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:	**Ghana International Bank Plc**
FCA Reference Number:	**204471**
Address:	**1st Floor Regina House, 67 Cheapside, London EC2V 6AZ**
Date:	**23 June 2022**

1. ACTION

1.1. For the reasons given in this Decision Notice the Authority has decided to impose on Ghana International Bank Plc ("GIB") a civil penalty of £5,829,900.

1.2. GIB 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 £8,328,500 on GIB.

2. SUMMARY OF REASONS

2.1. On the basis of the facts and matters described below, GIB breached Regulations 14(1), 14(3) and 20(1) of the Money Laundering Regulations 2007 (the "ML Regulations") by failing to:

(1) establish and maintain appropriate and risk-sensitive policies and procedures;

(2) conduct adequate enhanced due diligence ("EDD") when establishing new business relationships; and

(3) conduct adequate enhanced ongoing monitoring.

2.2. The breaches concerned GIB's anti-money laundering and counter-terrorist financing controls over its correspondent banking activities in the period between 1 January 2012 and 31 December 2016 (the "Relevant Period"). During the Relevant Period, the monetary value of funds flowing between GIB and its respondent banking customers, net of transfers between customers' own accounts and fixed deposits, totalled £9.5 billion.

2.3. When banks fail to implement and adhere to their legal and regulatory anti-money laundering obligations, the risk that they will be used to facilitate money laundering or terrorist financing is increased. The consequences of poor financial crime controls in a high-risk sector such as correspondent banking are significant. It can lead to criminals abusing the financial system to launder the proceeds of crime, supporting further criminal activity and damaging the integrity and stability of the UK financial system.

2.4. In correspondent banking transactions, correspondents often have no direct relationship with the underlying parties to a transaction and limited information regarding the nature and purpose of the underlying transaction. Correspondent banking is therefore in the main non face-to-face business and must be regarded as high risk from a money laundering and/or terrorist financing perspective. Firms undertaking such business are required by the ML Regulations to apply on a risk-sensitive basis enhanced customer due diligence measures and enhanced ongoing monitoring. For those correspondents proposing to have correspondent banking relationships with respondents from non-EEA states, the ML Regulations also require the correspondent to undertake a number of specific actions. These are listed in ML Regulation 14(3). In addition, the person subject to the ML Regulations must establish and maintain appropriate and risk-sensitive AML

policies and procedures relating, among other things, to customer due diligence, ongoing monitoring and also relating to the internal communication of and management of compliance with such policies and procedures.

2.5. Throughout the Relevant Period, GIB did not recognise its correspondent banking business as a separate business line or product area but instead included revenue from this business within its other business lines. GIB did not appropriately include correspondent banking business in any of its departmental-specific policies or procedures throughout the Relevant Period. Staff seeking practical instruction on how to onboard and monitor respondents needed to review several fragmented, confusing and overlapping policies, manuals, frameworks and forms, where correspondent banking was either insufficiently considered, or not at all.

2.6. Where GIB's policies or procedures provided for treatment of the AML risks associated with correspondent banking, references were vague and lacked sufficient detail so that staff undertaking EDD and ongoing monitoring could not adequately fulfil their critical roles in assisting GIB in preventing money laundering and financial crime. GIB failed to establish appropriate procedures which clearly explained to staff how to conduct EDD on respondents during their onboarding process, and subsequent ongoing monitoring. GIB's failure to establish, maintain and communicate appropriate and risk-sensitive policies and procedures in relation to correspondent banking contributed to its EDD and enhanced ongoing monitoring failures.

2.7. Examples of the practical effect of GIB failing to direct staff how to undertake EDD in respect of the 14 respondents it onboarded during the Relevant Period, include GIB's failure to:

(1) obtain sufficient information about the purpose and intended nature of business from all 14 respondents;

(2) perform adverse media checks in relation to 11 of the 14 respondents;

(3) determine the quality of supervision in respect of 8 out of the 9 respondents onboarded in 2014;

(4) evidence that it had received or assessed the AML controls for 12 of the 14 respondents;

(5) obtain senior management approval for 3 of the 14 respondents. A further 6 approvals were illegible and 1 was approved the day after GIB onboarded the respondent;

(6) document the respective responsibilities in the case of at least 12 of the 14 respondents.

2.8. GIB failed to ensure its staff undertook full periodic reviews of the information it held in relation to respondents on an annual basis and in accordance with its own requirements.

2.9. In response to certain trigger events, such as Ghana being subject to a FATF "Public Statement", FCA publications, and feedback from external experts, while GIB carried out exercises to seek to fill gaps in its EDD, it was slow to contact respondents, and then to follow up with those who failed to reply, routinely permitting many months to pass before repeating its requests. In the period between its initial contact and follow up contact, GIB did not place restrictions on the respondents' accounts. Ultimately, GIB failed to obtain important items concerning the respondents' anticipated transaction volumes and values, AML controls and client reputation. Without this information, GIB's ability to identify and adequately to assess the risks posed by each respondent was limited as it would have been unable to use such information to establish a base for monitoring customer activity and transactions.

