such significant volumes of customers and transactions, HSBC used automated transaction monitoring systems to seek to establish and maintain appropriate risk-sensitive policies and procedures prescribed under the ML Regulations. HSBC also had policies to monitor and manage those automated transaction monitoring systems. The standards set by these polices reflected HSBC's understanding of the key components required in automated transaction monitoring systems appropriate for a firm such as HSBC, including those key components that are the subject of this Notice.

2.5. Between 31 March 2010 and 31 March 2018 (the "relevant period"), HSBC failed to comply with the ML Regulations because its policies and procedures for 2 of its key automated transaction monitoring systems were not appropriate or sufficiently risk-sensitive, and HSBC did not ensure the policies that managed and monitored those systems were adequately followed. This is because, despite being aware of their importance from as early as December 2007, 3 key components of HSBC's automated transaction monitoring systems were deficient:

(1) **Scenario coverage:**

a. a failure to consider whether scenarios covered risk indicators faced by HSBC until 2014 and a failure to carry out timely risk assessments for the new scenarios rolled out after 2016;
b. inadequate monitoring coverage for risk indicators faced by HSBC; and
c. design issues with two of the scenarios rolled out after 2016 which contributed to a significant number of overdue alerts delaying the identification of potentially suspicious activity.

(2) **Parameters:**

a. a failure to test and update thresholds prior to 2016 and new thresholds rolled out after 2016 to ensure that potentially suspicious activity was being identified;
b. certain thresholds set in such a way that it was almost impossible for the relevant scenarios to identify potentially suspicious activity; and
c. the inclusion of rules that suppressed instances of potentially suspicious activity prior to August 2016 and a failure to understand those rules.

(3) **Data:**

a. a failure throughout the relevant period to check the completeness and accuracy of data fed into its transaction monitoring systems;
b. a failure to maintain a list of its correspondent banking relationships so that all necessary data could be fed in and monitored; and
c. incomplete and inaccurate data fed into the automated transaction monitoring systems. Together these failings often meant types of transactions which were in the millions in volume and billions of pounds in value were either monitored incorrectly or not at all.

2.6. Despite its policies requiring HSBC to maintain each of these components throughout the relevant period, HSBC failed to do so. HSBC identified some of these deficiencies as early as March 2010. HSBC later undertook a large-scale remediation programme beginning in late 2012, which spanned multiple years. In doing so, HSBC made material progress in addressing many of the deficiencies that they had identified. However, notwithstanding the considerable investment made, its transaction monitoring systems still had serious weaknesses throughout the relevant period. HSBC continued to invest in future remediation in order to address these weaknesses even after the relevant period.

2.7. The Authority therefore considers that HSBC has failed to comply with:

(1) Regulation 20(1)(a) of the ML Regulations to establish and maintain appropriate and risk-sensitive policies and procedures; and

(2) Regulation 20(1)(f) of the ML Regulations to establish and maintain appropriate and risk-sensitive policies and procedures for the monitoring and management of compliance with, and internal communication of, those policies and procedures.

Consequently, HSBC did not establish and maintain appropriate and sufficiently risk-sensitive policies and procedures to identify unusual transactions or those that may be indicative of money laundering or terrorist financing.

2.8. The Authority considers HSBC's failings to be particularly serious because:

(1) Many of the failings occurred over a prolonged period of time despite numerous internal and external reports highlighting these failings throughout the relevant period. This meant that for a prolonged period of time HSBC failed adequately to detect and report potentially suspicious activity; these reports may have assisted law enforcement in their active investigations;

(2) HSBC was also put on notice of the potential weaknesses in this area in 2012 when the U.S. Department of Justice found that HSBC Group's U.S. subsidiary failed to monitor wire transactions from Mexico, partly due to failings in CAMP. This prompted the Authority to direct HSBC Group to review relevant Group policies and procedures to ensure that all parts of the Group were subject to standards equivalent to those required under UK requirements and to instruct a Skilled Person in 2013 (who was also the U.S. Department of Justice's Monitor). This action was separate to but coordinated with the action by the U.S. Department of Justice; and

(3) Relevant guidance was issued by the Authority both before and during the relevant period in which it stressed the importance of maintaining appropriate financial crime controls.

2.9. For the avoidance of doubt, the matters addressed in this Notice are specific to the UK and relate to HSBC's compliance with the ML Regulations which apply to the UK and which were not part of the action taken by the U.S. Department of Justice in 2012.

2.10. Although HSBC did not have adequately effective automated transaction monitoring systems throughout the relevant period, the Authority recognises HSBC's commitment to its large-scale global remediation programme and there were some successful enhancements. These included the introduction of systems which allowed HSBC to conduct data integrity checks and complete data mapping before the data was fed into its automated transaction monitoring systems. In addition, it implemented a new segmentation methodology with customers based on line of business, customer type, historic transactional activity and risk rating.

2.11. In light of the above failings, the Authority has decided to impose a financial penalty of £63,946,800 after 30% (stage 1) discount (£91,352,600 before discount) pursuant to Regulation 42 of the ML Regulations.

2.12. For the avoidance of doubt, no criticism is made of any person other than HSBC in this Notice.

3. DEFINITIONS

3.1. The definitions below are used in this Notice.

"2011 Skilled Person report" means a report produced in July 2011 by a Skilled Person appointed by the Authority under section 166 of the Act to test the extent to which AML systems and controls in place at HSBC, relating to monitoring for suspicious activity and management of cases identified as actually or potentially suspicious, were fully compliant with the Authority's Rules and Principles for Business, the ML Regulations and the JMLSG Guidance 2007;

"2014 external report" means a report provided by an external party commissioned by HSBC as part of the TMO project which provided findings and recommendations to improve the design and effectiveness of HSBC's AML monitoring systems;

"2014 CB external report" means a separate report commissioned by HSBC as part of the TMO project on correspondent banking which was provided by the same external party that provided the 2014 external report;

"Above the Line" or "ATL" testing means reviewing alerts generated by a transaction monitoring system to ensure that the thresholds for generating those alerts are appropriate;

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

"alert" in this Notice means a notification by a transaction monitoring system to indicate that a transaction violates one or more of the rules run against it which are then reviewed to determine whether there is potentially suspicious activity;

"AML controls" means the controls used by HSBC to identify money laundering and terrorist financing, which included customer due diligence policies and procedures, transaction monitoring, financial intelligence units and sanctions screening;

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

"BACS" means Bankers Automated Clearing Service and is an interbank system that processes payments through electronic payment schemes;

"Below the Line" or "BTL" testing means reviewing transactions that do not generate an alert by a transaction monitoring system to ensure that the thresholds are appropriate;

"CAMP" means Customer Activity Monitoring Program and has been used by HSBC since 2002 as its automated transaction monitoring system to detect unusual transactions across RBWM, CMB and GBM;

"CAMP maintenance guide" means the CAMP Alert Generation and Maintenance Guide dated September 2010 which documented tasks to be performed monthly and periodically to ensure the optimum operation of CAMP;

"CMB" means the Commercial Banking Division, 1 of HSBC's 4 global business lines during the relevant period;

"correspondent banking" means the provision of banking-related services by one bank (Correspondent) to an overseas bank (Respondent) to enable the Respondent to provide its own customers with cross-border products and services that it cannot provide them with itself, typically due to a lack of an international network;

"customer segment" in this Notice means customers and accounts grouped together in a transaction monitoring system because they transact similarly with a view to setting risk-based thresholds applied according to that activity;

"data" in this Notice means data fed into HSBC's transaction monitoring systems from other systems that it used;

"data reconciliation" means the process of validating data that is fed from customer and transaction systems, also known as source systems, used by a firm to the transaction monitoring system to confirm that the data being fed is both complete and accurate;

"EEA" means European Economic Area;

"ETL" means Extract, Transform and Load, a new system introduced by HSBC in 2016, which sat between source systems and CAMP allowing HSBC to conduct data integrity checks before the data was fed into CAMP;

"ETMS" means the external transaction monitoring system used by HSBC to monitor correspondent banking customer activity from July 2017 onwards;

"exceptions management reporting process" means a process to identify and escalate any new, deleted or changes to transaction codes, transaction type codes and GMSAS scenario transaction lists in the transaction monitoring system;

"extreme threshold" means a threshold set restrictively high relative to a particular customer segment meaning that it is very difficult for a transaction monitoring system to generate an alert as demonstrated at paragraphs 4.61, 4.62 and 4.67 below;

"false positive alert" means an alert generated by a scenario when one should not be generated due to a system/technical issue (for example, in the coding of the scenario, or a data issue);

"Faster Payments" means a clearing scheme that allows payments to reach a beneficiary's account within 2 hours;

"freezing injunction" means a court order which prevents a person from disposing or dealing with their assets;

"GBM" means the Global Banking and Markets Division, 1 of HSBC's 4 global business lines during the relevant period;

"GMSAS" means the Global Minimum Standard Anti-Money Laundering Scenarios, a new suite of 15 scenarios that were rolled out in CAMP in 2016;

"GPB" means the Global Private Bank Division, 1 of HSBC's 4 global business lines during the relevant period;

"GPS" means HSBC's Global Payments System, a global payment platform used by HSBC in the UK;

"HSBC" means HSBC Bank plc, the UK authorised entity of HSBC Group prior to restructuring on 1 July 2018; at which point Retail Banking & Wealth Management (RBWM), UK Commercial Banking (CMB) and UK Private Banking became a ring-fenced bank (HSBC UK Bank plc), and Global Banking and Markets (GBM) became a non-ring-fenced bank and remained as HSBC Bank plc;

"HSBC Group" means HSBC Holdings plc which is the principal group holding company. This is organised according to its global businesses and global support functions. These are underpinned by its legal entity structure, which is made up by a global network of locally incorporated subsidiary companies that provide oversight at a country and regional level;

"HMRC" means Her Majesty's Revenue and Customs;

"HUB" means HSBC Universal Banking system. It provides a range of multi-currency banking products and services for International and Retail customers of HSBC and is the international equivalent of RPS;

"JMLSG" means the Joint Money Laundering Steering Group. The JMLSG is a body comprised of the leading UK trade associations in the financial services sector;

"JMLSG Guidance 2007" means the Joint Money Laundering Steering Group – Prevention of Money Laundering / Combating Terrorist Financing Guidance dated December 2007;

"JMLSG Guidance 2017" means the Joint Money Laundering Steering Group - Prevention of Money Laundering / Combating Terrorist Financing Guidance dated June 2017;

"Large Reportable Transaction scenario" means a GMSAS scenario that is designed to identify transactions that exceed a specified threshold;

"ML Regulations" means the Money Laundering Regulations 2007, which were in force in respect of conduct beginning after 15 December 2007 and before 26 June 2017 inclusive;

"money laundering" means a number of activities including trying to turn money raised through criminal activity into "clean" money, handling the benefit of acquisitive crimes such as fraud, handling stolen goods, being directly involved with any criminal or terrorist property and criminals investing the proceeds of their crimes into the whole range of financial products;

"Monitor" means an external party that was appointed pursuant to a deferred prosecution agreement between the U.S. Department of Justice and HSBC Group

and as a Skilled Person pursuant to related orders issued by the Authority to evaluate the overall effectiveness of HSBC's AML and sanctions compliance program and to make recommendations for strengthening the program;

"MPS" means HSBC's Multicurrency Payment System which processes high-value sterling, Euro and foreign currency payments for beneficiaries within the UK and abroad;

"NCA" means the National Crime Agency;

"on-behalf-of payments" means payments made on behalf of a third party who is not HSBC's direct customer;

"orphan accounts" mean accounts which cannot be matched to a specific customer and, in automated transaction monitoring, associated alerts generated are often unworkable if they cannot ultimately be matched to a customer;

"overdue alerts" means alerts generated by HSBC's automated transaction monitoring systems that had not been investigated or closed after a specified time period having been escalated for manual review. This period of time was 67 calendar days prior to May 2016 and 90 calendar days after May 2016;

"parameters" in this Notice mean the mechanism which determines when alerts are generated in a transaction monitoring system and assists the system in achieving the desired quality of alerts;

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

"Production Order" in this Notice means an order made under section 345(4)(a) of the Proceeds of Crime Act 2002;

"RBWM" means Retail Banking and Wealth Management, 1 of HSBC's 4 global business lines during the relevant period;

"relevant period" means the period from 31 March 2010 to 31 March 2018 inclusive;

"Respondent bank" – see the definition of Correspondent Banking;

"risk indicator" means a type of activity being carried out that could indicate money laundering;

"round amount" or "round value" transactions mean transactions that end in a round amount such as 000.00 which HSBC recognised as a possible indicator of money laundering;

"RPS" means HSBC's Retail Processing System, which is a suite of systems that cover the core functionality of UK customer and business accounts, with the exception of credit cards;

"SAR" means Suspicious Activity Report, which is a mechanism to alert law enforcement to potential instances of money laundering or terrorist financing;

"SCC" means Special Categories of Clients which were certain categories of HSBC clients that posed greater money laundering risks, requiring a more stringent approval process;

