Financial Services Authority

DECISION NOTICE

To: The Royal Bank of Scotland Plc (RBS)
National Westminster Bank Plc (NatWest)
Ulster Bank Limited (Ulster Bank) and
Coutts & Company (Coutts & Co)

(members of The Royal Bank of Scotland Group and together for the purposes of this Notice RBSG)

FSA Reference Numbers:

RBS	-	121882
NatWest	-	121878
Ulster Bank	-	122315
Coutts & Co	-	122287

Date: 2 August 2010

TAKE NOTICE: The Financial Services Authority of 25 The North Colonnade, Canary Wharf, London E14 5HS ("the FSA") has decided to take the following action:

1. ACTION

1.1. For the reasons set out below and pursuant to regulation 42 of the Money Laundering Regulations 2007[1] (the Regulations), the FSA has decided to impose a civil penalty of £5.6 million on RBSG in respect of breaches of regulation 20(1) of the Regulations which occurred between 15 December 2007 and 31 December 2008 (the Relevant Period).

1.2. RBSG confirmed on 30 June 2010 that it will not be referring the matter to the Upper Tribunal (Tax and Chancery Chamber).

[1] SI 2007 No. 2157.

1.3. RBSG agreed to settle at an early stage of the FSA's investigation. They therefore qualify for a 30% (Stage 1) discount under the FSA's executive settlement procedures. Were it not for this discount, the FSA would have proposed the imposition of a financial penalty of £8 million on RBSG.

1.4. Accordingly, the FSA imposes a financial penalty on RBSG in the amount of £5.6 million.

2. REASONS FOR THE ACTION

2.1. During the Relevant Period, RBSG breached regulation 20(1) of the Regulations by failing to establish and maintain appropriate and risk-sensitive policies and procedures relating to:

(1) customer due diligence measures and ongoing monitoring;

(2) internal control; and

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

in order to prevent funds or financial services being made available to designated persons on the list of financial sanctions targets maintained by Her Majesty's Treasury (the Treasury list).

2.2. RBSG failed to consider properly what policies and procedures were required to comply with their obligations under the Regulations and the UK financial sanctions regime. Consequently, RBSG failed, for an extended period of time, to put in place adequate systems and controls to screen both its customers and the payments they received against the Treasury list. In particular, during the Relevant Period, RBSG failed to establish and maintain appropriate and risk-sensitive policies and procedures relating to the following matters:

(1) RBSG failed properly to implement and oversee the systems used to screen relevant customers and payments against the Treasury list. As a result, notwithstanding that RBSG were one of the largest processors of foreign payments among UK banks, they did not screen the following cross-border payments:

(a) any incoming payments to customers;

(b) Sterling payments made by customers (except those going to US based institutions); and

(c) Euro payments made by customers (until 9 June 2008).

Whilst these issues were identified by RBS Group Security & Fraud (GS&F) within RBS Group's Manufacturing Division, and GS&F had put in place a plan to address them, such actions were not taken in a sufficiently timely manner.

(2) RBSG's automated screening failed to screen the majority of trade finance SWIFT messages generated in the international trade transactions that it carried out.

(3) RBSG did not consistently record sufficient information relating to the directors and beneficial owners of its corporate customers. Where information relating to directors and beneficial owners was recorded, RBSG failed to ensure that such individuals were screened against the Treasury list on an ongoing basis.

(4) After the screening systems used to check customers and payments against the Treasury list had initially been set up, RBSG failed to ensure that the design and implementation of the 'fuzzy matching' capabilities in the screening software – used to identify close matches to the Treasury list – continued to operate satisfactorily. After the initial set up, the results produced by the screening filters were not routinely reviewed or monitored by RBSG to ensure that they were appropriate. This meant that over time the 'fuzzy matching' parameters initially set by RBSG became significantly less effective at identifying potential matches.

2.3. The lack of adequate policies and procedures in respect of these matters gave rise to an unacceptable risk that RBSG could have breached the UK financial sanctions regime.

2.4. The FSA considers these failings to be particularly serious because:

(1) The involvement of UK financial institutions in providing funds, economic resources or financial services to designated persons on the Treasury list undermines the integrity of the UK financial services sector. Unless they have in place robust systems and controls, UK financial institutions risk being used to facilitate transactions involving sanctions targets, including terrorist financing. As the Joint Money Laundering Steering Group (JMLSG) guidance advises, small amounts of funding could be sufficient to finance terrorist activities and hence the sanctions-related systems and controls implemented by firms need to be robust enough to capture such payments.[2] The FSA's financial crime and market confidence statutory objectives are both endangered by firms' failures in this area. Adequate systems and controls relating to financial sanctions is an integral part of complying with the FSA's requirements on financial crime.