2.10. GIB routinely failed to obtain the evidence it needed to scrutinise transactions appropriately using a risk-based approach to ensure that transactions were in keeping with GIB's knowledge of the respondent, including their activities and risk profile.

2.11. In one instance, GIB failed to undertake any ongoing monitoring of a respondent from the start of the Relevant Period until March 2015 when it identified the respondent had ceased to trade some 5 years earlier. More typically, several years passed between periodic reviews.

2.12. GIB failed to provide guidance to its staff as to how it expected them to perform transaction monitoring, such as explaining methods of monitoring, identifying who was responsible, the risk thresholds, or practical guidance regards linked transactions.

2.13. From December 2014 until the end of the Relevant Period, GIB engaged with several independent experts who provided advice regarding steps GIB needed to

take to fulfil its AML obligations. In light of this advice, GIB failed to make sufficient amendments to its policies and procedures to ensure that they were appropriate and risk-sensitive before the end of the Relevant Period.

2.14. The Authority considers that GIB's failures are particularly serious as prior to and throughout the Relevant Period, the Authority issued a number of publications and disciplinary notices which highlighted the high-risk nature of correspondent banking. Further, other international and domestic governmental organisations issued communications regarding jurisdictions with a high risk of money laundering and financial crime, including a period during which Ghana, GIB's dominant respondent market, was subject to a FATF "Public Statement". Despite this, GIB still failed to address the deficiencies in its policies and procedures, due diligence and ongoing monitoring to ensure that they were sufficiently appropriate and risk-sensitive to counter the risks posed by correspondent banking. These failures meant that there was a significant risk that GIB would be unable to identify and adequately assess the risks posed by each respondent at onboarding and thereafter, and that GIB would fail to properly scrutinise the £9.5 billion respondent banking customer transactions it processed during the Relevant Period.

2.15. In December 2016, the Authority visited GIB to review its financial crime control framework. As a result of concerns identified during this visit, GIB agreed to a voluntary business restriction, preventing GIB from onboarding any new customers. The restriction remains in place. A skilled person was also appointed under section 166 of the Financial Services and Markets Act 2000. GIB continues to work with the Authority and the skilled person to improve its financial crime controls and to remediate its correspondent banking files.

2.16. In light of the above failings, the Authority has decided to impose a financial penalty on GIB in the amount of £5,829,900 after 30% (stage 1) discount (£8,328,500 before discount) pursuant to Regulation 42 of the ML Regulations.

2.17. The Authority recognises that:

(1) GIB and its senior management have worked in an open and co-operative manner with the Authority, including by agreeing to a voluntary business restriction while seeking to remediate its AML breaches and in notifying the Authority of AML shortcomings; and

(2) GIB has taken significant steps in improving its AML systems and controls including instituting a number of measures since the end of the Relevant Period seeking to address the issues in this Notice.

3. DEFINITIONS

3.1. The definitions below are used in this Notice:

"AML" means anti-money laundering;

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

"correspondent" – see definition of correspondent banking;

"correspondent banking" means the term as used in Regulation 14 of the ML Regulations and which is described in JMLSG Guidance, Part II, paragraph 16.1 as being the provision of banking-related service by one bank (the "correspondent") to an overseas bank (the "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;

"CTF" means counter terrorist financing;

"customer due diligence" and "CDD" mean customer due diligence measures as defined by Regulation 5 of the ML Regulations;

"DEPP" means the Authority's Decision Procedures and Penalties Guide;

"due diligence" means together customer due diligence and enhanced due diligence obligations;

"Enhanced due diligence" and "EDD" mean enhanced customer due diligence measures. The circumstances where enhanced due diligence should be applied are set out in Regulation 14 of the ML Regulations;

"FATF" means the Financial Action Task Force which is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing. FATF has established a set of recommendations that set out the basic framework for anti-

money laundering efforts and are intended to be of universal application. The mutual evaluation programme is the primary instrument by which the FATF monitors progress made by member governments in implementing the FATF recommendations;

"GIABA" means the Inter-Governmental Action Group Against Money Laundering in West Africa which is responsible for facilitating the adoption and implementation of AML and CTF in West Africa. GIABA is also a FATF-styled regional body working with its member states to ensure compliance with international AML/CTF standards;

"Internal Auditor" means a third-party firm contracted to act as GIB's internal auditor during the Relevant Period;

"JMLSG" means the Joint Money Laundering Steering Group;

"JMLSG Guidance" means the guidance issued by the JMLSG on compliance with the legal requirements in the ML Regulations, regulatory requirements in the Authority Handbook and evolving practice within the financial services industry from time to time;