"scenario coverage" involves looking at whether scenarios cover indicators in risk assessments, industry guidance and the flow of transactions. It includes the extent to which an automated transaction monitoring system can detect unusual activity that may involve money laundering or terrorist financing with appropriate account taken of the frequency, volume and size of transactions with customers and certain transaction characteristics, such as the geographic destination or origin of a payment;

"scenarios" in this Notice mean automated rules used by HSBC in its transaction monitoring systems that are intended to help identify unusual transactions or activity which could relate to money laundering or terrorist financing;

"segmentation" in this Notice means placing customers into demonstrably meaningful customer groups based on factors such as their risk rating and historical transactional activity to which different treatments of the scenarios can then be applied to ensure effective monitoring appropriate to the segment profile;

"SEPA payment" means Single European Payments Area and aims to make sure that European consumers, businesses and public authorities can make and receive payments in euro under the same basic conditions, rights and obligations and were introduced prior to the start of the relevant period;

"Skilled Person" means a person appointed to provide a report under section 166 of the Act;

"source systems" means the systems used by HSBC which feed data into its transaction monitoring systems and includes systems such as GPS, HUB, MPS and RPS;

"structuring" means an activity that may indicate money laundering and involves money launderers structuring their transactions in such a way as to avoid detection;

"suppression rules" mean rules that were applied to CAMP to suppress generated alerts. These alerts were then automatically discounted and not escalated for manual review and investigation;

"SWIFT payment" means a global provider of secure financial messaging services;

"terrorist financing" is similar to money laundering except that often only small amounts of money are required to commit terrorist acts and terrorists can be funded from legitimately obtained income;

"threshold tuning and optimisation" means looking at the alerts that are being generated by a transaction monitoring system (known as Above the Line or ATL testing – see definition above) and at transactions that do not generate an alert (known as Below the Line or BTL testing – see definition above). This ensures that

the thresholds for generating an alert for a scenario both identify unusual activity that might otherwise be missed and do not generate too many false positives;

"thresholds" in this Notice mean a parameter used in CAMP and ETMS to generate an alert for a scenario;

"TMO" means the Transaction Monitoring Optimisation project, a UK project which formed part of HSBC's response to the 2012 Deferred Prosecution Agreement with the U.S. Department of Justice which aimed to have an optimised transaction monitoring system, have the organisational capability to constantly review and update AML data and systems and ensure an appropriate strategic architecture in place to monitor all UK transactions;

"TMPIP" means Transaction Monitoring Post Implementation Project, a programme of work which post-dated the roll out of the GMSAS scenarios in 2016 and was scoped to address ongoing issues with the GMSAS scenarios, segmentation and thresholds;

"transaction mapping" means the mapping of transaction types from source systems to transaction monitoring systems;

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

"Unexplained Wealth Order" means an order in relation to a property made by a court under section 1 of the Criminal Finances Act 2017 which requires a respondent to provide a statement setting out the nature and extent of their interest in that property, explaining how the respondent obtained the property and any other specified information;

"unproductive alert" means an alert that is validly generated by a scenario but is not considered necessary to escalate via manual review in order to file a SAR;

"Unusual Activity Report" means a report made by a HSBC Group employee when transactions or activity is identified as being potentially suspicious; and

"User Defined Rules" or "UDRs" mean targeted rules that were introduced into CAMP in 2016 to detect UK specific behaviours.

4. FACTS AND MATTERS

Background

Structure and customer base

4.1. HSBC is a member of HSBC Group. HSBC Group is one of the largest banking and financial services organisations in the world operating in 64 countries and territories. HSBC Group has over 40 million customers worldwide.

4.2. The UK is a significant market for HSBC Group, with 30% of their customer accounts based in the UK, and saw USD$431bn in customer deposits and USD$281bn in customer lending as at 31 December 2020. HSBC Group's UK revenue in 2020 was USD$13.9bn. Since 1 July 2018, HSBC Group's UK operations have been split into ring-fenced and non-ring-fenced branches which are legally distinct, operationally separate and economically independent.

4.3. As at 31 December 2017, HSBC had 13.6 million active UK customers. Given the size of the UK customer base, an extensive range of products and services were offered across all 4 of HSBC Group's global business lines during the relevant period, all of which operated in the UK. These business lines were:

(1) Retail Banking and Wealth Management (RBWM). As at 31 December 2017, 12.7 million UK customers fell under this business line and HSBC undertook transactions with a total value of USD$106bn on these customers' behalf. The vast majority (84%) of HSBC's customers were classified as low risk rated RBWM customers;

(2) Commercial Banking (CMB). As at 31 December 2017, 871,537 UK customers fell under this business line and HSBC undertook a total of 76.5m transactions with a total value of USD$3.5tn on these customers' behalf;

(3) Global Banking and Markets (GBM). As at 31 December 2017, 26,231 UK customers fell under this business line and HSBC undertook a total of 30.1m transactions with a total value of $148.8tn on these customers' behalf;

(4) Global Private Bank (GPB). As at 31 December 2017, 7,132 UK customers fell under this business line and HSBC undertook a total of 58,721 transactions with a total value of USD$25.8bn on these customers' behalf.

4.4. HSBC also provides correspondent banking services. Correspondent banking was recognised by the ML Regulations as an activity requiring risk based enhanced monitoring. As at March 2018, HSBC had approximately 850 correspondent banking relationships. Between June 2017 and March 2018, HSBC monitored 110m correspondent banking transactions using ETMS with a total value of £101.3tn.

4.5. UK firms are required by the ML Regulations to establish and maintain appropriate and risk-sensitive policies and procedures in order to minimise the risk of their being used by those seeking to launder the proceeds of crime, evade financial sanctions, or finance terrorism. The purpose of monitoring is to identify unusual or uncharacteristic behaviour by customers and patterns of behaviour which are characteristic of money laundering or terrorist financing, which after analysis may lead to a suspicion of money laundering or terrorist financing. It can also help firms to know their customers, assist in assessing risk and provide assurance that the firm is not being used for the purposes of financial crime. Given the large volume of transactions that HSBC needed to monitor, as part of its wider financial crime systems and controls, it used an automated transaction monitoring system to seek to establish and maintain the policies and procedures prescribed under the ML Regulations.

Overview of AML legal and regulatory obligations

Money Laundering Regulations 2007

4.6. A firm must carry out ongoing monitoring of a business relationship on a risk-sensitive basis. This includes scrutiny of transactions undertaken throughout the course of a relationship to ensure that transactions are consistent with a firm's knowledge of the customer, business and risk profile.

4.7. In order to prevent activities relating to money laundering and terrorist financing, a firm must establish and maintain appropriate and risk-sensitive policies and procedures relating to the ongoing monitoring of business relationships.

4.8. In addition, a firm must 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.

4.9. These policies and procedures referred to above must provide for the identification and scrutiny of:

(1) complex or unusually large transactions;

(2) unusual patterns of transactions with no apparent economic or visible lawful purpose; and

(3) any other activity which the firm regards as particularly likely by its nature to be related to money laundering or terrorist financing.

JMLSG guidance

4.10. The ML Regulations provide that, when considering whether a failure to comply with the ML Regulations has occurred, the Authority will have regard to whether a firm has followed guidance approved by the Treasury, such as the JMLSG Guidance, or

issued by the Authority. Guidance concerning monitoring customer activity is set out below and reflects the JMLSG Guidance 2007 and JMLSG Guidance 2017.

4.11. Monitoring customer activity can identify unusual activity which, if not rationally explained, may involve money laundering or terrorist financing. Monitoring customer activity and transactions helps firms to know their customers, assist in assessing risk and provide assurance that the firm is not being used for the purposes of financial crime.

4.12. Essential to a monitoring system is that it flags up transactions and/or activities for further examination, ensures the reports are reviewed promptly by the correct person and appropriate action is taken on the findings of any further examination.

4.13. Monitoring is not necessarily a mechanical process but the scope and complexity of it will be influenced by a firm's business activities and whether the firm is large or small. A monitoring system may be manual or automated but for firms where there are significant issues of volume, a more sophisticated automated system may be necessary. The greater the volume of transactions, the less easy it will be for a firm to monitor them without the aid of some form of automation.

4.14. Correspondent banking is, in the main, non-face to face business and must be regarded as potentially high risk from a money laundering and/or terrorist financing perspective. Correspondents often have limited information regarding the nature or purpose of the underlying transactions, particularly when processing electronic payments or clearing cheques. Monitoring can help to mitigate the money laundering risks when undertaking correspondent banking customer activity and the monitoring guidance set out at paragraphs 4.10 to 4.13 above also applies to such activity. Where there is a correspondent banking relationship, the level of monitoring undertaken on a Respondent bank's activity should be commensurate with the risks posed by the Respondent bank. This is likely to include monitoring the Respondent's activity with high-risk geographies or anomalies in behaviour. Due to the high volume activity involved in correspondent banking, automated transaction monitoring is often the normal approach.

4.15. HSBC has both significant numbers of customers and significant volumes of transactions. HSBC had 13.6 million active customers in the UK as at 31 December 2017, and during the relevant period an average of 272.6m transactions per month were monitored by CAMP, and an average of 12.2m correspondent banking transactions per month were monitored by ETMS. This being the case, HSBC used an automated transaction monitoring system in order to seek to establish and maintain appropriate and risk-sensitive policies and procedures relating to ongoing monitoring which could identify and scrutinize the types of transactions set out in the ML Regulations.

4.16. For a firm that uses automated transaction monitoring, such as HSBC, certain components (and associated policies and procedures) within its automated

transaction monitoring system are important to ensure that it is compliant with the ML Regulations. During the relevant period, HSBC's monitoring systems had a number of components which influenced their effectiveness. HSBC should therefore have been aware of the importance of these components to an effective automated transaction monitoring system from before, and during, the relevant period. These included:

(1) ***Scenario coverage:*** HSBC used scenarios in its automated transaction monitoring systems which were automated rules that can identify unusual transactions or activity which relate to potential money laundering or terrorist financing. Firms needed to consider the risk indicators which could be addressed by any monitoring system that it used and whether they were relevant to their line of business. It was important that the frequency, volume and size of transactions, in the context of the risk these present, were taken into account, and there was a considered identification of the characteristics of the transaction, including whether it was unusual and the geographic location. What is an unusual or uncharacteristic transaction was often defined by a monitoring system and should be in line with the nature of the business being conducted. HSBC assessed scenario coverage by looking at whether the scenarios it used covered the risk indicators identified in risk assessments, applicable industry guidance and the flow of transactions;

(2) **Parameters:** A transaction monitoring system generates an alert where there is unusual activity which is then manually reviewed. The effectiveness of a transaction monitoring system depends on the quality of the parameters that determine which alerts were generated. Consideration should be given to the quality of the alerts that are generated and how the system's parameters can achieve this desired quality of alerts; any such alerts needed to be reviewed promptly with appropriate action taken on the findings of any further examination. HSBC used thresholds and (until August 2016) suppression rules as parameters in its automated transaction monitoring systems; and

(3) **Data:** The effectiveness of a transaction monitoring system is heavily reliant on the quality of the data that is fed into it from other systems used by a firm.

4.17. Extracts from the ML Regulations and JMLSG Guidance that are relevant to HSBC's failings are set out in Annex A to this Notice.

HSBC's automated transaction monitoring systems and associated policies

4.18. To seek to comply with the obligation to have appropriate and risk-sensitive policies and procedures to detect unusual transactions, CAMP has been used by HSBC since 2002 as its automated transaction monitoring system across RBWM, CMB and GBM. CAMP monitored an average of 272.6m transactions in the UK per month which

translates to an average of almost 3.3bn transactions annually, with a value in 2017 equating to at least £402tn. CAMP also monitored correspondent banking until July 2017, when ETMS started to do so.

4.19. CAMP and ETMS worked by generating alerts when transactions were indicative of unusual activity by a customer, which were then reviewed to help determine whether there was potentially suspicious activity. If there was potentially suspicious activity, then a SAR would be filed with law enforcement authorities.

4.20. From September 2010 the monitoring and management of CAMP was in part governed by the CAMP Maintenance Guide which provided that the key components of the system needed to be reviewed at least annually and, in some cases, monthly. Despite being aware of this, HSBC did not adequately do so as set out at paragraphs 4.34, 4.37, 4.52, 4.63 and 4.70.

4.21. As set out at paragraph 4.12 above, an essential feature of monitoring is that reports are reviewed promptly by the correct person. To ensure that alerts were reviewed promptly, HSBC used a service level agreement which specified a time period within which alerts, and cases were to be reviewed and closed with or without the filing of a SAR depending on the circumstances. This time period was 67 calendar days after the alert had been escalated for review until May 2016, when it was extended to 90 calendar days in line with what HSBC considered to be industry practice. If alerts had not been reviewed after the expiry of this time period, they were considered to be overdue. If alerts remained open for a lengthy period of time, such as more than 90 days, this could delay the identification of potentially suspicious activity and meant the policies and procedures were not appropriate or sufficiently risk-sensitive.

<u>HSBC's automated transaction monitoring systems during the relevant period</u>

4.22. HSBC was first put on notice that its automated transaction monitoring system was deficient when an internal report from 2010 found that the UK ownership of CAMP was fragmented and that there was a general lack of maintenance of activities in an earlier version of the CAMP maintenance guide, with some activities not undertaken since 2002, as well as a lack of expertise regarding the operation of CAMP. These deficiencies impacted parameters and data.