(2) The systems and control failings at RBSG presented a serious risk to the FSA's financial crime and market confidence statutory objectives. During 2007, the London division responsible for processing payments for RBSG dealt with the largest volume of foreign payments of any financial institution in the UK. For example, it processed £7.6 trillion of inward Euro payments

[2] JMLSG Guidance, Part I, Preface, paragraphs 9 and 10.

and £8.6 trillion of outward Euro payments, across a total volume of 1.8 million payment transactions.

(3) RBSG, through GS&F, were aware of deficiencies in the screening systems used during the Relevant Period but did not act on these deficiencies in a timely manner. This contributed to the above failings in systems and controls remaining in existence for one year and not being remedied earlier. For example, GS&F raised issues relating to their sanctions screening software with the software provider but failed to ensure that these issues were resolved promptly. Further, after GS&F instructed a leading firm of accountants (the Accountants) in early 2008 to carry out an independent review to benchmark RBSG's screening software against a peer group, the key issues identified in the review were not appropriately escalated and as a result were not considered by the relevant committees within RBSG who would have overseen remedial action. The required remedial action was not taken until a number of months later.

2.5. RBSG's failings therefore merit the imposition of a significant financial penalty. In deciding the level of disciplinary sanction, the FSA recognises that RBSG have taken action to mitigate the seriousness of their failings, including:

(1) once the failings came to the attention of the current management within RBSG, they promptly reported them to the FSA; and

(2) RBSG took expedient and appropriate remedial action in respect of screening payments, improving the effectiveness of the software and improving governance and oversight of UK sanctions compliance. This included implementing screening of all inbound payments, outbound domestic Sterling payments, various Trade Finance messages and payments entered directly into the gateway application for SWIFT messages.

2.6. Since the discovery of its failings in December 2008, RBSG and its current senior management have fully cooperated with the FSA's investigation.

3. RELEVANT STATUTORY AND REGULATORY PROVISIONS

UK financial sanctions regime

3.1. The relevant provisions of the UK financial sanctions regime are set out in Appendix 1 of this Notice. In general terms, the regime lists individuals and entities that are subject to financial sanctions (designated persons). The law requires firms not to provide funds or, in the case of the Terrorism Order, financial services, to designated persons unless a licence is obtained from the Treasury.

3.2. The Treasury is responsible for the implementation and administration of international financial sanctions in the UK, for domestic designation (principally under the Terrorism Order) and for licensing exemptions to financial sanctions. The Treasury's Asset Freezing Unit (AFU) maintains a consolidated list of designated persons which consists of the names of individuals and entities that have been listed by the United Nations, European Union and/or the United Kingdom under specific financial sanctions regime.

3.3. Any firm which identifies a payment it believes may be a match to a designated person on the Treasury list must block the relevant payment, subject to further investigation. Following this investigation, if the firm believes that the payment is indeed an exact match, it must inform the AFU. In these circumstances, the firm may only process the payment in the event that a licence to do so is granted by the AFU.

3.4. A failure to comply with these obligations can carry serious consequences. A breach of the regime may result in a criminal offence being committed, as well as leading to reputational damage to firms. In addition, it carries the risk of criminal penalties being sought by the government against the firm and, in certain circumstances, against the management of the firm.

Money Laundering Regulations 2007

3.5. The FSA is a designated authority under regulation 36 of the Regulations. RBSG, as financial institutions, are relevant persons pursuant to regulations 2(1) and 3(1)(b) of the Regulations.

3.6. Regulation 20(1) (a), (d) and (f) of the Regulations require that:

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

(a) customer due diligence measures and ongoing monitoring;

…

(d) internal control;

…

(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."

3.7. Under Regulation 2, "terrorist financing" includes offences under Articles 7 and 8 of the Terrorism Order and Articles 7 and 8 of the Al-Qaida and Taliban Order. Regulation 42(3) states that:

"In deciding whether a person has failed to comply with a requirement of these Regulations, the designated authority must consider whether he followed any relevant guidance which was at the time—

(a) issued by a supervisory authority or any other appropriate body;

(b) approved by the Treasury; and

(c) published in a manner approved by the Treasury as suitable in their opinion to bring the guidance to the attention of persons likely to be affected by it."