"KYC" means know your customer;

"the ML Regulations" means the Money Laundering Regulations 2007, which were in force in respect of conduct from 15 December 2007 until 25 June 2017 inclusive and implement the third money laundering directive. The ML Regulations impose requirements on relevant persons (including credit institutions) to establish, maintain and apply appropriate AML controls over their customers;

"PEP" means politically exposed person as defined in Regulation 14(5) of the ML Regulations;

"Public Statement" means FATF's 16 February 2012 list of jurisdictions with strategic AML/CTF deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies, that included Ghana;

"the Relevant Period" means the period from 1 January 2012 to 31 December 2016;

"respondent" – see definition of correspondent banking;

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

"Wolfsberg Questionnaire" means the anti-money laundering questionnaire produced and updated from time to time by the Wolfsberg Group, an association of 13 global banks which aims to develop frameworks and guidance for the management of financial crime risks, particularly with respect to Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies. The questionnaire was available on the Wolfsberg Group's website and could be downloaded and used by financial institutions.

4. FACTS AND MATTERS

Background

4.1. GIB is a Ghanaian owned bank based in London with an office in Accra, Ghana. Throughout the Relevant Period, GIB did not recognise its correspondent banking business as a separate business line or product area but instead revenue generated from correspondent banks was included within GIB's relevant business lines: retail banking, global transfer services, international trade finance and treasury business lines, depending upon the specific transaction/product area. The number of GIB's correspondent banking relationships varied from time to time during the Relevant Period, but at its peak consisted of 51 financial institutions in non-EEA jurisdictions, 28 of which were in Ghana with most of the rest in West Africa. During the Relevant Period, GIB onboarded 14 respondents.

Overview of AML legal and regulatory obligations

4.2. The ML Regulations require UK firms to establish and maintain appropriate and risk sensitive policies and procedures to prevent activities related to money laundering and terrorist financing. This includes conducting due diligence and ongoing monitoring for all customers on a risk-sensitive basis. Where a firm offers products and services which could present a higher risk of financial crime, such as in relation to correspondent banking relationships with respondents from non-EEA countries, it must conduct EDD and enhanced ongoing monitoring on its respondents. This requirement is set out in Regulations 14 (1) and (3) of the ML Regulations.

4.3. The ML Regulations also require UK firms to establish and maintain appropriate and risk sensitive policies and procedures relating to the monitoring and management of compliance with, and internal communication of, those policies and procedures.

4.4. As all the respondents with whom GIB had a correspondent banking relationship during the Relevant Period were based in non-EEA jurisdictions, Regulation 14 of the ML Regulations required GIB to apply EDD and enhanced ongoing monitoring. Consequently, throughout the Relevant Period, GIB assigned correspondent banking its highest risk rating, acknowledging these relationships are "*the most risky in terms of Compliance risks*".

4.5. 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 including that (1) approved by HM Treasury, such as the JMLSG Guidance, and (2) issued by the Authority.

4.6. Relevant extracts from the ML Regulations and JMLSG Guidance are set out in Annex A to this Notice.

Due diligence and ongoing monitoring arrangements

4.7. The ML Requirements set out:

(1) When firms must apply CDD measures. These include when establishing business relationships and when carrying out occasional transactions.

(2) When carrying out CDD, firms must determine the extent of CDD measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction.

(3) A definition of CDD measures as identifying and verifying a customer or beneficial owner, and obtaining information on the purpose and intended nature of the business relationship.

4.8. If a firm is unable to apply CDD measures, it must not carry out a transaction with or for that customer through a bank account, must not establish a business relationship or carry out an occasional transaction with the customer, and must terminate any existing business relationship with the customer.

4.9. EDD and enhanced ongoing monitoring measures are designed to take account of the greater potential for money laundering in higher risk business relationships and reduce the risk that a firm will be used by those seeking to launder the proceeds of crime, finance terrorism or evade financial sanctions. Where a firm has assessed that the business relationship with the customer presents a higher risk of money laundering or terrorist financing, it must conduct EDD.

4.10. A firm must also conduct ongoing monitoring of all business relationships, tailored in accordance with the firm's risk assessment of that customer. Ongoing monitoring includes:

(1) keeping customer information up to date through periodic review or reviews of the due diligence in response to trigger events; and

(2) scrutinising customer transactions to ensure that they are consistent with the firm's knowledge of the customer (including where necessary, the source of funds), its business and risk profile.

4.11. Where the business relationship is considered to be higher risk, the ongoing monitoring must be enhanced, meaning more frequent or intensive monitoring.

Correspondent banking requirements

4.12. Correspondent banking is the provision of banking-related services by one bank (the correspondent) to an overseas bank (the respondent) to enable the respondent to provide its own customers with cross-border products and services that it cannot provide itself, typically because of a lack of international network.