4.23. The 2011 Skilled Person report found that CAMP was effective in identifying potential alerts, but made findings rated as "Significant" about the lack of controls relating to the accuracy of the data being fed into CAMP and the lack of data reconciliations between CAMP and the information systems feeding it. This report also found that there were numerous threshold settings in CAMP which meant that it was almost impossible to test them all to determine whether these were appropriate.

4.24. In 2012, the U.S. Department of Justice found that HSBC Group's U.S. bank failed to monitor wire transactions from Mexico, partly due to failings in CAMP. These

specific failings did not include the UK subsidiary, but it did prompt the Authority to direct HSBC Group to review relevant Group policies and procedures to ensure that all parts of the Group were subject to standards equivalent to those required under UK requirements. This action was separate to but coordinated with the action by the U.S. Department of Justice.

4.25. From 2013 onwards, HSBC Group put in place a global remediation plan for its AML controls which included UK automated transaction monitoring with a Monitor appointed to oversee compliance with UK anti-money laundering requirements. The UK transaction monitoring project was known as the TMO programme. The 2014 external report and the 2014 external CB report were part of this programme and were prepared on HSBC's instructions to assist it in identifying in more detail the issues which needed to be addressed as part of the remedial work.

4.26. Remediation for transaction monitoring in the UK was due to be completed for RBWM and CMB by June 2016 and for correspondent banking by August 2017. By these dates it was expected that HSBC's systems would reach the appropriate standard. The Authority recognised the scale and complexity of the remediation plan that HSBC was required to undertake as well as the interdependencies within that plan. This was reflected in its acceptance of the amount of time given to HSBC to fulfil the remediation plan.

4.27. In 2016, HSBC rolled out GMSAS which took into account recommendations from the Monitor and provided a new suite of scenarios to the existing CAMP system, new parameters for generating alerts and a new way of processing customer and transactional data. In July 2017, HSBC started using ETMS, a separate transaction monitoring system to CAMP, to monitor correspondent banking activity.

4.28. The Authority acknowledges that changes to the system did improve automated transaction monitoring in comparison to where it had been prior to 2016. However, some key tasks fundamental to an adequately effective automated transaction monitoring system, such as threshold tuning were taken out of scope for the TMO programme so that HSBC was able to implement the remaining key deliverables for transaction monitoring to improve risk coverage as quickly as possible but at the expense of efficiency. These descoped tasks were included in a new programme with a longer timetable, known as TMPIP which was designed to address ongoing issues and was effectively a continuation of the TMO programme. TMPIP was not completed until after the end of the relevant period.

4.29. GMSAS and ETMS had significant limitations and, for both systems, each of the three components listed at paragraph 4.16 above were in a state of regulatory non-compliance throughout the relevant period. This meant that, despite it being aware of this non-compliance as early as 2010, HSBC failed to ensure that its transaction monitoring policies and procedures were appropriate. In addition, HSBC did not adequately monitor and manage those procedures, and so did not meet its legal and regulatory obligations for the entire relevant period.

Deficiencies in HSBC's transaction monitoring components

4.30. The policies and procedures underlying HSBC's transaction monitoring systems were not appropriate or sufficiently risk-sensitive owing to failures throughout the relevant period in three key components of CAMP and ETMS. These were as follows:

(1) Scenario coverage (paragraphs 4.32 to 4.48);

(2) Parameters (paragraphs 4.49 to 4.81); and

(3) Data (paragraphs 4.82 to 4.118).

4.31. From at least September 2010 the importance of these components was recognised in the CAMP maintenance guide. This guide provided that HSBC was responsible for reviewing these components at least annually, and in some cases monthly, to ensure that CAMP produced unusual activity alerts that were relevant and proportionate without too many false positive alerts.

Scenario coverage

Pre-2016 – Retail and Commercial Banking

4.32. HSBC recognised the importance of scenario coverage in the CAMP maintenance guide which provided that it was extremely important to consider, on at least an annual basis, the need for additional scenarios and not to rely solely on the pre-existing scenarios. HSBC should therefore have been reviewing its scenario coverage from at least the publication of the CAMP maintenance guide in September 2010.

4.33. Despite what was set out in the CAMP maintenance guide, CAMP had the same 6 scenarios from when it was implemented in 2002 until 15 new scenarios were put in place in 2016. As a result of the failure to identify the need for new scenarios until 2014, and implement additional scenarios, the scenarios in CAMP prior to 2016 provided inadequate monitoring coverage for the nature, scale and complexity of HSBC's business. This contributed to the policies and procedures underlying the system not being appropriate or sufficiently risk-sensitive.

4.34. It was not until the 2014 external report and the 2014 CB external report that HSBC carried out risk assessments of these scenarios to determine whether the system was effective, and these assessments found that there were significant coverage gaps. By failing to follow the prescribed annual review of its scenario coverage until 2014 HSBC did not recognise until then that it needed new scenarios to monitor certain money laundering and terrorist financing typologies that presented a financial crime risk. Even when it did identify these coverage gaps, these scenarios were only identified at a global level and not tailored specifically to the financial crime risks the UK branch faced.

4.35. Financial crime risks that HSBC faced in the UK and did not identify as potentially requiring to be monitored by CAMP until 2014 included the following:

(1) monitoring a customer's actual activity that was not in line with their expected activity based on onboarding information;

(2) monitoring transactions from specified high-risk countries (other than by wire transfer);

(3) monitoring repeated transactions in round amounts;

(4) detecting non-cash (e.g., wire or cheque) structuring activity; and

(5) monitoring customer's behaviour over a period of time to detect month-on-month changes in customer behaviour.

Customer examples

4.36. The following examples illustrate some of the risks of having scenarios which did not cover certain risk indicators which HSBC only identified that it needed in 2014:

Customer A

(1) Customer A was the company director of a UK construction company with a gross annual income of £40,000, an expected net monthly income of £1,500 and monthly outgoings of £500. An HMRC investigation found that between 2009 and 2011, Customer A had a leading role in a criminal gang involved in an attempt to steal several million pounds by setting up fake construction companies; in May 2014, he pleaded guilty to VAT Fraud and received a custodial sentence.

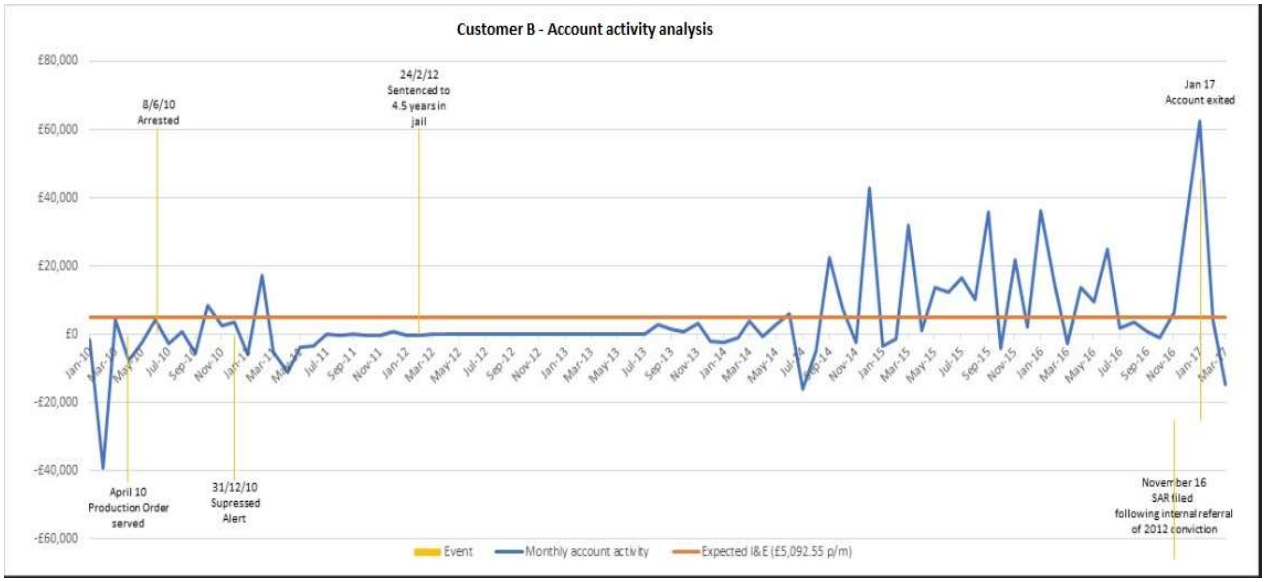
(2) During the period in which he was engaged in this criminal activity, HSBC did not identify certain unusual activity. In April 2010, Customer A received 18 payments totalling £127,000. 16 payments were received on a single day in mid-April and totalled £120,000. This transactional activity was clearly outside of the expected activity for Customer A's account, given his declared income and outgoings. These payments were all round number transactions which, as set out at paragraph 4.35(3) above, HSBC did not identify that it needed to monitor until 2014; these transactions were made up of 8 payments of £10,000 and 8 payments of £5,000. This type of activity is also indicative of structuring and did not generate any CAMP alerts so therefore went undetected by HSBC.

Customer B

(3) On 4 February 2010, Customer B opened a savings account with HSBC and declared a gross annual income of £81,851. On 16 February 2010, there were 5 separate payments made from Customer B's account, all in the sum of £9,830.32 – a total of £49,151 in a single day. Given his gross annual income,

this activity was outside the expected activity for this customer. However, no CAMP alert was triggered. The value of understanding Customer B's transaction activity was demonstrated in May 2010 when HMRC issued a Production Order requesting all documentation relating to customer B's accounts for the period covering June 2007 to May 2010. Customer B was arrested in June 2010 for involvement in an operation to smuggle cigarettes into the UK and, in February 2012, received a custodial sentence for involvement in a conspiracy to evade excise duty chargeable on the importation of cigarettes.

(4) Customer B was subsequently ordered in July 2013 to pay £1.2m to HMRC or face a further four years in prison. From July 2014 until the account was closed in March 2017, there was a sustained period of unusual activity of both incoming and outgoing transactions outside of that expected on the account, but no transaction monitoring alerts were triggered. These transactions were unusual given the expected activity on the account as illustrated in the graph below.



Pre-2016 – Correspondent Banking

4.37. The monitoring of correspondent banking customer activity by CAMP relied on a scenario which did not provide adequate coverage of the financial crime risk presented by the products and services offered to its correspondent banks. A number of risk indicators relevant to HSBC's correspondent banking customer activity were not covered by any scenario, and HSBC did not identify that it needed scenarios until the 2014 external CB report due to their failure to follow the prescribed annual review of its scenario coverage. Scenarios that HSBC identified as potentially needed included the following:

(1) transactions involving high-risk jurisdictions (other than by wire transfer);

(2) attempts to conceal the location of a transaction;

(3) transactions in round amounts;

(4) high-risk originators or beneficiaries of transactions; and

(5) transactions of large amounts.

4.38. Over a 4-year period up until early 2017, the Monitor estimated that 43m correspondent banking transactions were not adequately monitored. A tactical solution to this issue which HSBC introduced in 2015 was identified by the Monitor as inappropriate as it reviewed alerts from an existing CAMP scenario that HSBC acknowledged was not able to identify the risks it faced from its correspondent banking customers. This meant HSBC could not carry out appropriate and sufficiently risk-sensitive monitoring of its respondent banks' transactions to ensure those banks' activities were consistent with its knowledge of their business and risk profile.

Post 2016 – Retail and Commercial banking

4.39. In August 2016, 15 new scenarios were rolled out in CAMP, known as GMSAS scenarios, which covered many of the risk indicators that HSBC had identified as requiring coverage in 2014. Whilst this did significantly increase scenario coverage, these were a global minimum set of scenarios which were not specifically tailored to the money laundering and terrorist financing risks that HSBC faced in the UK. HSBC carried out a review prior to the implementation of GMSAS which compared the number of risk indicators applicable to the UK covered by GMSAS scenarios and pre-2016 CAMP scenarios. The review concluded that the number of risk indicators covered would increase under the GMSAS scenarios. However, HSBC did not fully assess whether CAMP covered all of its money laundering and terrorist financing risks in the UK throughout the relevant period. This was because the risk assessments prior to the implementation of GMSAS did not go into sufficiently granular detail and were not sufficient to ensure operational effectiveness.

4.40. A further limited risk assessment was carried out in the UK prior to the GMSAS scenario rollout, based on a sample of just over 17,000 SARs filed in the UK over the previous year. This indicated that these new scenarios would have covered 88% of the SARs filed but after setting thresholds implemented in August 2016 the scenarios would only identify approximately 10% of the SARs. At the time GMSAS was implemented, HSBC sought to increase coverage of more specific UK money laundering and terrorist financing risks by deploying 6 UDRs, improving

segmentation of customers and planning to deploy an actual versus expected activity scenario.

4.41. However, HSBC only deployed the 6 UDRs which on their own would not fully resolve the coverage gap. 4 of the UDRs implemented contributed to a significant backlog of alerts and were paused in March 2018. The alerts were isolated and following a sampling exercise to assess the risk in the population, the majority (some 72,000) were not reviewed for over a year which left the risk of financial crime going unassessed. All but 1 of the UDRs were permanently removed. In some cases, HSBC was not even able to identify the risk indicator that the UDR was intended to cover.