Joint Money Laundering Steering Group guidance

3.8. The JMLSG is a body made up of the leading UK trade associations in the financial services industry, whose aim is to promulgate good practice in countering money laundering and to give practical assistance in interpreting UK money laundering and terrorist finance regulations. Since 1990 it has provided advice on anti-money laundering controls by issuing guidance for the financial sector. Subsequent editions of the JMLSG guidance have taken into account relevant legal changes and evolving practice within the financial services industry. The guidance produced by the JMLSG in November 2007 entitled '*Prevention of money laundering / combating terrorist financing: Guidance for the UK Financial Sector*' (the JMLSG Guidance Notes) fulfils the requirements of regulation 42(3). The FSA has had regard to the JMLSG Guidance Notes in considering whether a breach of the Regulations has occurred in this case.

3.9. Maintaining confidence in the financial system and the reduction of financial crime are statutory objectives for the FSA under section 2(2) of the Financial Services and Markets Act 2000.

4. FACTS AND MATTERS RELIED ON

Background

4.1. The firms comprising RBSG have been authorised by the FSA to perform a number of regulated activities since 1 December 2001. These include accepting deposits; arranging and advising on mortgages; advising on pensions; arranging, managing and dealing in investments; and safeguarding assets. NatWest, Ulster Bank and Coutts & Co are all wholly owned by RBS.

4.2. In addition to these regulated activities, RBSG also transfer and accept funds on behalf of their customers. During 2007, the London division responsible for processing payments for RBSG dealt with the largest volume of foreign payments of any financial institution in the UK. For instance, inward EURO payments totalled £7.6 trillion and outward payments totalled £8.6 trillion across a total volume of 1.8 million payment transactions. The various payments generated a large number of SWIFT messages per day.

4.3. The large volume of daily payments meant that there was a significant risk that attempts to route payments to or from or involving a designated person would be made through RBSG.

4.4. In 2006, the RBS Group started the implementation of its Financial Sanctions & Terrorist Financing Project. The project involved introducing automated screening mechanisms for both customer and payment screening by reference to the Treasury, OFAC and other relevant sanctions lists. A phased approach to the introduction of payment screening was adopted, including: all outbound US dollar payment traffic, which was screened from 8 October 2007; sterling payments to the US, which were

screened from December 2007; and sterling payments to other countries, which were screened from 29 December 2008.

Governance of compliance with UK financial sanctions regime

4.5. During the Relevant Period, the weaknesses identified in paragraphs 4.6 to 4.10 below existed in the governance framework that oversaw RBSG's compliance with the UK sanctions regime.

4.6. GS&F was responsible for the strategic direction and oversight of screening for designated persons within RBSG in the Relevant Period. In June 2006, this responsibility had been transferred from Group Risk Management to GS&F within RBS Group's Manufacturing Division. At the time, Group Manufacturing was already responsible for the screening operations which were carried out by the Financial Sanctions Unit (FSU) and the Payment Filtering Unit (PFU). The FSU carried out most of the customer screening and the PFU carried out most of the payment screening on behalf of RBSG in respect of its retail and corporate customers. The rationale for the move was that Group Manufacturing were also responsible for other aspects of financial crime at the time, especially fraud prevention.

4.7. This transfer of responsibility had the following implications:

(1) Oversight of screening against the Treasury list was removed from RBS Group Risk's support which, as a regulatory risk area, had a better appreciation of UK sanctions risks than Group Manufacturing, which was primarily a processing and service division.

(2) Whilst members of the GS&F team had expertise in the area of financial sanctions, some individuals with responsibility for the team did not and were not provided with training on UK financial sanctions compliance. GS&F therefore lacked appropriate management expertise relating to UK sanctions screening during the Relevant Period.

4.8. In the Relevant Period, GS&F issued and maintained the Financial Sanctions and Terrorist Financing (FS&TF) Procedural Guidelines, which set out RBS Group's approach to screening customers and payments against the Treasury list. These high level guidelines set out minimum standards in order for RBSG to meet their statutory obligations. Among other matters, RBSG had to check all their customers and payments against the Treasury list, document the investigation of any potential matches to ensure that true matches were reported and dealt with appropriately. The guidelines also specified the actions and reporting procedures for potential and actual matches. The guidelines applied to all business areas, subsidiaries and associates of RBSG as well as their employees.

4.9. GS&F was also involved with setting up the payment and customer screening software used by FSU and PFU. However, notwithstanding the minimum requirements in its FS&TF Procedural Guidelines to screen all payments and customers, the screening system established by GS&F was not sufficiently robust in its screening of customers and payments against the Treasury list (see paragraphs 4.13 to 4.20 below). Further, GS&F failed to monitor the output of the screening software

to ensure that its calibration was appropriate in light of changes to the names on the Treasury list, the RBSG customer database and the number of false positive results produced between 2006 and 2008 (see paragraphs 4.21 to 4.24 below).