4.13. As the correspondent often has no direct relationship with the underlying parties to a transaction, it is reliant on the respondent's AML controls to prevent the underlying parties from gaining access to the UK financial system for the purposes of money laundering or terrorist financing. The ML Regulations and JMLSG Guidance acknowledge that correspondent banking relationships with respondents from non-EEA states presents a particularly high risk of money laundering.

4.14. The ML Regulations at Regulation 14 therefore require, specific to the respondent relationship, correspondents to carry out EDD and enhanced ongoing monitoring on non-EEA respondents. Actions the correspondent must take include:

(1) gathering sufficient information about the respondent to fully understand the nature of its business;

(2) determining the respondent's reputation and the quality of its supervision from publicly available information;

(3) assessing the respondent's AML controls;

(4) obtaining senior management approval before establishing a new correspondent banking relationship; and

(5) documenting the respective responsibilities of the respondent and correspondent.

4.15. The ML Regulations stipulate that these requirements must be applied on a risk-sensitive basis.

Deficiencies in GIB's AML controls

4.16. The Authority found deficiencies in GIB's AML controls regarding its correspondent banking relationships. These included failings in its:

(1) policies and procedures;

(2) EDD; and

(3) enhanced ongoing monitoring.

Deficiencies in policies and procedures

4.17. In response to its legal and regulatory obligations under the ML Regulations, as applicable to its correspondent banking business, GIB established versions of various policies and procedures during the Relevant Period, including the following non-exhaustive list. Each was in force throughout the Relevant Period unless otherwise stated:

(1) Fraud and Money Laundering Policy;

(2) Money Laundering Reporting Manual;

(3) Retail Banking Manual;

(4) KYC Procedures – Know Your Customer Policy Manual (KYC Policy Manual) – effective from November 2016;

(5) Risk Management Policy – effective from November 2014;

(6) Risk Management Framework – effective from February 2016;

(7) Operational Risk Management Framework – effective from February 2016;

(8) Risk Assessment Form – effective from September 2012; and

(9) Anti-Financial Crime Policy - effective from October 2016.

4.18. Throughout the Relevant Period, staff employed to onboard and monitor respondents in accordance with GIB's policies and procedures, needed to rely on fragmented, confusing and overlapping policies, manuals, frameworks and forms including those listed at paragraph 4.17 above. As detailed in paragraphs 4.19 to 4.78 below, when taken individually, or as a body of corporate documentation, these policies and procedures were not appropriate or sufficiently risk-sensitive to address the money laundering risks posed by GIB's correspondent banking business.

Fraud and Money Laundering Policy

4.19. Throughout the Relevant Period, while GIB had a Fraud and Money Laundering Policy in place, the policy was vague and lacked sufficient detail, as set out below, for staff to understand their responsibilities, carry out their role in a consistent manner and in accordance with the rules, regulations and guidance to which GIB was required to adhere.

Lack of detailed explanation of risk

4.20. The Fraud and Money Laundering Policy referred to the need to conduct due diligence to identify all new customers satisfactorily. However, it did not include detail on the different classifications of risk nor the circumstances in which EDD needed to be performed.

4.21. When, from April 2013, a section was added to the policy referring to higher risk customer types, this was limited to requiring "*Enhanced due diligence to be undertaken on customers assessed to be high risk*". While the policy specified the broad types of customer that staff should consider high-risk, including correspondent banking customers, this addition failed to provide any further detail or context such as what GIB meant by "*Enhanced due diligence*" specific to its systems and processes, nor how staff should practically apply the policy. This aspect of the policy was in place for the remainder of the Relevant Period.

Absence of guidance on periodic review

4.22. Aside from requiring an annual sanctions check, the Fraud and Money Laundering Policy did not reflect the need to undertake periodic reviews for the purposes of keeping due diligence up to date for all of GIB's customers nor the frequency of those reviews. From April 2015, the policy was amended to require that customer files should be subject to "*update*", with frequency ranging from every 1 to 3 years depending on their risk categorisation. With no further practical detail provided,

GIB failed to establish an appropriate policy. GIB's Fraud and Money Laundering Policy therefore left the process for individual staff members to interpret themselves without communicating it effectively internally.

4.23. The failure to produce a sufficiently detailed policy meant there was a significant risk that staff would not understand what activities could constitute money laundering or the due diligence and ongoing monitoring they needed to undertake in an effort to prevent money laundering from taking place.

Anti-Financial Crime Policy

4.24. While GIB's Fraud and Money Laundering Policy was effective until at least the end of the Relevant Period, on 19 October 2016, GIB's Board approved a separate Anti-Financial Crime Policy. Despite the clear potential for overlap between these two policies, the Anti-Financial Crime Policy made no reference to the Fraud and Money Laundering Policy leaving it unclear which policy staff should follow.