4.42. It was not until after the rollout of the GMSAS scenarios, that HSBC completed a further, more detailed transaction monitoring risk assessment in the UK. HSBC assessed that the GMSAS scenarios provided 94% coverage of identified risk indicators. However, this 94% coverage figure did not reflect all weaknesses in HSBC's transaction monitoring.

4.43. It was not until this transaction monitoring risk assessment that HSBC identified 124 high-risk gaps in coverage across certain money laundering and terrorist financing risk indicators specific to the UK that needed to be covered by transaction monitoring or another AML control. Although the scenarios in place covered a number of risk indicators, they had not provided coverage for a number of HSBC's UK-specific typologies. These included:

(1) In CMB, a gap in relation to the risk indicator of frequent transactions that were inconsistent with a customer's expected activity or line of business, which was identified as a possible indicator of modern slavery and/or human trafficking;

(2) In RBWM, a gap in relation to the risk indicator where funds were sent to jurisdictions in which there was a known risk of drugs or human trafficking without economic or legal purpose. The GMSAS scenarios that were rolled out only provided partial coverage; and

(3) Also, in RBWM, a gap in relation to the risk indicator where large volumes of cheques were being deposited into accounts where the nature of the account holder's business would not appear to justify such activity, and multiple or frequent deposits were made to various accounts which were purportedly unrelated. This arose from an IT issue where in-branch foreign currency transactions were monitored as internal transfers rather than cash.

4.44. HSBC's assessment that the GMSAS scenarios provided 94% coverage of identified risk indicators also did not reflect the seriousness of the risk indicators not covered. HSBC was unable consistently to identify all of the risk indicators that it should be monitoring against when assessing coverage and subsequently which scenarios should be implemented into CAMP. This was a risk with significant impact and resulted in CAMP being in a state of regulatory non-compliance. This meant that

despite the GMSAS scenarios that were introduced in 2016, for the entire relevant period HSBC had limited assurance that the scenarios in place in CAMP provided sufficient coverage of the money laundering and terrorist financing risks that it faced. This was a direct consequence of HSBC not adhering to its prescribed annual review of scenario coverage from September 2010, even after scenario coverage gaps had been highlighted in April 2014 by the 2014 external report.

CAMP scenario design issues

4.45. Effective monitoring requires alerts to be reviewed promptly and from May 2016 onwards HSBC's policy stipulated that alerts needed to be reviewed within 90 days otherwise these would be overdue. However, the Large Reportable Transaction scenario contributed to a significant backlog of alerts with nearly 35% of alerts generated by this scenario between August 2016 and March 2018 taking more than 90 days to review and so being overdue. This delayed the identification of potentially suspicious activity meaning that policies and procedures for transaction monitoring would not be appropriate or sufficiently risk-sensitive. This was because the scenario was designed in such a way that it did not distinguish between different types of transactions such as cash, wire and cheques. This meant that what CAMP recognised as a large transaction was the same regardless of whether that transaction was made in cash, as a cheque or electronically and the minimum transaction value that could be included in an alert was £25. HSBC rolled out this scenario knowing that this was the case and that doing so would lead to a very high alert volume. The design issue also meant it did not have as large a risk coverage than it would have had if it could have distinguished between transaction types. This design issue was not resolved throughout the relevant period.

4.46. The structuring scenario which was rolled out in 2016 produced alerts on single transactions when, by definition, structuring involves multiple transactions. Just over half of all transactions generated by this scenario related to single transactions. HSBC became aware of the issue 9 months after GMSAS implementation, but did not remediate the issue immediately because, notwithstanding the erroneous generation of alerts on single transactions, these still generated valid SARs. This structuring scenario design issue also contributed to the backlog of alerts referred to in paragraph 4.45 above. This design issue was also not resolved throughout the relevant period.

Post 2016 – Correspondent Banking

4.47. HSBC sought to remediate the previous lack of correspondent banking coverage in its transaction monitoring system, described at paragraphs 4.37 and 4.38 above, using ETMS to monitor correspondent banking customer activity from July 2017. The ETMS system had 12 scenarios taken from GMSAS which targeted various transaction types and customer behaviours which were especially relevant to identifying whether correspondent banking activity was unusual or suspicious which might be indicative of money laundering and/or terrorist financing. However, the

risk assessments carried out prior to rollout were not comprehensive enough and were inaccurate. In particular:

(1) A comprehensive risk assessment had not been carried out which meant it was unclear on what basis HSBC had identified the correspondent banking risk indicators to be monitored by ETMS; and

(2) The assessment of how scenarios covered the list of risk indicators that were identified was not accurate and suggested gaps in coverage. 5 scenarios that were said to partially cover risk indicators did not actually cover the risk indicators at all.

4.48. These risk assessment failings for correspondent banking indicated a critical level of regulatory impact. This contributed to ETMS having significant limitations during the relevant period. Given that the scenarios in place prior to the rollout of ETMS also provided limited coverage of correspondent banking money laundering and terrorist financing risk indicators, it meant that throughout the relevant period HSBC could not be sure that the scenarios it had in place provided sufficient coverage of these risks. Once again, this was a direct consequence of HSBC not reviewing its scenario coverage from at least September 2010, even after scenario coverage gaps had been highlighted in July 2014 by the 2014 external CB report. Accordingly, these aspects of the policies and procedures which HSBC had in place for correspondent banking transaction monitoring were not appropriate or sufficiently risk-sensitive at any point during the relevant period.

Parameters

4.49. As set out in JMLSG, the effectiveness of any transaction monitoring system in identifying unusual activity depends on the quality of the parameters that determine what alerts are generated and need to be appropriate.

4.50. In any monitoring system used, firms should consider how parameters aid a risk-based approach and which will affect the quality and volume of alerts which are generated. Two types of parameters were used in HSBC's automated transaction monitoring systems – thresholds and suppression rules.

Thresholds

4.51. Thresholds are used by HSBC's transaction monitoring systems as a parameter to generate an alert for a scenario. In both CAMP and ETMS, thresholds are tuned by looking at the alerts that are being generated (known as Above the Line or ATL testing) and at transactions that do not generate an alert (known as Below the Line or BTL testing). This ensures that the thresholds for generating an alert for a scenario are appropriate in that they identify unusual activity. The CAMP maintenance guide set out that HSBC should review thresholds on at least an annual basis. However, in some situations, such as where new codes were introduced, the

CAMP maintenance guide stated that it was critical to carry out monthly reviews to ensure effective monitoring and quality alert generation.

Pre-2016

4.52. In the early part of the relevant period, the policies and procedures set out in the CAMP maintenance guide were not adequately followed in that HSBC failed to review thresholds on at least an annual basis. In March 2010 it was found that HSBC did not have sufficient in-house expertise to understand how the thresholds worked. Thresholds were seldom updated and there was little management information or supporting records to explain why thresholds had been set at a certain level. This failure to maintain thresholds meant that by February 2011 7% of the customer segments had no thresholds set at all over an unknown period of time leading to a risk that CAMP would not be generating any alerts for these customers.

4.53. The 2011 Skilled Person report found that the number of threshold settings within CAMP was so large (over 2.8m in total) that it was almost impossible to test them all to determine whether these were appropriate. This finding was rated "Significant" which meant that, if left uncorrected, it could lead to systemic weaknesses and lead to actual or potential regulatory breaches. The Skilled Person recommended that there should be a very significant reduction in the number of thresholds to ensure that these could be tested on a regular basis. A programme to review all thresholds was initiated at the end of 2012 but this identified issues with CAMP's system architecture and data integrity which needed to be addressed before any further review could take place.

4.54. This contributed to a finding in the 2014 external report that the thresholds were ineffective. The 2014 external report also found that there was still no defined process for tuning the excessive and complex threshold settings and no documentation explaining how to set them. This is despite the 2011 internal report and the 2011 Skilled Person report having previously identified these issues.

4.55. Despite the significant findings and recommendations of these internal and external reports dating back to March 2010, the Monitor found that by 2016 more than three-quarters of the thresholds had not been modified since 2012 or earlier.

Post 2016 – CAMP

4.56. The deployment of the GMSAS scenarios in CAMP in 2016 meant that HSBC did not have any historic data available to tune the thresholds for these new scenarios; instead, it applied a statistical approach to set these new thresholds. Whilst HSBC considered this to be an appropriate approach, some 16,000 thresholds were set in just a week with the result that HSBC had little opportunity to examine these thresholds in detail. HSBC anticipated there would be an increase in alerts as result of a conservative approach to threshold setting. HSBC viewed this as an operational matter and sought to address it by employing approximately 650 people to assist

with reviewing alerts. Despite this, the Monitor found that these thresholds led to unsustainable alert volumes.

4.57. The task of tuning the thresholds was descoped from the original TMO programme with the intention to tune the thresholds using the alerts and transaction data generated by CAMP 7 months after the GMSAS scenarios were deployed. By de-scoping the task of threshold tuning HSBC was able to implement the remaining key deliverables for transaction monitoring through the TMO programme with the intention of reducing its risk more quickly. However, whilst some initial assessments of the thresholds were carried out a year after the thresholds were rolled out, threshold tuning was then put on hold pending deployment of the TMPIP programme. TMPIP was not originally anticipated when the scenarios went live in August 2016. HSBC subsequently determined that it was necessary to address a number of technical issues, with optimising thresholds and improving alert quality through threshold tuning becoming part of this programme, in order to address the high volumes of unproductive alerts and an alert volume which HSBC was advised by the Monitor to be unsustainable.

4.58. This unsustainable alert volume contributed to a very high number of overdue alerts that were present during this period, i.e., those alerts that took more than 90 days to be reviewed as specified in HSBC's service level agreement. This delayed the identification of potentially suspicious activity and meant that the policies and procedures could not be said to be appropriate or sufficiently risk-sensitive.

4.59. TMPIP did not go live within the relevant period which left the thresholds untuned. The impact of delaying this threshold tuning was demonstrated by HSBC's own analysis before the new thresholds were activated. This found that when comparing the new thresholds to the thresholds implemented in 2016 , the number of alerts was reduced by 48%, i.e., prior to tuning there were, on average, 319,127 alerts per month and afterwards 164,736 alerts per month. Whilst the number of customers generating alerts broadly remained the same, there was a 13% increase in the number of new customers generating alerts. This demonstrates that the new thresholds were capturing customers not previously monitored who were potentially carrying out suspicious activity.

4.60. The impact of delaying the threshold tuning and the activation of the re-tuned thresholds was further demonstrated when HSBC later assessed the impact of the tuned thresholds, once these thresholds had been introduced:

(1) A significant proportion (c.13%) of RBWM and CMB customers whose activity generated alerts after the threshold tuning would not have generated alerts prior to the threshold tuning. This suggests that a significant proportion of customers whose activity should have generated an alert were not generating alerts prior to the threshold tuning, which indicated that the policies and procedures around this were not appropriate and, in turn, meant that HSBC was less likely to have identified instances of potentially suspicious activity

between the thresholds implemented in 2016 and the introduction of the new thresholds; and

(2) Despite these customers' activity generating alerts, after threshold tuning there was a material reduction in the quantity of alerts which was 52% for RBWM and 44% for CMB customers. This indicated that the policies and procedures around tuning might not previously have been appropriate.

4.61. The delay to threshold tuning also resulted in the persistence of 'extreme thresholds' which meant the thresholds for some scenarios were set in such a way that it was very difficult to generate an alert. This meant there was a risk that the coverage for those scenarios was significantly reduced, sometimes to "*what is effectively non-coverage*", and the ability of CAMP to identify unusual activity was diminished. Notwithstanding this issue, HSBC subsequently determined that extreme thresholds were a low-risk issue.

4.62. The effect of extreme thresholds can be demonstrated by the following examples:

(1) For 1 of the change in behaviour GMSAS scenarios, 52% of RBWM customers (5.4 million customers) and over 570,000 CMB customers needed a 500,000% (or 5,000 times) increase in their yearly peak transactional activity to trigger an alert.

(2) For another change in behaviour GMSAS scenario, a low-risk retail customer who had a medium to high activity level needed their monthly debit activity to increase by 791,900% (or almost 8,000 times) over the preceding 12 months to trigger an alert. These customers, who typically spent £19,322 per month, would have needed to spend over £153m per month (i.e., 791,900% x £19,322) to trigger an alert.

4.63. TMPIP carried out testing for alerts that were generated (ATL testing) but it did not test transactions that did not generate alerts (BTL testing). This had, under CAMP, been an important check that thresholds were set to ensure that potentially suspicious activity was being identified. BTL testing had still not been carried out and so HSBC could not confirm whether thresholds in CAMP were set appropriately and would not miss the identification of suspicious activity. This failure was a risk with a critical impact putting HSBC in a state of regulatory non-compliance. This meant that, despite the new thresholds that were introduced in 2016, for the entire relevant period HSBC had limited assurance that the thresholds in place in CAMP were set at a level that could identify potentially suspicious activity. This was despite the unambiguous requirement in its own CAMP maintenance guide that HSBC should review thresholds on at least an annual basis. Accordingly, these aspects of the policies and procedures which HSBC had for retail and commercial banking transaction monitoring were not appropriate or sufficiently risk-sensitive at any point during the relevant period.