4.10. The FS&TF Procedural Guidelines were updated in December 2008. The new guidelines specified that screening was required for messages in all currencies and for both inbound and outbound traffic. Additionally, as RBSG was using automated screening methods, the system settings for the fuzzy matching had to be discussed with and approved by GS&F.

4.11. In December 2008, the responsibility for sanctions screening policies and procedures was transferred from GS&F to Group Regulatory Risk and Compliance.

Relevant procedures

4.12. As a result of the failings in the governance framework overseeing compliance with UK sanctions, RBSG failed to implement procedures which ensured that all relevant customers and payments were screened against the Treasury list.

Payment screening

4.13. During the Relevant Period, RBSG failed to screen a number of categories of cross-border payments made to or by its customers:

(1) Incoming payments to customers

During the Relevant Period, RBSG did not screen any incoming payments remitted from outside of the UK. The failure to screen these incoming payments was not raised as a significant issue by GS&F until October 2008.

(2) International Sterling payments made by customers (except those going to US based institutions)

During the Relevant Period, RBSG only screened Sterling payments made by its customers to US based institutions. This represented a small proportion of the total Sterling payments made. The failure to screen international Sterling payments made by customers was first identified as a significant issue by GS&F in November 2007. A project was initiated to close this gap in the screening process. It was due to be implemented by the second half of 2008. However, international Sterling payments were not screened until 29 December 2008.

(3) Euro payments made by customers

Euro payments made by customers were not screened against the Treasury list until 9 June 2008.

As RBSG were one of the largest processors of foreign payments among UK banks, RBSG should have been screening all of the above payments throughout the Relevant Period. RBSG also failed to screen:

(1) payments entered manually into RBSG's gateway application for SWIFT messages

The gateway application for SWIFT messages provided RBSG with access to external SWIFT networks, enabling payments to be made to other financial institutions. The majority of the payment messages were screened automatically using the sanctions screening software prior to being routed to the gateway application. However, based on the volume and value of payment instructions directly keyed into the gateway application for SWIFT for one day in October 2008, approximately 14,000 payments with a value of £2.5 billion were manually processed directly into the gateway application during the Relevant Period across the RBS Group, hence bypassing the sanctions screening software. Consequently, such messages were not screened against the Treasury list.

(2) trade finance messages

Out of a possible 47 SWIFT trade finance message types, RBSG's automated screening software only screened three message types (MT400, MT752 and MT756) in the Relevant Period. The three message types screened by RBSG accounted for 21% of all SWIFT message types involved in the international trade transactions carried out by RBSG. Whilst we note that manual checks of some trade finance transactions were undertaken by reference to financial sanctions (including those transactions which involved countries perceived as high risk), messages not being screened may have contained information which could have identified an individual or entity as a designated person.

4.14. RBSG were unable to provide an analysis of the volumes of payments and payment messages that they did not screen during the Relevant Period. However, data for one day in July 2009 (i.e. outside of the Relevant Period) indicates that approximately 75% of all inbound and outbound messages would not have been screened by RBSG during the Relevant Period. RBSG's failure to screen these messages presented an unacceptable risk of payments being made to designated persons.

4.15. In addition, the main screening software used to screen payments against the Treasury list during the Relevant Period did not screen or block payments where the beneficiary name was presented across more than one line in the SWIFT message. The software only screened the top line of the name, so if the name contained in the

message was longer than the space allocated in that line, the payment would not be effectively screened. This meant that in some instances the screening software would not pick up exact matches to the Treasury list. This weakness in the software's functionality had not been detected during the testing of the screening software when it was initially implemented in 2006. The issue was first identified by the Accountants when they completed their review of the sanctions screening processes within the RBS Group in mid-2008. Prior to this review, GS&F had not been aware of this weakness with its screening software. A solution to this issue was eventually identified and implemented in June 2009.

Customer screening

4.16. RBSG did not consistently record the names of directors and beneficial owners of their corporate customers in their customer databases. Consequently, where such names were not recorded, they could not be screened against the Treasury list. Moreover, in relation to certain businesses, RBSG were not screening the names of any directors and beneficial owners against the Treasury list on an ongoing basis during the Relevant Period.

4.17. RBS and NatWest provided facilities for corporate customers to accept payments by cards and receive those funds. The customer database used by RBS and NatWest for this business only recorded details for each customer of a maximum of two directors or beneficial owners who held more than 20% ownership of the companies. The system did not have the capacity to record details for other directors or beneficial owners and did not record subsequent changes to the names of the original directors and beneficial owners. Consequently, these additional individuals could not be filtered using the screening software.

4.18. Ulster Bank and Coutts & Co did not record on their electronic databases all customer information relating to directors, beneficial owners and guarantors required for automated screening.