4.25. The Anti-Financial Crime Policy included reference to GIB's "*comprehensive set of measures to identify, manage and control its AML risk*" that includes a list of "*risk analysis*", "*controls*", "*programs*", "*safeguards*", "*training*", "*processes*", and a separate "*Anti-Bribery and Corruption (ABC) Policy*", but failed to specify which of GIB's various policies and procedures were applicable in which circumstances. The cumulative effect was that GIB's failure to communicate its policies clearly internally meant it could not rely on staff to interpret them in a consistently appropriate and risk-sensitive way.

4.26. GIB's Anti-Financial Crime Policy included some additional sections beyond those included in its Fraud and Money Laundering Policy but was similarly framed as a high-level overview and did not provide further sufficient practical detail.

4.27. Improvements on the April 2015 Fraud and Money Laundering Policy contained within the Anti-Financial Crime Policy included a list of 7 "*safeguards*" for its correspondent banking business. These were high-level, for example "*obtaining sufficient information on the correspondent to fully understand the nature of its business, its reputation, management and ownership structure and maturity of the bank's regulation and supervision in the respondent's country*". GIB provided no guidance as to how staff should interpret "*sufficient*" or "*fully understand*" in this context.

Procedures

4.28. During the Relevant Period, GIB's Fraud and Money Laundering Policy was supplemented by several manuals, including the Money Laundering Reporting Manual and the Retail Banking Manual. At the end of the Relevant Period, GIB further implemented a KYC Policy Manual.

(1) The purpose of the Money Laundering Reporting Manual was to assist staff to understand GIB's Money Laundering Policy, the legal requirements and penalties for non-compliance, and the procedures that GIB had in place.

(2) The purpose of the Retail Banking Manual was to assist staff with the opening of new customer accounts as well as the practicalities of providing over the counter services to customers on a day-to-day basis.

4.29. GIB's Money Laundering Reporting and Retail Banking manuals failed to establish appropriate procedures which would have assisted staff to perform EDD on proposed respondents and ongoing monitoring and transaction monitoring over all of its respondents. (The failings in this regard are detailed in paragraphs 4.31 to 4.34 and 4.42 to 4.43 below).

Failure to establish an appropriate procedure for conducting due diligence on proposed respondents

4.30. GIB failed to establish appropriate procedures which explained how to conduct due diligence on proposed respondents.

Money Laundering Reporting Manual

4.31. GIB's Money Laundering Reporting Manual included a section on customer due diligence with separate sections which set out how personal customers, corporate customers, clubs, societies and charities, and correspondent banks should be vetted.

4.32. At the start of the Relevant Period, the correspondent banking section of the Money Laundering Reporting Manual included a short 6-point list of the due diligence to be performed before establishing a correspondent banking relationship. This included instruction for staff to:

(1) Collect "*the necessary information*" about the ownership, management, major business activities, location, the quality of AML prevention and detection efforts of the respondent; and

(2) "*review publicly available information to determine whether the institution/Bank with which it has correspondent/inter banking relationship has* (sic) *been subject to breach* (sic) *of money laundering regulations*".

4.33. In limiting its instruction to collecting "*the necessary information*", GIB took insufficient steps to prevent a "paper gathering" exercise with staff undertaking no or only limited assessment of the information collected. The Money Laundering Reporting Manual did not set out the practical instructions staff would require to collect or assess the respondent's AML controls in an appropriate or risk-sensitive way, to determine the respondent's reputation and the quality of its supervision or to document the respective responsibilities of the respondent and GIB, as correspondent.

4.34. In September 2012, GIB amended its Money Laundering Reporting Manual. Whilst the requirements of Regulation 14(3) of the ML Regulations were broadly listed in the correspondent banking section, the Money Laundering Reporting Manual still did not explain how EDD checks relevant to GIB's business should be performed in practice. This provided insufficient guidance to enable consistent staff interpretation and this remained the case when GIB further updated its Money Laundering Reporting Manual in May 2013 and June 2014. In a report dated 19 December 2014, the Internal Auditor provided detailed recommendations on steps GIB needed to take to improve the design and operation of its AML controls. 18 months later, in an internal report dated June 2016, GIB acknowledged that its Money Laundering Reporting Manual still required updating. Despite this, GIB did not update its Money Laundering Reporting Manual again before the end of the Relevant Period and it consequently was not fit for purpose throughout the Relevant Period.

Checklists

4.35. Throughout the Relevant Period, each version of GIB's Money Laundering Reporting Manual had as an appendix a specimen checklist which staff were to use when opening new customer accounts. While sections of the Money Laundering Reporting Manual pertaining to personal customers, general corporate customers, and clubs, societies and charities included direct instruction for staff to complete the relevant checklist, there was no such reference to checklists within the correspondent banking section of the Money Laundering Reporting Manual. In any event, the checklists appended were not specific to respondents

and did not refer to any of the EDD requirements in Regulation 14(3) of the ML Regulations as detailed in paragraph 4.34 above.