<u>Post 2016 - ETMS</u>

4.64. Thresholds for correspondent banking scenarios in ETMS were set using a statistical method when this system was introduced in 2017 because, as with CAMP, it had no historical data to carry out threshold tuning. This threshold setting only focused on projected alert volumes in each customer segment rather than being risk focused at a level that was appropriate for identifying suspicious activity.

4.65. HSBC also did not document the rationale for how the thresholds were set, creating the risk that this would be difficult to understand for those subsequently using the system. This issue with documenting the rationale for thresholds had previously been identified as far back as 2011. This was a high-risk issue indicating a significant level of regulatory impact during the relevant period.

4.66. HSBC also failed to carry out tuning of the ETMS thresholds during the relevant period; it did not complete testing for alerts that were generated (ATL testing) or for those that were not generated (BTL testing). This meant HSBC was not able to assess whether the ETMS thresholds were set in such a way that it could identify transactions that were indicative of money laundering. This was a high-risk issue indicating a significant level of regulatory impact during the relevant period. This contributed to ETMS having significant limitations during the relevant period.

4.67. Extreme thresholds were also an issue in ETMS which led to a risk that the new correspondent banking scenarios would not generate appropriate alerts. These included 93 instances where the activity of a respondent bank's customer needed to increase by 3,000% in order to generate an alert. These policies and procedures hindered HSBC's ability to carry out adequate monitoring of its respondent banks to ensure their activities were consistent with HSBC's knowledge of their business and risk profile.

Parameters - Suppression rules

4.68. Suppression rules were used from the implementation of CAMP in 2002 until the introduction of the GMSAS scenarios in 2016. Suppression rules were a type of parameter used in CAMP to manage alert volumes and were designed to suppress alerts that were unlikely to be indicative of unusual or suspicious activity. Suppressed alerts were not subsequently reviewed. By 2015, 67% of all alerts generated by CAMP in the UK were being suppressed by these rules.

4.69. From September 2010 the CAMP maintenance guide set out that the suppression rules should be reviewed at least annually to ensure that they were still valid. The CAMP maintenance guide also prescribed that any new suppression rules that were created had to be agreed by a Local Head of Compliance.

4.70. However, HSBC did not fully follow the CAMP maintenance guide and had little assurance that these rules were not suppressing alerts that were in fact indicative of unusual or suspicious activity. This was demonstrated in 2011 when a rule had to be deactivated after it was found to be inadvertently suppressing all alerts generated for retail customer accounts in Wales. As a result, HSBC incorrectly

suppressed 89,000 alerts, and 1,780 SARs had to be subsequently filed as a result once these suppressed alerts had been reviewed. HSBC could not identify the original reasons why this rule had been implemented. Although transactions for an entire region were not being monitored, this was not reported in the 2011 Skilled Person report that was being undertaken at the time.

4.71. Despite becoming aware of this incident as early as 2011, HSBC did not take wider steps to understand and mitigate the risks presented by the suppression rules at that time. Accordingly, it was not until 2013 that HSBC carried out a review of the suppression rules. There was insufficient detail in the available documentation to enable the review team to understand the history and rationale of how the suppression rules worked. This meant that HSBC had to analyse the rules by attempting to reconstruct the logic behind them and often could not understand the business justification for the rules after doing so.

4.72. These rules were suppressing transactions that were unusual when taking into account a customer's profile as illustrated in the cases of Customer A and Customer C below.

Customer A

4.73. As described at paragraph 4.36(1) above, Customer A was the company director of a UK construction company with a gross annual income of £40,000, an expected net monthly income of £1,500 and monthly outgoings of £500. Customer A had a leading role in a criminal gang involved in an attempt to steal several million pounds by setting up fake construction companies; in May 2014, he pleaded guilty to VAT Fraud and received a custodial sentence. In addition to the suspicious activity which did not generate alerts, as set out at paragraph 4.36(2) above, the rules suppressed 5 alerts that otherwise would have been generated for unusual transactions in the years before his conviction, which were as follows:

(1) In February 2011, 3 cheques for £30,000, £5,533.80 and £2,276.22, totalling £37,810.02 were deposited into Customer A's account;

(2) In June 2011, there were 2 cash deposits of £25,000 and £18,000, a cheque deposit of £40,000 and further cash deposits of £20,000, £10,000 and £15,000;

(3) In August 2011, there were 2 cheque payments of £6,800, 1 of which was reversed and credited back to the account the following day. There was then a cheque withdrawal of £10,750;

(4) In September 2011, 4 large cheque payments were made from the account totalling £51,000 (2 x £10,000, £15,000 and £6000); and

(5) In December 2011, there was a cash deposit of £3,000 and a payment of £3,000 just over a week later. A further £17,000 was received followed by a

£17,000 cash withdrawal on the same day. £20,000 was also received, followed by a cash withdrawal of £17,500 on the same day.

Customer C

4.74. Customer C was categorised by HSBC as a low risk rated customer who had an annual income of £100,000 in 2006. Customer C made a number of large and unusual transactions in 2008 and 2009 despite HSBC being put on notice of a freezing injunction in October 2008 over the entirety of his assets and accounts, and this triggering an internal request to inhibit his accounts. These transactions included:

(1) In September 2008, over £27,000 paid into Customer C's accounts and over £54,000 paid out;

(2) In March 2009, over £154,000 paid into Customer C's accounts and over £202,000 paid out;

(3) In June 2009, over £55,000 paid into Customer C's accounts and over £110,000 paid out; and

(4) In September 2009, over £162,000 paid into Customer C's accounts and over £137,000 paid out.

4.75. Whilst 4 transaction alerts appear to have been generated in CAMP during 2008 and 2009, all of these alerts were suppressed and not investigated. Customer C was subsequently placed on the UK Disqualified Directors Register in March 2011 and jailed for 6 years in October 2016 for fraudulently claiming over £4.7m in VAT repayments.

4.76. Even though issues with the suppression rules had been identified previously (as set out at paragraphs 4.70 and 4.71 above), it was not until February 2014 that HSBC decided that suppression rules should be lifted for high-risk customers or those connected to a high-risk country. Further, it was not until 2015, in an incident with Customer D, that HSBC's senior management realised that the financial crime risk presented by these rules was not theoretical but could actually crystallise which meant that these rules could, in practice, be suppressing alerts indicative of suspicious activity.

4.77. After an Unusual Activity Report had been raised against Customer D, a SAR was filed in November 2014. However, HSBC realised that these rules could be suppressing alerts indicative of suspicious activity only after subsequent media reports surfaced about this customer being investigated in an overseas jurisdiction. A review of this customer's accounts found that CAMP had generated 3 alerts against this customer, but all of these had been suppressed by the rules including after the SAR had been filed in November 2014.

4.78. The significance of this crystallised financial crime risk was demonstrated when Customer D subsequently pleaded guilty in an overseas jurisdiction to offences involving fraud and market misconduct and was ordered to pay, amongst other sanctions, a multi-million-dollar financial penalty.

4.79. As a result of this incident, HSBC carried out a lookback exercise where it reviewed a sample of 100,000 alerts out of the 4.4m alerts that had been suppressed by these rules between 2008 and 2016. This sample included all suppressed alerts relating to high-risk customers. 68 SARs were filed as a result of this lookback exercise; 5 of these 68 SARs related to customers categorised as high-risk with the remaining categorised as medium or low risk.

4.80. These 68 SARs all provided examples of these rules suppressing alerts indicative of potentially suspicious activity carried out by:

(1) A customer categorised by HSBC as a high-risk individual with potential links to a known terrorist organisation;

(2) A customer categorised by HSBC as a low-risk individual with connections to a person subject to an NCA Unexplained Wealth Order; and

(3) A customer categorised by HSBC as a low-risk individual suspected of money laundering and where HSBC had been unable to determine the true source of funds into their accounts.

4.81. Although HSBC decided that suppression rules should be immediately lifted for high-risk customers or those connected to a high-risk country in February 2014, it was not until October 2015 that this decision was put into effect. Suppression rules were removed altogether in August 2016 when the GMSAS scenarios had been rolled out.

Data

4.82. The effectiveness of a transaction monitoring system is heavily reliant on the completeness and accuracy of the customer reference data and transaction data. This data was fed into CAMP and ETMS from other customer and transaction systems used by HSBC.

4.83. The importance of data to an effective transaction monitoring system was recognised by HSBC in its CAMP maintenance guide in September 2010. This stated that it was critical for certain customer and transaction data used by CAMP to be reviewed on a monthly basis to ensure effective monitoring and quality alert generation with other customer and transaction data needing to be reviewed on at least an annual basis. In January 2011 HSBC acknowledged that if the process by which associated systems fed data to CAMP consistently failed then it could be exposed to regulatory investigations, punitive action, unfavourable media attention and an associated loss of customer confidence.

<u>Data reconciliations pre-2016</u>

4.84. Data reconciliation is the process of validating data that is fed from a firm's customer and transaction systems ("source systems") to the transaction monitoring system to confirm that this data is both complete and accurate. If the data differs between the source system and the transaction monitoring system, then it could lead to transactions not generating alerts (and therefore not monitored) or too many unproductive alerts being monitored and therefore increasing the risk of delay in identifying potentially suspicious activity.

4.85. As set out at paragraphs 4.85 to 4.88 and 4.101 to 4.103, HSBC failed to carry out data reconciliations throughout the relevant period. Potential procedural issues regarding the incompleteness of data being fed from source systems to CAMP were identified in an internal report as early as January 2011; the report recommended that testing be carried out on transactions to ensure that HSBC had a true picture of the transactions and could amend thresholds accordingly. A report the following month found no evidence that the data feeds into CAMP were enabling it to monitor 100% of transactions and so HSBC could not certify that all potential alerts were being picked up.

4.86. The 2011 Skilled Person report found, notwithstanding that a sample of data from all the source systems were found to feed into CAMP, HSBC did not carry out reconciliations between the customer data in the source systems and in CAMP. This was rated as a "Significant" finding which meant that, if left uncorrected, it could lead to systemic weaknesses and represent actual or potential breaches of regulatory standards. It recommended that HSBC implement a periodic review to ensure that all necessary data was being fed into CAMP.

4.87. Following on from the 2011 Skilled Person report, HSBC did carry out a project to capture and document the data being fed in and out of CAMP. However, the remediation and reviews continued to be limited in nature and failed to identify a number of data integrity issues prior to the 2014 external report. With no process to reconcile the data being fed into CAMP from source systems, prior to 2014 HSBC was not able to identify the extent to which necessary data was being fed into CAMP or whether that data was accurate.

4.88. The 2014 external report identified issues such as gaps in the quality assessments of the data fed from source systems to CAMP and customers flagged as SCC in a source system but missing that flag in CAMP. The 2014 external report recommended carrying out data reconciliation exercises between source systems and CAMP to ensure that data was being correctly sent and received.

Data completeness pre-2016

4.89. Internal reports from 2010 and 2011 raised a number of concerns about whether all relevant data was being fed into CAMP. This included certain types of

transactions not being monitored by CAMP including SEPA payments and certain SWIFT payments. Data completeness issues were considered as part of the TMO.

4.90. Following these earlier warnings, the 2014 external report found a number of data completeness issues concerning CAMP, including duplicate transactions which increased the risks of overdue alerts, in turn delaying the identification of potentially suspicious activity. These included, over a 6-month period between October 2012 and March 2013:

(1) Around 1.3m HUB transactions with a value of approximately £24.1bn were duplicated in CAMP resulting in an increase in alert volume;

(2) 12m duplicate transactions with a value of over £36tn as a result of the GPS and HUB source systems sending the same feeds into CAMP;

(3) Over 7m internal and operational accounts which should have been excluded from CAMP were actually included which meant there was an increase in false positive alerts;

(4) Around 4,500 GPS transactions with a value of approximately £1.1bn were not sent to CAMP for monitoring; and

(5) Over 100,000 RPS transactions with a value of £158m which should have been excluded from CAMP were actually included which, in turn, skewed alert volumes.

4.91. There were also issues concerning the monitoring of SEPA payments. These payments ensure that European consumers, businesses and public authorities can make and receive payments in euro under the same basic conditions, rights and obligations. HSBC identified in the early part of the relevant period that SEPA payments were excluded from CAMP when they should not have been and these only started to be monitored by CAMP in 2014. However, due to a rule intended to prevent duplicate monitoring of transactions, around 12% of all SEPA payments were excluded from CAMP from April 2014 onwards.

4.92. Data completeness was also an issue in the monitoring of correspondent banking activity. HSBC was significantly hindered in its monitoring of correspondent banking because, as first identified in the 2014 CB external report, it did not maintain a list of correspondent banking relationships and products offered in that context. This meant a significant number of accounts and transactions on its correspondent banking accounts were not being identified by CAMP for effective monitoring. Over a 6-month period between October 2012 and March 2013, as a result of this issue, an additional 12,122 correspondent banking accounts undertaking 21.6m transactions with a value of £107bn were not identified.