4.19. The limited information relating to directors and beneficial owners captured by RBSG was screened at the point when the account was opened. However, following this initial screening, the names of directors and beneficial owners were not screened against the Treasury list on an ongoing basis. Further, as subsequent changes to the names of the original directors and beneficial owners were not recorded, such changes could therefore not be screened against the Treasury list.

4.20. In January 2008, the RBSG credit card customer database containing 12 million customers (which included customers belonging to all RBS Group companies, including RBSG) was linked to the screening software and the full customer database was screened against the Treasury list. This retrospective screening generated 26,000 potential alerts (although an undetermined proportion of these were duplicates). Although the credit card database had been screened using the old screening software, that system could only match against exact names and had no fuzzy matching capabilities. This backlog was finally cleared in August 2009, approximately one and a half years after being initially identified. Accordingly, for the majority of the Relevant Period, RBSG had been providing credit to individuals without having adequately screened them against the Treasury list. However, in mitigation, we note

that approximately half of these individuals' bank accounts (to which the credit cards relate) would have been screened when the customer accounts databases were screened. Also no positive matches were identified once the backlog had been processed.

Weaknesses with fuzzy matching

4.21. 'Fuzzy matching' relates to the ability of the screening software to identify words within the payment messages that are either mis-spelt, inaccurately translated, and/or have variances of or contain common data-inputting errors relating to designated persons. This technology therefore allows firms to identify names which are very similar to those contained on the Treasury list, which could then be investigated further to ascertain whether the payment is indeed a match.

4.22. Where firms use automated processes for screening, they must carry out regular reviews of the appropriateness of the screening system to ensure that the system remains up-to-date and effective. GS&F failed to monitor the output of the screening software to ensure that its calibration was appropriate in light of changes to the names on the Treasury list, the RBSG customer database and the number of false positive results produced between 2006 and 2008.

4.23. The fuzzy matching logic for the payment and customer screening software used by RBSG was calibrated only once, when the software was initially installed in 2006. At the time, the system was calibrated in an attempt to find the appropriate output by balancing the system performance, the number of alerts generated for review and the number of potential false positives. However, GS&F did not subsequently review the output of the screening software to determine whether the software was still generating the appropriate number of alerts for the detailed review. No such reviews were conducted until 2008.

4.24. In 2008, the effectiveness of the fuzzy matching logic was tested for the first time since its implementation in 2006. The results of this testing highlighted weaknesses in the calibration of the fuzzy matching within the main screening software used by RBSG. For example:

(1) if an exact sanctioned term was rearranged so that the first name was substituted with its initial, and the first name and the surname were rearranged (e.g. "SMITH, John" became "J SMITH"), less than 5% of the terms on the Treasury list screened triggered alerts for further investigation;

(2) if an individual was added to the Treasury list part of whose name had six or less characters, a payment to such an individual would not have caused an alert to be generated by the screening software in the event that the payment message contained one incorrect character in the individual's name. For instance, when John SMITHE was substituted with John SMYTHE, the screening software would not have triggered an alert; and

(3) in relation to company names, the main payment screening software used by RBSG did not produce matches against the Treasury list in all cases when company abbreviations were removed. In other words, when "ABC GmbH"

was substituted with "ABC", the screening software did not identify 27% of potential matches.

Discovery and escalation of information and issues

Review by the Accountants

4.25. Following the acquisition of ABN Amro Holding N.V. in 2007, GS&F decided to review the effectiveness of its customer and payments screening system. In early 2008, GS&F instructed the Accountants to carry out an independent review to benchmark RBSG's screening software against a peer group. The scope of this review included both payment and customer screening. However, for some time before the Accountants had been instructed, RBSG (through GS&F) had been aware of certain deficiencies in its sanctions screening processes, including the lack of screening of various trade finance messages and most of the Sterling payments made by customers.

4.26. The results of this review highlighted various weaknesses in the systems used by PFU and FSU on behalf of RBSG, including the following:

(1) inadequate screening of trade finance messages;

(2) the customer and payment screening software was not performing as expected; and

(3) the lack of screening of incoming payments made to RBSG customers.

4.27. RBSG used an internal risk logging system to log and track issues affecting its business. Issues were classified as either 'major', 'significant' or 'important'. The correct classification of issues on the risk logging system was designed to escalate issues to the appropriate level of senior management. If an issue was logged on the risk logging system as 'significant' or 'major', it would have been considered by the relevant financial crime and risk committees responsible for UK sanctions screening.