4.36. In April 2015, GIB introduced a "*Requirements for correspondent banking*" checklist. However, this still did not list all the information that staff needed to obtain nor the checks and searches that they needed to perform when onboarding a respondent. For example, the checklist did not remind staff to obtain information about the nature of the respondent's business, expected account activity including anticipated transaction volumes and values, or include details of the checks and searches staff should perform when determining the reputation of the respondent and the quality of its supervision.

4.37. In a report dated 9 November 2015, the Internal Auditor noted that "*A standard checklist outlining all required checks to be performed and evidence to be obtained is not currently in use. This has resulted in gaps in the evidence within the correspondent banking client files*."

4.38. Although an updated version of the "*Requirements for correspondent banking*" checklist was introduced in August 2016, it still did not direct staff to obtain information about expected account activity or list the checks that staff needed to perform to determine reputation and quality of supervision.

4.39. In a report dated 6 September 2016, the Internal Auditor commented that "*On-boarding checklists are inconsistently used."* The following month, in October 2016, GIB implemented an "*Account Opening Requirement List*" and a "*Financial Institutions Account Opening Checklist*". Whilst the later checklist included more detail about the information to be obtained and the checks to be performed when onboarding a respondent, GIB did not address the inadequacies set out in paragraph 4.38 above in the requirement list. This version of the checklist remained in use until the end of the Relevant Period.

<u>KYC Policy Manual</u>

4.40. In November 2016, GIB implemented a "*KYC Procedures – Know Your Customer Policy Manual*" with the purpose of "*implementing the KYC norms*". This was a high-level document which set out GIB's customer acceptance policy, risk categories, customer identification and transaction monitoring procedures. The annex contained indicative guidelines which set out the customer identification requirements for all GIB's customer types, including respondents. Staff were advised to "*gather sufficient information to understand fully the nature of the*

business of the correspondent/respondent bank" to include "*information on the other bank's management, major business activities, level of AML/CTF compliance, purpose of opening the account, identity of any third-party entities that will use the correspondent banking services, and regulatory/supervisory framework in the correspondent's/respondent's country*." Staff were also required to ascertain from publicly available information whether the respondent had been subject to any money laundering or terrorist financing investigations or regulatory action.

4.41. The KYC Policy Manual and annex did not explain how staff should meet GIB's customer identification requirements in practice or specify the level of detail required. Consequently, it was not clear to staff who they should approach to obtain the information needed or if any particular searches or analysis needed to be performed.

Retail Banking Manual

4.42. The Retail Banking Manual in use during the Relevant Period did not contain information about the EDD that needed to be performed when onboarding a respondent. It included cross-references to the Money Laundering Reporting Manual and instructed staff to complete a checklist that was appended to that manual as part of the account opening process. As stated in paragraphs 4.35 to 4.39 above, the checklist was not specific to respondents in correspondent banking relationships so did not set out all of the EDD that needed to be performed.

4.43. In the absence of communicating an appropriate procedure which explained how to conduct EDD on a proposed respondent, there was a risk that GIB's staff would not understand what information and documentation they needed to obtain and what related checks they needed to perform. Any gaps in the EDD performed would directly affect GIB's ability to determine the risks posed by each respondent and thus its decision as to whether a business relationship should be established.

Failure to establish an appropriate procedure for determining the reputation of a respondent

4.44. Regulation 14(3)(b) required correspondents to determine from publicly available information the reputation of a respondent.

4.45. At the start of the Relevant Period and as noted above in paragraphs 4.32 and 4.33, GIB's Money Laundering Reporting Manual included a requirement for staff

to ascertain "*necessary information*", and to review publicly available information to determine whether a respondent had been subject to breach of the ML Regulations. The requirement for staff to collect necessary information about the reputation of its respondents' owners, managers and business was added to the manual in September 2012. This version of the Money Laundering Reporting Manual went further by also requiring that staff:

(1) consider material ownership changes within the prior 5 years;

(2) consider "*a more detailed understanding of the experience*" of all respondents' executive management, including "*recent material changes*" in respondents' executive management structure within the prior 2 years; and

(3) "*understand fully*" the nature of the respondents' business.

4.46. Following GIB's amendment in September 2012, this aspect of the Money Laundering Reporting Manual then remained unchanged until the end of the Relevant Period. None of GIB's other policies and procedures contained further instruction regarding determination of respondents' reputation.