4.93. This failure to monitor significant volumes and values of respondent bank customers' transactions meant HSBC could not carry out adequate monitoring of its

respondent banks to ensure those banks' activities were consistent with its knowledge of their business and risk profile.

4.94. There were other correspondent banking data completeness issues identified in the 2014 CB external report including over a 6-month period:

(1) 22.1m transactions with a total value of £454.1bn from 6 source systems consisting of wires, cheques, BACS and Faster Payments had not been fed into CAMP. This is despite over 80% of the transactions being recorded in the source systems; and

(2) 13.5m transactions with a value of £36.9tn in HUB were duplicates of transactions found in GPS resulting in potential increased alert volume.

Data accuracy pre-2016

4.95. Prior to 2014, there were concerns raised within HSBC about the quality of the data being fed into CAMP and the effect this had on the quality of the alerts being produced. The 2011 Skilled Person report found that outdated reference data could be fed into CAMP and there was no process to review data feeds. This was rated as a "Significant" finding which meant that, if left uncorrected, it could lead to systemic weaknesses and could be actual or potential breaches of regulatory requirements. Data accuracy was therefore also considered as part of the TMO.

4.96. Following this earlier warning, the 2014 external report found a number of data accuracy issues concerning CAMP including, over a 6-month period between October 2012 and March 2013:

(1) Data quality issues, including transaction codes and customer identifiers that were missing or inconsistent, affecting transactions to a value of £1bn per month;

(2) Country of residence and nationality codes were not captured in CAMP, affecting a total of 24m transactions; and

(3) Country codes for 10.2m wire transactions were not captured in CAMP.

4.97. These prolonged data accuracy issues in CAMP also affected the monitoring of correspondent banking customer activity. The 2014 CB external report found that over a 6-month period between October 2012 and March 2013:

(1) 26.1m transactions with a total value of £46.3tn from GPS and MPS source systems were not monitored effectively due to issues affecting the quality of the data in CAMP. These transactions were not correctly marked in CAMP with the result that the incorrect counterparty was being monitored; and

(2) The GPS/MPS High Value feed did not correctly identify HSBC's role in the payment chain for 2.9m transactions totalling £16.6tn fed into CAMP which

meant that correspondent banking transactions were being recognised as non-correspondent banking transactions resulting in the incorrect counterparty being monitored for each transaction.

4.98. These data issues in CAMP were exacerbated by issues related to the completeness and accuracy of the originating party information for "on-behalf-of" payments. The failure to have complete and accurate information for these payments is likely to have had some impact on the generation of alerts by one of the pre-2016 CAMP scenarios and the subsequent review of those alerts. The extent to which this actually affected transaction monitoring in CAMP is unclear as HSBC found it would be impractical to conduct a lookback exercise. This issue was not resolved until the end of 2015.

Data changes in 2016

4.99. In July 2016, HSBC implemented a new "Extract, Transform and Load" (ETL) system which sat between source systems and CAMP; COPS was the equivalent system to ETL that sat between source systems and ETMS. These allowed HSBC to conduct data integrity checks and complete data mapping before the data was fed into CAMP and ETMS. Despite the implementation of ETL, reconciliations for data completeness and accuracy were not implemented (paragraphs 4.101 to 4.103 below). Issues affecting the completeness (paragraphs 4.104 to 4.108) and accuracy (paragraphs 4.111 to 4.114) of the data fed into CAMP also persisted after 2016. This is despite HSBC identifying completeness and accuracy data problems as early as 2010 and 2011 respectively (paragraphs 4.89 for data completeness and 4.95 for data accuracy).

4.100. Data issues were also present in ETMS including both completeness (paragraphs 4.109 to 4.110) and accuracy (paragraphs 4.115 to 4.118).

<u>Data Reconciliation- post 2016</u>

4.101. A data reconciliation programme for CAMP was mobilised in June 2016. However, overall progress was slow, and, by May 2017, HSBC was instructed by the Monitor to conduct regular and rigorous data reconciliations to ensure both data completeness and data accuracy which were required to carry out effective transaction monitoring. This is despite issues with data completeness and accuracy having been identified as far back as 2010 and 2011.

4.102. HSBC subsequently delivered and executed this plan to conduct data reconciliation. However, even after this had been put in place, HSBC was unable to verify whether data reconciliation was in place for all critical data elements from source systems to ensure that the data was complete and accurate throughout the relevant period. This was identified as a limitation which might indicate critical financial, reputational or strategic impact and/or create such regulatory non-compliance as would require immediate notification to the regulator because there was a risk that CAMP would not generate alerts when it should. This was a significant period after HSBC was made aware of the need to address issues relating to poor data reconciliation.

4.103. HSBC also delayed the reconciliation of the data fed into ETMS; HSBC only started investigating data reconciliations for this system after the implementation of ETMS.

Data completeness in CAMP post 2016

CAMP - Orphan accounts

4.104. Orphan accounts are accounts which cannot be matched to a specific customer. This meant that the alerts generated in respect of these accounts needed to be matched to a customer outside of an automated transaction monitoring system before they could be reviewed.

4.105. Following the rollout of ETL in August 2016, 2 of the source systems which fed transactions into CAMP did not reconcile correctly which meant that transactions were not linked to customers and only monitored in CAMP at account level. This limited the ability of CAMP to monitor transactions as it could not use scenarios to monitor transactions by using a customer's profile and past activity and had to rely on non-customer specific scenarios such as the round amount scenario. This issue affected over 62,000 customers, approximately 92,500 accounts and approximately 45m payments with a value of £103.4tn. Alerts generated by these transactions were deemed unworkable and so these could not be reviewed effectively.

4.106. A new system introduced in October 2017 meant HSBC could not review any alerts affected by this issue until February 2018 when a fix was deployed. This led to a backlog of alerts with the risk of potentially suspicious activity going undetected. HSBC was unable to quantify the extent of the issue from October to December 2017, though in January 2018, HSBC had some 400,000 orphan accounts with transactions for these accounts having an estimated value of £3.2tn. A subsequent lookback exercise conducted by HSBC did not result in the filing of any SARs.

4.107. HSBC later started producing monthly reports of the number of orphan accounts and the volume and value of transactions affected. It was identified that 0.25% of the value of transactions monitored by CAMP, around £1tn, involved orphan accounts.

SEPA payments

4.108. The SEPA payment issue referred to at paragraph 4.91 above persisted after 2016 in CAMP and was also present in ETMS, after correspondent banking related SEPA payments were monitored by ETMS from 2017. This issue meant that around 520,000 transactions per month were excluded from CAMP and ETMS with a value of over £5.8bn per month. HSBC was not able to put in place a remediation plan for the affected transactions until this issue was identified. HSBC conducted a lookback exercise and as a result filed a small number of SARs.

Data completeness in ETMS post 2016

List of correspondent banking relationships

4.109. As set out at paragraph 4.92 above, it had been identified in 2014 that HSBC did not maintain a list of correspondent banking relationships. This issue had still not been resolved when ETMS went live in 2017 and persisted during the relevant period. As an interim measure, when ETMS was implemented, HSBC put in place coding that was designed to identify entities that were exhibiting "*correspondent-like*" banking behaviours and ETMS was monitoring around 96% to 97% of correspondent banking customer activity when it went live.

4.110. This was subsequently highlighted as a high-risk issue with 13 out of a sample of 30 GBM relationships incorrectly excluded for correspondent banking. It was subsequently clarified that 4 of these customers were not identified using the same interim measure and were highly likely to be conducting correspondent customer banking activity. HSBC subsequently developed an automated capability to identify its correspondent banking customers.

<u>Data accuracy in CAMP post 2016</u>

Transaction mapping

4.111. The accurate mapping of transaction types from source systems to transaction monitoring systems is a process to ensure the full suite of scenarios are applied to different products being monitored. Transactions therefore need to be mapped correctly from source systems to transaction monitoring systems to ensure that they are monitored effectively by the correct scenarios.

4.112. Transaction mapping had been an issue for HSBC at a UK and global level prior to 2016. These issues persisted after 2016 and included the following:

(1) Between August 2016 and March 2018, approximately 24m cash transactions with a total value of approximately £24.5bn were not monitored by 2 of the 15 GMSAS scenarios and a UDR. This was because the cash amount was not populated in the necessary transaction field when it was fed into CAMP. This was not fully resolved during the relevant period. Notwithstanding this issue, HSBC later carried out a risk assessment and concluded the impact on the UDR to be of limited financial crime risk; and

(2) 52 out of 540 transaction codes from 3 source systems that fed into CAMP were incorrect. This included 29 transaction codes involving, in the period of a year, over 17.6m transactions with a value of over £64bn which were categorised as EFT/Wire transactions when they should have been classified as cheques and monetary instruments. This led to a risk that these transactions were inadequately monitored by two GMSAS scenarios.

4.113. HSBC had not assessed the financial crime risk posed by transactions not being monitored by the full suite of scenarios during the relevant period. HSBC

subsequently implemented new controls that aimed to ensure a consistent mappings process with a new exceptions management reporting process.

Data quality issues

4.114. Certain data elements within CAMP, including country codes, counterparty identifier and financial transaction originator/beneficiary identifier, were of poor quality and had been so for a prolonged period of time. This led to a risk that CAMP would not generate alerts when it should. This failure was a risk with a critical impact putting HSBC in a state of regulatory non-compliance. HSBC's policies and procedures around data quality were therefore not appropriate or sufficiently risk-sensitive throughout the relevant period.

Data accuracy post 2016 – (Correspondent Banking) ETMS

Transaction mapping

4.115. HSBC also identified transaction mapping issues in ETMS. 24 transaction codes with a total value of £239.6bn were incorrectly mapped into ETMS. These included:

(1) 4 transaction codes for over 475,000 transactions with a value of over £1.2bn were categorised as wire transactions when these should have been categorised as cash transactions;

(2) 18 transaction codes for over 530,000 transactions with a value of over £238bn were categorised as wire transactions when these should have been categorised as cheques and monetary instruments.

4.116. This led to a risk that these transactions would be under-monitored at a correspondent banking level by 1 of the ETMS scenarios, which had parameters specific to the different transaction type codes. These transaction mapping issues in ETMS were not resolved during the relevant period and the impact of the associated financial crime risk on transaction monitoring had not been assessed.

Data quality assessment

4.117. HSBC did not undertake a formal data quality assessment for ETMS during the relevant period and so had not addressed the data issues identified from the limited assessment that was carried out prior to its implementation. HSBC continued to identify data quality issues after the implementation of ETMS. These data quality issues impacted the effectiveness of ETMS. This was a very high-risk issue which may indicate a critical level of regulatory impact. This contributed to ETMS as having significant limitations during the relevant period.

4.118. The data quality issues that needed to be addressed meant HSBC had to delay the threshold tuning and testing of transactions that did not generate alerts. This in turn meant HSBC was not able to understand whether the ETMS thresholds were

set in such a way that it could identify transactions that were indicative of money laundering.

Remediation action

4.119. The failings set out above meant that HSBC still did not have an adequately effective automated transaction monitoring system throughout the relevant period. However, the Authority recognises HSBC's commitment to its large-scale global remediation programme. In particular, the Authority acknowledges the following successful enhancements.

(1) The introduction of an Extract, Transform and Load system which sat between source systems and CAMP, allowing HSBC to conduct data integrity checks and complete data mapping before the data was fed into CAMP and the equivalent system (COPS) for ETMS; and

(2) A new methodology for the segmentation of customers based on lines of business, customer type, historic transactional activity and risk rating.

5. FAILINGS

5.1. The statutory and regulatory provisions relevant to this Notice are set out in Annex A.

5.2. On the basis of the facts and matters set out above, the Authority considers that HSBC failed to comply with ML Regulation 20(1)(a), by failing to establish and maintain appropriate and sufficiently risk-sensitive policies and procedures relating to ongoing monitoring which provided for the identification and scrutiny of:

(1) complex or unusually large transactions;

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

(3) any other activity which it regarded as particularly likely to be related to money laundering or terrorist financing.

5.3. HSBC failed to ensure that its processes and procedures around automated transaction monitoring systems were appropriate and sufficiently risk-sensitive throughout the relevant period. In particular:

(1) From 2002 until 2016, HSBC's processes for automated transaction monitoring used the same 6 scenarios which failed to provide appropriate monitoring coverage for the nature, scale and complexity of HSBC's business. They also did not provide appropriate coverage of the risks presented by its correspondent banking business.

(2) When 15 new scenarios were rolled out for CAMP in 2016, the scenarios were not tailored to specific UK risks and 124 UK high-risk gaps across certain money laundering and terrorist financing risk indicators were not covered. Efforts to improve coverage of specific UK risks through implementation of UDRs were unsuccessful. This meant that the policies and procedures around this were not appropriate for the risks presented by the business.

(3) Thresholds used prior to 2016 had too many settings to allow testing to determine whether they were appropriate; they were also found to be ineffective in the 2014 external report.

(4) From August 2016 until the end of the relevant period, the thresholds for CAMP were potentially not capturing all suspicious activity that needed to be identified.