4.28. The issues raised by the Accountants following their review of sanction screening policies and procedures across RBSG in 2008 were recorded by GS&F on the risk logging system. However, these issues were not treated as sufficiently material: when logged by GS&F on the system, two of the above issues were classed as 'important', the third as 'significant'. GS&F's rationale for this classification was based on the fact that they had already carried out a risk analysis and begun implementation of various programmes to address these issues. Although senior management within Group Manufacturing were provided with a summary of the Accountants' findings and were aware of the issues identified by the Accountants, this did not occur as a result of formal risk escalation procedures. The incorrect logging of the issues meant that there was inadequate discussion of the Accountants' findings at the relevant financial crime and risk committees responsible for UK sanctions screening which had the appropriate expertise for sanctions related matters. The minutes of these committees demonstrate that during the Relevant Period they did not discuss the work carried out by the Accountants. Accordingly, the issues identified by the Accountants were not adequately considered and consequently RBSG failed to ensure that the remedial action to address the relevant issues was subject to appropriate oversight.

4.29. A review by RBS Group Internal Audit (GIA) of the RBSG's UK sanctions screening policies and procedures in the last quarter of 2008 noted that the classification of these issues did not accurately reflect the materiality of the risks. During the GIA review, these risks were reassessed and their classifications were appropriately updated on the risk logging system. All three risks were reclassified as having a 'significant' impact. These reclassifications were based on the perceived regulatory risk arising from the issues identified.

Dealing with the screening software provider

4.30. During the Relevant Period, RBSG (through GS&F) identified weaknesses in the sanctions screening software which put it at material risk of making payments to designated persons. However, GS&F did not act in a timely or effective way to address the weaknesses it had identified.

4.31. GS&F logged issues relating to the screening software application on a separate log, classifying them as 'High', 'Medium', and 'Low' risk. The screening software provider independently logged and graded the issues identified by GS&F from P1 (most critical) to P5 (lowest priority) and would progress the resolution of these issues according to its own priority ranking. This meant that application issues raised by GS&F with the software provider were prioritised at different risk levels. As a result, the software provider did not resolve application issues in accordance with RBSG's requirements. This was despite the fact that GS&F and the software provider used to hold weekly meetings to discuss any open issues and their priority for resolution.

4.32. GIA's review identified that at the time of its review:

(1) thirteen issues logged by GS&F with the screening software provider were still unresolved with four issues still open since the first quarter of 2008. These issues had therefore been outstanding for more than six months;

(2) four out of the thirteen outstanding issues were raised by GS&F as 'high' risk, but the software provider had categorised these four issues as a 'medium' (P3) priority; and

(3) one issue was classified by GS&F as 'medium' but the software provider had raised it as the lowest priority (P5).

4.33. Accordingly, RBSG did not continually ensure that material issues it had identified with the sanctions screening software it had adopted were swiftly resolved.

5. BREACHES

5.1. By reason of the facts and matters set out above, RBSG breached regulation 20(1)(a) of the Regulations. RBSG failed to ensure that sufficient information was recorded regarding the directors and beneficial owners of its corporate customers. In many cases, the directors and beneficial owners were not therefore screened against the Treasury list. RBSG also failed to ensure that directors and beneficial owners it did record were screened against the Treasury list on an ongoing basis. In this respect, the JMLSG Guidance Notes specifically warn firms against the potential for "*complex business ownership structures, which can make it easier to conceal underlying*

beneficiaries". RBSG failed to mitigate the risk that such structures could be used to conceal payments to designated persons.

5.2. By reason of the facts and matters set out above, RBSG breached regulation 20(1)(d) of the Regulations. RBSG failed properly to implement and oversee the systems used by FSU and PFU to ensure that they carried out screening of all relevant customers and payments against the Treasury list. As a result, RBSG failed to screen the following cross-border payments:

(1) incoming payments to customers;

(2) Sterling payments made by customers (except those going to US based institutions); and

(3) Euro payments made by customers (until 9 June 2008).

5.3. As one of the largest processor of foreign payments among UK banks, RBSG should have been screening these payments during the Relevant Period. RBSG also failed to screen:

(1) payments entered manually into RBSG's gateway application for SWIFT messages; and

(2) the majority of trade finance SWIFT messages.

5.4. As such, a significant proportion of payments made by or received on behalf of RBSG customers were not screened against the Treasury list.

5.5. By reason of the facts and matters set out above, RBSG breached regulation 20(1)(f) of the Regulations. After the sanctions screening software was initially calibrated in 2006, RBSG failed to ensure that the design and implementation of the screening systems used to check customers and payments against the Treasury list were routinely reviewed and monitored. In this regard, the JMLSG Guidance Notes specifically acknowledge the value an automated system can add, "*provided that the parameters determining the outputs of the system are appropriate*". They also specifically state that firms' "*policies and procedures will need to be kept under regular review*". RBSG did not ensure that this was the case. It was subsequently discovered in 2008 that the 'fuzzy matching' parameters set by RBSG to identify close matches to the Treasury list were ineffective and failed to pick up potential matches that ought to have been identified.