4.47. Aside from the above, GIB's Money Laundering Reporting Manual provided no further guidance as to how staff should undertake reputational checks. Relying on the Money Laundering Reporting Manual would not have provided sufficient clarity to staff as to when and in which circumstances checks should be carried out nor how to assess and deal with any adverse public information found. Therefore, while the Authority recognises that GIB did establish a procedure for determining the reputation of a respondent, which from September 2012 included a requirement to determine the reputation of the respondent's owners, managers and business, that procedure was not appropriate or risk sensitive because it was not of sufficient rigour to identify potential activities related to money laundering and terrorist financing.

Failure to establish an appropriate procedure for the ongoing monitoring and transaction monitoring of respondent accounts

4.48. Transaction monitoring of respondent accounts can help mitigate the money laundering risks arising from correspondent banking activities. GIB was required by the ML Regulations to maintain appropriate and risk-sensitive ongoing monitoring policies and procedures.

4.49. This included requirements for GIB to:

(1) Identify and scrutinise specified types of high-risk transactions undertaken by its respondent banking customers, such as:

a) unusually large transactions;

b) transactions with no apparent purpose; and

c) transactions regarded by the nature of the respondent's business, to be related to money laundering.

(2) Scrutinise its respondent banking customers' transactions, including the source of funds, to ensure that the transactions were consistent with GIB's knowledge of the customer, its business and its risk profile; and

(3) Keep the documents, data or information obtained from its respondent banking customers for the purpose of applying customer due diligence measures up-to-date.

4.50. GIB failed to establish an appropriate procedure which explained to staff how, in relation to respondent banks, they should (1) undertake ongoing monitoring to identify and scrutinise transactions, whether specified types of high-risk transaction or otherwise, and (2) ensure that information was up-to-date.

Money Laundering Reporting Manual

4.51. The Money Laundering Reporting Manual in place at the start of the Relevant Period included a requirement for staff to "*to revisit and update customer information […] whenever a customer is formally interviewed or opens a new account or new information is received*". It further stated that updated information, "*will assist in deciding whether a transaction is out of the ordinary or not and therefore whether it should be reported as suspicious*". However, while this requirement was included in relation to several customer types, including personal and corporate customers, the section of the Money Laundering Reporting Manual dedicated to correspondent banking, including a subsection specific to "*due diligence procedures*" contained no such requirement. More generally, it failed to state or explain that reviews should take place in accordance with the risk rating assigned to each customer or provide any indication of the risk-related frequency with which GIB required the reviews to be undertaken, (for example, annually), despite this being a recognised industry standard at the time.

4.52. The correspondent banking section of this version of the Money Laundering Reporting Manual referred to the need to perform "*periodical*" reviews. However, this was in the context of performing reviews to identify higher risk counterparties and not in the context of keeping the documents, data or information obtained for the purpose of initial due diligence measures up-to-date, of which this section made no mention.

4.53. Whilst the Money Laundering Reporting Manual referred to the general need, irrespective of the customer type, for staff to report suspicious transactions, it failed to state that transaction monitoring would need to be performed as part of GIB's ongoing monitoring obligations. Consequently, the Money Laundering Reporting Manual did not contain any information about:

(1) who was responsible for performing the transaction monitoring of respondents' accounts;

(2) how transaction monitoring reports were to be produced;

(3) what thresholds were in place; or

(4) the factors that would need to be taken into consideration as part of the monitoring process e.g. nature of business, volume and value of transactions, thresholds or linked transactions.

4.54. In September 2012, GIB amended the correspondent banking section of the Money Laundering Reporting Manual to state that information collected during the customer acceptance and due diligence processes had to be reviewed and updated:

(1) on a periodic (annual) basis for its respondents, as high-risk customers;

(2) on an ad hoc basis as a result of changes to the customer information identified during normal business practices; and

(3) when external factors resulted in a material change in the risk profile of the customer.

4.55. The Money Laundering Reporting Manual still failed to include any practical information regarding how the periodic reviews should be performed, managed or tracked.

4.56. This section of the Money Laundering Reporting Manual was also amended in September 2012 to require ongoing monitoring to include scrutiny of transactions and that the level of account/transaction monitoring activity undertaken should be commensurate with the risks posed by the respondent. No information was added, however, to explain how the transaction monitoring should be performed in practice. This meant that it remained silent on who was to perform the monitoring, how the transaction monitoring reports were to be produced and the factors that needed to be taken into consideration as part of the monitoring process. This remained the case when the Money Laundering Reporting Manual was updated in May 2013 and June 2014. It was not subsequently updated again before the end of the Relevant Period.

4.57. In a report dated 19 December 2014, the Internal Auditor noted that "*There is no process to perform a periodic file review of KYC documentation to ensure it remains up-to-date. This is a requirement of the JMLSG guidance*." In a further report dated 6 September 2016, the Internal Auditor again commented that "… *the client annual KYC review process has not been formalised*." Throughout the Relevant Period, GIB failed to put in place appropriate policies or procedures that explained to staff how to periodically review and update the information it held relating to respondents.