(5) Extreme thresholds for certain scenarios that were introduced after 2016, in both CAMP and ETMS, were set in such a way that it was almost impossible for those scenarios to detect unusual activity; for example, in a CAMP scenario 52% of RBWM customers (5.4m customers) and over 570,000 CMB customers needed a 500,000% (or 5,000 times) increase in their monthly transactional activity to trigger an alert. This meant that the processes were not sufficiently risk-sensitive.

(6) The suppression rules at one point in 2011 inadvertently suppressed all alerts in Wales with 1,780 SARs having to be retrospectively filed as a result. These rules also suppressed alerts that were indicative of unusual and sometimes suspicious activity, as demonstrated by the cases of Customer A, Customer C, Customer D and the 68 SARs for the period 2008 to 2016 that were subsequently filed after a lookback exercise in 2017. The use of these rules as part of HSBC's automatic transaction monitoring were therefore not appropriate or sufficiently risk-sensitive.

(7) HSBC delayed the implementation of its decision to remove the suppression rules for all high-risk accounts and those associated with high-risk countries for a year and a half which meant it delayed ensuring that its policies and procedures were appropriate and sufficiently risk-sensitive for identifying potentially high-risk transactions.

(8) Inaccurate and incomplete data was fed into the CAMP system prior to 2016, often affecting millions of transactions which in turn impacted the effectiveness of the processes for transaction monitoring.

(9) After 2016, HSBC continued to encounter data completeness and accuracy issues in CAMP and ETMS. These prevented the systems from effectively monitoring transactions and meant that HSBC's processes and procedures were neither appropriate nor sufficiently risk-sensitive during the relevant period.

5.4. The Authority also considers that HSBC failed to comply with ML Regulation 20(1)(f), by failing to establish and maintain appropriate and sufficiently risk-sensitive policies and procedures for the monitoring and management of compliance with, and internal communication of policies and procedures for ongoing monitoring.

5.5. Policies that were put in place to do this included the CAMP maintenance guide and a service level agreement to ensure that alerts were reviewed within a specific timeframe. However, HSBC failed to establish and maintain these compliance procedures in the following ways:

(1) The processes set out in the CAMP maintenance guide required that scenarios be reviewed annually, and that HSBC should not just rely on the scenarios that were already being used, but this was not followed. It was not until 2014 that HSBC considered that it needed new scenarios to monitor certain money laundering and terrorist financing typologies that presented a financial crime risk and even then, these scenarios were only identified at a global level.

(2) When new scenarios were rolled out for CAMP in 2016 and when ETMS was introduced in 2017, HSBC did not implement policies and procedures to ensure that it could carry out adequate or timely risk assessments for these scenarios. This failure meant that HSBC had limited assurance that these systems were covering sufficient money laundering and terrorist financing risks in the UK to minimise the risk of financial crime.

(3) Between 2016 and March 2018, nearly 35% of alerts generated by the LRT scenario in CAMP took more than 90 days to review, as prescribed by HSBC's own policy for ensuring compliance with processes. The structuring scenario design issue also contributed towards the backlog of alerts. This, in turn, contributed towards the delay of the swift identification of unusual activity, increasing the risk that money laundering and terrorist financing went either completely undetected or were not detected for a significant period of time.

(4) Prior to 2016, HSBC did not have appropriate and risk-sensitive procedures to ensure that it followed the CAMP maintenance guide's requirement that account and customer thresholds be reviewed annually. This was demonstrated by thresholds being seldom updated and HSBC having no defined processes or documentation for tuning thresholds.

(5) HSBC set the post 2016 CAMP thresholds in just a week; consequently, there was little opportunity to examine their effectiveness and ensure that they were appropriate and sufficiently risk-sensitive. Such thresholds were not tuned to ensure they were appropriate and sufficiently risk-sensitive throughout the relevant period. This contributed to HSBC not reviewing a significant number of its alerts within the 90-day period specified in its policies.

(6) HSBC failed to carry out any testing of the alerts that were generated, and transactions that did not generate an alert, during the relevant period. This meant that HSBC could not be sure that alerts being generated were indeed indicative of unusual activity and were adequately identifying unusual activity; this contributed to these systems having significant limitations throughout the relevant period.

(7) HSBC set the ETMS thresholds in a manner focused only on projected alert volumes in each customer segment and without documentation, so these were not demonstrably appropriate or risk-sensitive.

(8) HSBC did not have appropriate policies and procedures in place to ensure that its staff adequately followed the CAMP maintenance guide's requirement that suppression rules be reviewed annually. In some cases, the rules needed to be reverse engineered in order for HSBC to understand how the rules operated. HSBC also failed to consider whether there were wider issues with the suppression rules and whether these policies and procedures were appropriate after one rule was found to be suppressing all alerts in Wales.

(9) HSBC failed to check the completeness and accuracy of data that was being fed into CAMP and ETMS throughout the relevant period despite being recommended to do so by a number of external advisory parties over a prolonged period of time. This meant that HSBC did not have appropriate or sufficiently risk-sensitive policies and procedures in this regard during the relevant period. HSBC also failed to carry out a data quality assessment for ETMS.

(10) HSBC failed to maintain a list of correspondent banking relationships which meant that not all relevant data for correspondent banking was being fed into the transaction monitoring systems. This was an example of policies and procedures to ensure compliance with internal policies and procedures not being appropriate or sufficiently risk-sensitive. As a result, HSBC failed to adequately monitor all of its respondent banks' activity.

6. SANCTION

6.1. Pursuant to Regulations 36(a) and 42(1) of the ML Regulations, the Authority may impose a penalty of such amount as it considers appropriate on a relevant person who fails to comply with the ML Regulations at issue in this notice.

6.2. HSBC is a relevant person pursuant to Regulations 3(2) and 3(3) of the ML Regulations.

6.3. In deciding whether HSBC has failed to comply with the relevant requirements of the ML Regulations, the Authority has considered whether HSBC followed the

relevant JMLSG Guidance as the JMLSG meets the requirements set out in Regulation 42(3) of the ML Regulations (being guidance approved by the Treasury).

6.4. In accordance with Regulation 42(2) of the ML Regulations, the Authority has considered whether it can be satisfied that HSBC took all reasonable steps and exercised all due diligence to ensure that the requirements of the ML Regulations would be complied with. The Authority has concluded that it cannot, for the reasons set out in Section 5 of this Notice.

6.5. Regulation 42(1) of the ML Regulations states that the Authority may impose a penalty of such amount that it considers appropriate on a relevant person for failure to comply with the ML Regulations at issue in this Notice.

6.6. The Authority has concluded that a financial penalty is the appropriate sanction in the circumstances of this particular case.

6.7. During the relevant period, paragraph 19.15.5 of the Enforcement Guide stated that, when imposing or determining the level of a financial penalty under the ML Regulations, the Authority's policy includes having regard, where relevant, to relevant factors in DEPP 6.2.1G and DEPP 6.5 to DEPP 6.5D.

6.8. DEPP 6.5A sets out the details of the 5-step framework that applies in respect of the financial penalties imposed on firms.

6.9. The application of the Authority's penalty policy is set out below in relation to HSBC's breaches of the ML Regulations relating to:

(1) HSBC's RBWM and CMB business (paragraphs 6.10 to 6.34); and

(2) HSBC's Correspondent Banking business (paragraphs 6.35 to 6.59).

FAILINGS RELATING TO HSBC'S RBWM AND CMB BUSINESS

Step 1 – disgorgement

6.10. 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.

6.11. The Authority has not identified any financial benefit that HSBC derived directly from its breaches.

6.12. The figure after Step 1 is therefore £0.

Step 2 – the seriousness of the breach

6.13. 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.

6.14. The Authority considers that the revenue generated by HSBC is indicative of the harm or potential harm caused by its breaches. The Authority has therefore determined a figure based on a percentage of HSBC's relevant revenue. HSBC's relevant revenue is the revenue derived from RBWM and CMB business during the period of the breach. The period of HSBC's breaches in relation to the RBWM and CMB business was from 31 March 2010 to 31 March 2018 inclusive. The Authority considers HSBC's relevant revenue for its failings relating to its RBWM and CMB business for this period to be £39,009,000,000.

6.15. 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 breaches and chooses a percentage between 0% and 20%. This range is divided into 5 fixed levels which represent, on a sliding scale, the seriousness of the breaches; the more serious the breaches, the higher the level. For penalties imposed on firms there are the following 5 levels:

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

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

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

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

6.17. DEPP 6.5A.2(12) goes onto identify level 1, 2 and 3 factors. Of these, the Authority considers the following factors to be relevant:

(b) there was no or little risk of loss to consumers, investors or other market users individually and in general;"

6.18. Taking these factors into account, the Authority considers the level most appropriate for the seriousness of the failings to be level 4 and so the Step 2 figure is 15% of £39,009,000,000.

6.19. The figure after Step 2 is therefore £5,851,298,100.

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

(1) The breaches are limited to automated transaction monitoring only, which, whilst important, is only 1 aspect of its AML framework; and

(2) Whilst HSBC Bank plc had a very large volume of transactions to monitor, the vast majority of customers (84%) were assessed as having a very low financial crime risk.

6.21. In order to achieve a penalty that (at Step 2) is proportionate to the breach, and having taken into account previous cases, the Step 2 figure is reduced to £62,320,875.

Step 3 – mitigating and aggravating factors.

6.22. 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 to take into account factors which aggravate or mitigate the breach.

6.23. 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 ML Regulations, regulatory requirements in the Handbook and evolving practice in the financial services industry.

6.24. Before and during the relevant period, the Authority published the following guidance relating to AML controls, which set out examples of good and poor industry practice to assist firms:

(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 notes that the Proceeds of Crime Act 2002 requirements on reporting suspicious activity make an appropriate degree of monitoring desirable. It also included examples of good and poor industry practice, such as large firms using automated transaction monitoring, and reminded firms that their approach to AML should be aligned with JMLSG guidance;

(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

(3) In December 2011, the Authority published the "Financial Crime: A Guide for Firms". This included guidance on the requirements of automated transaction monitoring, good and poor practices, which remained consistent throughout regular updates of this guide during the relevant period.

6.25. Consequently, HSBC was aware, or ought to have been aware, of the importance of putting in place and maintaining effective policies and procedures for automated transaction monitoring to detect and prevent money laundering.

6.26. HSBC has invested heavily in the next generation of automated transaction monitoring. The Authority recognises the importance of innovation in this area, and notes the commitment already made by HSBC in the use of new and market leading technologies.

6.27. As referred to in paragraph 2.10 above, the Authority recognises HSBC's commitment to its large-scale global remediation programme (which was a key priority for senior management and the Board of Directors), the enhancements reflected in this Notice and the significant increase in resource dedicated to managing financial crime risk including the tripling of personnel working on transaction monitoring related activity.

6.28. Having taken into account the above, the Authority considers that the Step 2 figure should be increased by 10%.

6.29. The figure after Step 3 is therefore £68,552,963.

Step 4 – adjustment for deterrence.

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

6.31. The Authority considers that the Step 3 figure of £68,552,963 represents a sufficient deterrent to HSBC and others, and so has not increased the penalty at Step 4.

6.32. The figure after Step 4 is therefore £68,552,963.

Step 5 – penalty discount.

6.33. The Authority and HSBC reached agreement at stage 1 in relation to all relevant facts and all issues as to whether those facts constitute breaches and so has applied a 30% discount to the Step 4 figure.

6.34. The figure after Step 5 is therefore £47,987,074.

FAILINGS RELATING TO HSBC'S CORRESPONDENT BANKING BUSINESS

Step 1 – disgorgement

6.35. 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.

6.36. The Authority has not identified any financial benefit that HSBC derived directly from its breaches.

6.37. The figure after Step 1 is therefore £0.

Step 2 – the seriousness of the breach

6.38. 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.

6.39. The Authority considers that the revenue generated by HSBC is indicative of the harm or potential harm caused by its breaches. The Authority has therefore determined a figure based on a percentage of HSBC's relevant revenue. HSBC's relevant revenue is the revenue derived from the Correspondent Banking business during the period of the breach. The period of HSBC's breaches in relation to the Correspondent Banking business was from 31 March 2010 to 31 March 2018 inclusive. The Authority considers HSBC's relevant revenue for its failings relating to the Correspondent Banking business for this period to be £384,875,000.

6.40. 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 breaches and chooses a percentage between 0% and 20%. This range is divided into 5 fixed levels which represent, on a sliding scale, the seriousness of the breaches: the more serious the breaches, the higher the level. For penalties imposed on firms there are the following 5 levels:

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

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

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

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

6.42. DEPP 6.5A.2(12) goes onto identify level 1, 2 and 3 factors. Of these, the Authority considers the following factors to be relevant:

(b) there was no or little risk of loss to consumers, investors or other market users individually and in general;"

6.43. Taking these factors into account, the Authority considers the level most appropriate for the seriousness of the failings to be level 4 and so the Step 2 figure is 15% of £384,875,000.

6.44. The figure after Step 2 is therefore £57,731,200.

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

6.46. In order to achieve a penalty that (at Step 2) is proportionate to the breach, and having taken into account previous cases, the Step 2 figure is reduced to £20,727,000.

Step 3 – mitigating and aggravating factors.

6.47. 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 to take into account factors which aggravate or mitigate the breach.