5.6. Regulation 42(3) states that:

"In deciding whether a person has failed to comply with a requirement of these Regulations, the designated authority must consider whether he followed any relevant guidance which was at the time—

(a) issued by a supervisory authority or any other appropriate body;

(b) approved by the Treasury; and

(c) published in a manner approved by the Treasury as suitable in their opinion to bring the guidance to the attention of persons likely to be affected by it."

5.7. The JMLSG Guidance Notes fulfil the requirements of regulation 42(3) and provides commentary on best practice within the financial services industry. The FSA has had regard to the JMLSG Guidance Notes in considering whether a breach of the Regulations has occurred in this case.

5.8. Regulation 42(2) of the Regulations provides that:

"The designated authority must not impose a penalty on a person under paragraph (1) where there are reasonable grounds for it to be satisfied that the person took all reasonable steps and exercised all due diligence to ensure that the requirement would be complied with."

5.9. The FSA is not satisfied that RBSG took all reasonable steps and exercised all due diligence during the Relevant Period to ensure that regulations 20(1)(a), (d) and (f) would be complied with for the following reasons:

(1) the sanctions screening project with RBSG initially focussed on screening payments made to the US, and to US institutions. There was a lack of timely consideration throughout 2008 of the risks associated with a failure to comply with the Regulations;

(2) RBSG failed to regularly review the effectiveness of fuzzy matching following its initial implementation in 2006;

(3) RBSG (through GS&F) began to become aware of weaknesses in its sanctions screening procedures from November 2007, prior to the commencement of the independent review by the Accountants. However, GS&F did not act to address those weaknesses prior to the completion of the independent review;

(4) GS&F failed to ensure that issues relating to their UK sanctions screening software were resolved with the software provider in a timely manner; and

(5) although GS&F instructed the Accountants in early 2008 to carry out an independent review to benchmark RBSG's screening software against a peer group, two of the key issues identified by the Accountants were not correctly classified on RBSG's internal risk logging system with the result that the issues were not escalated appropriately and addressed by the relevant risk management committees within RBSG.

6. FACTORS RELEVANT TO DETERMINING THE PROPOSED ACTION

Relevant guidance on sanction

6.1. Regulation 42(1) of the Regulations provides that the FSA:

"*may impose a penalty of such amount as it considers appropriate on a relevant person who fails to comply with any requirement in regulation … 20(1) … and, for this purpose, "appropriate" means effective, proportionate and dissuasive.*"

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

6.3. Paragraph 19.82 of the Enforcement Guide states that, when imposing or determining the level of a financial penalty under the Regulations, the FSA's policy includes having regard to relevant factors in the Decisions Procedure and Penalties manual (DEPP) which came into force as part of the FSA's Handbook of Rules and Guidance on 28 August 2007, specifically DEPP 6.2.1G and DEPP 6.5.

6.4. DEPP 6.5 sets out some of the factors that may be of particular relevance in determining the appropriate level of a financial penalty. DEPP 6.5.1 G states that the criteria listed in DEPP 6.5 are not exhaustive and all relevant circumstances of the case will be taken into consideration. In determining whether a financial penalty is appropriate and the amount, the FSA is required therefore to consider all the relevant circumstances of the case.

Deterrence

6.5. The involvement of UK financial institutions in providing funds, economic resources or financial services to or for the benefit of designated persons, without having first obtained a licence from the Treasury undermines the integrity of the UK financial services sector. Unless they have in place robust systems and controls which govern the circumstances in which customers are accepted or payments may be made or received, UK financial institutions risk contravening the UK's financial sanctions and anti-terrorism regime. The FSA's financial crime and market confidence statutory objectives are both endangered by UK firms' failures in this regard.

6.6. The FSA considers that the financial penalty imposed will promote high standards of regulatory conduct within RBSG and deter them from committing further breaches. The FSA also considers that the financial penalty will help deter other firms from committing similar breaches as well as demonstrating generally the benefits of a compliant business.

The nature, seriousness and impact of the breach in question

6.7. The FSA has had regard to the seriousness of the breaches, including the nature of the requirements breached, the number and duration of the breaches and whether the breaches revealed serious or systemic weakness of the management systems or internal controls. The FSA considers that RBSG's breaches, which existed for a

period of approximately one year, are of a particularly serious nature. In particular, the failure to screen certain payments created an unacceptable risk that payments could have been made to or from a designated person.