6.48. Since 1990, the JMLSG has published detailed written guidance on AML controls. During the relevant period, the JMLSG provided guidance on compliance with the legal requirements of the ML Regulations, regulatory requirements in the Handbook and evolving practice in the financial services industry.

6.49. Before and during the relevant period, the Authority published the following guidance relating to AML controls, which set out examples of good and poor industry practice to assist firms:

(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 notes the Proceeds of Crime Act 2002 requirements on reporting suspicious activity make an appropriate degree of monitoring desirable. It also included examples of good and poor industry practice, such as large firms using automated transaction monitoring, and reminded firms that their approach to AML should be aligned with JMLSG guidance;

(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 *"Transaction monitoring of respondent accounts can help mitigate the money-laundering risks arising from correspondent banking activities"*; and

(3) In December 2011, the Authority's published the "Financial Crime: A Guide for Firms". This included guidance on the requirements of automated transaction monitoring, good and poor practices, which remained consistent throughout regular updates of this guide during the relevant period.

6.50. Consequently, HSBC was aware, or ought to have been aware, of the importance of putting in place and maintaining effective policies and procedures for automated transaction monitoring to detect and prevent money laundering.

6.51. HSBC has invested heavily in the next generation of automated transaction monitoring. The Authority recognises the importance of innovation in this area, and notes the commitment already made by HSBC in the use of new and market leading technologies.

6.52. As referred to in paragraph 2.10 above, the Authority recognises HSBC's commitment to its large-scale global remediation programme (which was a key priority for senior management and the Board of Directors), the enhancements reflected in this Notice and the significant increase in resource dedicated to managing financial crime risk including the tripling of personnel working on transaction monitoring related activity.

6.53. Having taken into account the above, the Authority considers that the Step 2 figure should be increased by 10%.

6.54. The figure after Step 3 is therefore £22,799,700.

Step 4 – adjustment for deterrence.

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

6.56. The Authority considers that the Step 3 figure of £22,799,700 represents a sufficient deterrent to HSBC and others, and so has not increased the penalty at Step 4.

6.57. The figure after Step 4 is therefore £22,799,700.

Step 5 – penalty discount.

6.58. The Authority and HSBC reached agreement at stage 1 in relation to all relevant facts and all issues as to whether those facts constitute breaches and so has applied a 30% discount to the Step 4 figure.

6.59. The figure after Step 5 is therefore £15,959,790.

Total penalty

6.60. The Authority has therefore decided to impose a total financial penalty (rounded down to the nearest £100) of £63,946,800 (£91,352,600 before 30% (stage 1) discount) on HSBC for breaching Regulations 20(1)(a) and 20(1)(f) of the ML Regulations. Of the penalty, £47,987,000 (£68,552,900 before 30% (stage 1) discount) relates to HSBC's RBWM & CMB failings, and £15,959,700 (£22,799,700 before 30% (stage 1) discount) relates to Correspondent Banking failings.

7. PROCEDURAL MATTERS

7.1. This Decision Notice is given in accordance with Regulation 42(7) of the ML Regulations. The following information is important.

Decision maker

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

The Tribunal

7.3. The person to whom this Notice is given has the right to refer the matter to the Tribunal. The Tax and Chancery Chamber is the part of the Upper Tribunal, which, among other things, hears references arising from decisions of the Authority. Under paragraph 2(2) of Schedule 3 of the Tribunal Procedure (Upper Tribunal) Rules 2008, the person to whom this Notice is given has 28 days to refer the matter to the Tribunal.

7.4. A reference to the Tribunal is made by way of a reference notice (Form FTC3) signed by the person making the reference (or on their behalf) and filed with a copy of this Notice. The Tribunal's correspondence address is 5th Floor, The Rolls Building, Fetter Lane, London EC4A 1NL.

7.5. Further details are available from the Tribunal website:

http://www.justice.gov.uk/forms/hmcts/tax-and-chancery-upper-tribunal

A copy of Form FTC3 must also be sent to Steve Page at the Financial Conduct Authority, 12 Endeavour Square, London E20 1JN at the same time as filing a reference with the Tribunal.

Manner and time for payment

7.6. The financial penalty must be paid in full by HSBC to the Authority by no later than 10 January 2022.

If the financial penalty is not paid

7.7. If any or all of the financial penalty is outstanding on 10 January 2022, the Authority may recover the outstanding amount as a debt owed by HSBC and due to the Authority.

Access to evidence

7.8. The Authority grants the person to whom this Notice is given access to:

(1) the material upon which the Authority has relied in deciding to give this Notice; and

(2) the secondary material which, in the opinion of the Authority, might undermine that decision.

Third party rights

7.9. No third party rights apply in respect of this Notice.

Confidentiality and publicity

7.10. This Notice may contain confidential information and, unless it has been published by the Authority, should not be disclosed to a third party (except for the purpose of obtaining advice on its contents).

7.11. The Authority will publish such information about the matter to which a Decision Notice relates as it considers appropriate.

Authority contacts

7.12. For more information concerning this matter generally, contact Oliver Hitman or Simon Lickley at the Authority: Oliver Hitman, direct line: 020 7066 1078/email: oliver.hitman2@fca.org.uk; Simon Lickley, direct line: 020 7066 4608/email: simon.lickley@fca.org.uk.

Mark Steward

Settlement Decision Maker, for and on behalf of the Authority

Sheldon Mills

Settlement Decision Maker, for and on behalf of the Authority

ANNEX A – RELEVANT STATUTORY AND REGULATORY PROVISIONS AND GUIDANCE

The Money Laundering Regulations 2007 (referred to in this Notice as the "ML Regulations") were in force from 15 December 2007 to 25 June 2017 inclusive and have been replaced by the Money Laundering Regulations 2017, in respect of conduct beginning on or after 26 June 2017. In this Notice, the Authority refers to the Money Laundering Regulations 2007 as the relevant period occurred when the Money Laundering Regulations 2007 were in force.

Relevant extracts from the ML Regulations

Ongoing monitoring

1. Regulation 8 states:

"(1) A relevant person must conduct ongoing monitoring of a business relationship.

(2) "Ongoing monitoring" of a business relationship means-

(a) scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile; and

(b) keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date.

(3) Regulation 7(3) applies to the duty to conduct ongoing monitoring under paragraph (1) as it applies to customer due diligence measures."

Enhanced customer due diligence and ongoing monitoring

2. Regulation 14 states:

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

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

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

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

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

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

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

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

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

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

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

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

Policies and procedures

3. Regulation 20 states:

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

(a) customer due diligence measures and ongoing monitoring;…

(f) the monitoring and management of compliance with, and the internal communication of, such policies and procedures, in order to prevent activities related to money laundering and terrorist financing.

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

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

(i) complex or unusually large transactions;

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

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

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

Power to impose civil penalties

4. Regulation 42 provides that a designated authority (here the Authority) may impose a penalty of such amount as it considers appropriate on a relevant person failing to comply with certain requirements under the ML Regulations.

Relevant extracts from the JMLSG Guidance

5. The JMLSG Guidance provisions set out below are taken from the December 2007 and June 2017 versions of the guidance. The wording is the same in both versions. The JMLSG Guidance is periodically updated, however, there were no material changes to the provisions set out below during the relevant period.

Part I, Chapter 5 Customer due diligence

Monitoring customer activity

The requirement to monitor customers' activities

6. Paragraph 5.7.2 states:

"Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps give firms know their customers, assist them to assess risk and provides greater assurance that the firm is not being used for the purposes of financial crime."

What is monitoring?

7. Paragraph 5.7.3 states:

"The essentials of any system of monitoring are that:

- *it flags up transactions and/or activities for further examination;*
- *these reports are reviewed promptly by the right person(s); and*
- *appropriate action is taken on the findings of any further examination."*

8. Paragraph 5.7.4 states:

"Monitoring can be either:

- *in real time in that transactions and/or activities can be reviewed as they take place or are about to take place; or*

- *after the event, through some independent review of the transactions and/or activities that a customer has undertaken.*

and in either case, unusual transactions or activities will be flagged for further examination."

9. Paragraph 5.7.5 states:

"Monitoring may be by reference to specific types of transactions, to the profile of the customer, or by comparing their activity or profile with that of a similar, peer group of customers, or through a combination of these approaches."

10. Paragraph 5.7.7 states:

"In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer and product risk."

11. Paragraph 5.7.8. states:

"Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. The scope and complexity of the process will be influenced by the firm's business activities, and whether the firm is large or small. The key elements of any system are having up-to-date customer information, on the basis of which it will be possible to spot the unusual, and asking pertinent questions to elicit the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious."

Nature of monitoring

12. Paragraph 5.7.9 states:

"Some financial services businesses typically involves transactions with customers about whom the firm has a good deal of information, acquired for both business and regulatory reasons. Other types of financial services businesses involve transactions with customers about whom the firm may need to have only limited information. The nature of the monitoring in any given case will therefore depend on the business of the firm, the frequency of customer activity, and the types of customer that are involved."

13. Paragraph 5.7.10 states:

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

- *the unusual nature of a transaction: e.g., abnormal size or frequency for that customer or peer group; the early surrender of an insurance policy;*
- *the nature of a series of transactions: for example, a number of cash credits;*
- *the geographic destination or origin of a payment: for example, to or from a high-risk country; and*
- *the parties concerned: for example, a request to make a payment to or from a person on a sanctions list."*

14. Paragraph 5.7.11 states:

"The arrangements should include the training of staff on procedures to spot and deal specially (e.g., by referral to management) with situations that arise that suggest a heightened money laundering risk; or they could involve arrangements for exception

reporting by reference to objective triggers (e.g. transaction amount). Staff training is not, however, a substitute for having in place some form of regular monitoring activity."

15. Paragraph 5.7.12 states:

"Higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring."

Manual or automated?

16. Paragraph 5.7.13 states:

"A monitoring system may be manual, or may be automated to the extent that a standard suite of exception reports are produced. One or other of these approaches may suit most firms. In the relatively few firms where there are major issues of volume, or where there are other factors that make a basic exception report regime inappropriate, a more sophisticated automated system may be necessary."

17. Paragraph 5.7.15 states:

"In relation to a firm's monitoring needs, an automated system may add value to manual systems and controls, providing that the parameters determining the outputs of the system are appropriate. Firms should understand the workings and rationale of an automated system, and should understand the reasons for its output of alerts, as it may be asked to explain this to its regulator."

18. Paragraph 5.7.16 states:

"The greater the volume of transaction, the less easy it will be for a firm to monitor them without the aid of some automation. Systems available include those that many firms, particularly those that offer credit, use to monitor fraud. Although not specifically designed to identify money laundering or terrorist financing, the output from these anti-fraud monitoring systems can often indicate possible money laundering or terrorist financing."

19. Paragraph 5.7.17 states:

"There are many automated transaction monitoring systems available on the market; they use a variety of techniques to detect and report unusual/uncharacteristic activity. These techniques can range from artificial intelligence to simple rules. The systems are available are not designed to detect money laundering or terrorist financing, but are able to detect and report unusual/uncharacteristic behaviour by customers, and patterns of behaviour that are characteristic of money laundering or terrorist financing, which after analysis may lead to suspicion of money laundering or terrorist financing. The implementation of transaction monitoring systems is difficult due to the complexity of the underlying analytics used and their heavy reliance on customer reference data and transaction data."

20. Paragraph 5.7.18 states:

"Monitoring systems, manual or automated, can vary considerably in their approach to detecting and reporting unusual or uncharacteristic behaviour. It is important for firms to ask questions of the supplier of an automated system, and internally within the business, whether in support of a manual or an automated system, to aid them in

selecting a solution that meets their particular business needs best. Questions that should be addressed include:

- *How does the solution enable the firm to implement a risk-based approach to customers, third parties and transactions?*
- *How do system parameters aid the risk-based approach and consequently affect the quality and volume of transactions alerted?*
- *What are the money laundering/terrorist financing typologies that the system addresses, and which component of the system addresses each typology? Are the typologies that are included with the system complete? Are they relevant to the firm's particular line of business?*
- *What functionality does the system provide to implement new typologies, how quickly can relevant new typologies be commissioned in the system and how can their validity be tested prior to activation in the live system?*
- *What functionality exists to provide the user with the reason that a transaction is alerted and is there full evidential process behind the reason given?*
- *Does the system have robust mechanisms to learn from previous experience and how is the false positive rate continually monitored and reduced?"*

21. Paragraph 5.7.19 states:

"What constitutes unusual or uncharacteristic behaviour by a customer, is often defined by the system. It will be important that the system selected has an appropriate definition of 'unusual or uncharacteristic' and one that is in line with the nature of business conducted by the firm."

22. Paragraph 5.7.20 states:

"The effectiveness of a monitoring system, automated or manual, in identifying unusual activity will depend on the quality of the parameters which determine what alerts it makes, and the ability of staff to assess and act as appropriate on these outputs. The needs of each firm will therefore be different, and each system will vary in its capabilities according to the scale, nature and complexity of the business. It is important that the balance is right in setting the level at which an alert is generated; it is not enough to fix it so that the system generates just enough output for the existing staff complement to deal with – but equally, the system should not generate large numbers of 'false positives', which require excessive resources to investigate"