The extent to which the breach was deliberate or reckless

6.8. The FSA does not consider that the misconduct on the part of RBSG was deliberate or reckless.

The size, financial resources and other circumstances of the person on whom the penalty is to be imposed

6.9. The FSA has taken into account RBSG's size and financial resources.

Disciplinary record and compliance history

6.10. RBS was fined £750,000 in December 2002 for contravening the FSA's Money Laundering Handbook (in force at the time) by failing to adequately establish customers' identities prior to opening an account.

Conduct following the breach

6.11. The FSA recognises that the following steps carried out by the current senior management of RBSG aimed at enhancing systems and controls in relation to UK sanctions screening served to mitigate the seriousness of the failings of RBSG:

(1) in 2009, a co-ordinated action plan was put in place by the senior management of RBSG to address issues raised by GIA and the Accountants;

(2) RBSG reviewed its governance arrangements and consequently the management of the UK sanctions screening policies was transferred from Group Manufacturing to Group Regulatory Risk and Compliance;

(3) management information requirements were reviewed, leading to improved information on sanctions-related issues for senior management review;

(4) screening of various payments was commenced, including all inbound payments, outbound domestic Sterling payments, various Trade Finance messages and payments entered directly into the gateway application for SWIFT messages;

(5) the FS&TF Procedural Guidelines were revised in December 2008; and

(6) application of fuzzy matching standards were clarified and enhanced.

6.12. Since the discovery of its failings in December 2008, RBSG and their current senior management have fully cooperated with the FSA's investigations.

7. DECISION MAKER

7.1. The decision which gave rise to the obligation to give this Notice was made by the Settlement Decision Makers on behalf of the FSA.

8. IMPORTANT

Access to Evidence

8.1. The FSA grants you access to:

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

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

8.2. There is no such secondary material to which the FSA grants you access.

Manner of and time for Payment

8.3. The financial penalty must be paid in full by RBSG to the FSA by no later than 2 August 2010, 14 days from the date of this Notice.

If the financial penalty is not paid

8.4. If all or any of the financial penalty is outstanding on 3 August 2010, the FSA may recover the outstanding amount as a debt owed by RBSG and due to the FSA.

Confidentiality and Publicity

8.5. The FSA must publish such information about the matter to which this Notice relates as the FSA considers appropriate. The information may be published in such manner as the FSA considers appropriate. However, the FSA may not publish information if such publication would, in the opinion of the FSA, be unfair to you or prejudicial to the interests of consumers.

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

FSA Contacts

8.7. For more information concerning this matter generally, you should contact Mark Lewis at the FSA (direct line: 020 7066 4244 / fax: 020 7066 4245).

…….

Margaret Cole

Settlement Decision Maker,
acting for and on behalf of the FSA

……..

Clive Adamson

Settlement Decision Maker,
acting for and on behalf of the FSA

Appendix 1

1.1. As a member of the United Nations, the United Kingdom is required by article 25 of the United Nations Charter to carry out decisions of the UN Security Council. Consequently, the United Kingdom enacted the United Nations Act 1946 (the Act), section 1 of which empowered the making of Orders in the UN Security Council to make such provision as appeared "*necessary or expedient*" for enabling measures required by such Resolutions to be effectively applied in the United Kingdom. The Terrorism (United Nations Measures) Order 2006[1] (the Terrorism Order) and The Al-Qaida and Taliban (United Nations Measures) Order 2006[2] (the Al-Qaida and Taliban Order) were adopted by the United Kingdom using the powers conferred by section 1 of the Act[3].

1.2. Article 8 of the Terrorism Order provides that:

"A person must not make funds, economic resources or financial services available, directly or indirectly, to or for the benefit of a person referred to in article 7(2) unless he does so under the authority of a licence granted (by the Treasury) under article 11."

1.3. Article 8 of the Al-Qaida and Taliban Order states that:

"A person must not make funds or economic resources available, directly or indirectly, to or for the benefit of a person referred to in article 7(2) unless he does so under the authority of a licence granted (by the Treasury) under article 11."

1.4. In both Orders, a person referred to in article 7(2) includes any person identified in a direction by the Treasury (a designated person).

---

[1] SI 2006 No. 2657.
[2] SI 2006 No. 2952.
[3] In *Ahmed and others v HM Treasury* [2010] 2 W.L.R. 378 the Terrorism Order and article 3(1)(b) of the Al-Qaida and Taliban Order were declared *ultra vires* by the UK Supreme Court. Both Orders have subsequently been revoked by the Terrorism (United Nations Measures) Order 2009/1747 and the Al-Qaida and Taliban (Asset Freezing) Regulations 2010/1197 respectively.