KYC Policy Manual

4.58. GIB's KYC Policy Manual, effective from November 2016, did not include requirements for staff to obtain documents, data or information for the purpose of keeping customer due diligence measures up to date.

4.59. Although the introduction of GIB's KYC Policy Manual stated generically that the policy is "*to be read in conjunction with related operational guidelines*" and from September 2012, the requirement to keep documents, data or information up to date was included within GIB's Money Laundering Reporting Manual, this piece-meal approach necessitated staff referencing multiple policies and manuals in order to obtain organisational guidance. Further, whilst the KYC Policy Manual referred to the need to undertake transaction monitoring, it did not set out how this should be performed in practice.

4.60. In the absence of communicating an appropriate procedure which explained how to perform ongoing monitoring and transaction monitoring, there was a risk that staff would not understand how to perform reviews either of the due diligence held for each respondent or of the transactions that were going through each

respondent's account. This in turn meant that the procedures were not appropriate to prevent money laundering.

Failure to establish an appropriate sanctions screening procedure to follow when onboarding

4.61. Throughout the Relevant Period, GIB's Money Laundering Reporting Manual included a restriction which stated that GIB did not do business with any person or entity on the Consolidated List, a public record of asset freeze targets designated by the United Nations, European Union and United Kingdom. In order to ascertain if a person or entity was on the Consolidated List, sanctions screening needed to be performed.

4.62. At the start of the Relevant Period, sanctions screening when onboarding new customers was performed manually. The process that staff were to follow when performing the sanctions screening was not documented.

4.63. In May 2012, GIB implemented sanctions screening software and introduced a sanctions screening manual to assist with using it. The sanctions screening manual was subsequently amended in December 2012 and November 2015. Whilst all versions of the sanctions screening manual included a direction to use the software's "*lookup*" facility to screen all new customers and the directors and beneficial owners of corporate customers, it did not explain what this facility was until November 2015. Further, whilst all versions of the sanctions screening manual stated that potential matches flagged by the software would be investigated, it did not specify the investigative steps to be followed in order to ascertain if the match was false or positive.

4.64. In July 2016, GIB's Board approved a formal sanctions policy. This was high-level in nature and did not set out the practical steps staff were expected to take when performing sanctions screening or investigating potential matches to the Consolidated List.

4.65. The failure to establish an appropriate sanctions screening procedure to follow when onboarding respondents meant there was a risk that screening would not be performed properly and that potential matches would not be identified, escalated or resolved leading to the risk of money laundering going undetected.

Failure to establish a correspondent banking risk appetite statement

4.66. Regulation 20(1)(e) required firms to establish and maintain appropriate and risk-sensitive policies and procedures relating to risk assessment and management in order to prevent activities related to money laundering and terrorist financing.

4.67. During the Relevant Period, there was no clear articulation of GIB's assessment of the risks associated with correspondent banking, its appetite to such risks or any tolerance towards them. Although GIB introduced a Risk Management Policy in November 2014, its risk management framework and operational risk management framework were not approved until February 2016. Neither the policy nor the frameworks included an assessment of the risks associated with correspondent banking.

4.68. The failure to articulate its assessment of the risks associated with correspondent banking clearly meant that GIB's attitude to risk would not necessarily be taken into consideration when decisions to establish business relationships with respondents were made and thus that decisions might be made which allowed money laundering to take place.

Failure to establish an appropriate risk assessment procedure

4.69. The Authority expects firms to use a risk-based approach to target activities that present the greatest risks, including correspondent banking. This approach enables firms to:

(1) Identify as early as possible suspicious activity and / or high-risk customers;

(2) Prioritise high-risk customers and transactions for review and investigation;

(3) Ensure that resources are focused on higher risk relationships and transactions; and

(4) Ensure AML work on correspondent banking is consistent and high quality on a global basis.

4.70. One key area for firms to consider is the location of the respondent and / or where its parent is based. Some jurisdictions may have more robust regulatory environments and be correspondingly lower risk. Conversely, other jurisdictions are recognised internationally as having inadequate anti-money laundering standards, insufficient regulatory supervision and/or presenting greater risk of financial crime.

4.71. Following the Authority's publication of the Turkish Bank (UK) Ltd Decision Notice in July 2012, GIB introduced a risk assessment form which was to be completed in respect of a proposed respondent at onboarding and thereafter as part of annual periodic reviews. This was inconsistently completed by GIB's staff or the respondents themselves. GIB failed to accompany the risk assessment form with guidance on how it should be completed, or a methodology for determining the resulting risk classification. It was therefore not clear:

(1) what level of detail was required when completing the form;

(2) where guidance could be found which would assist staff to complete the form (for example, in relation to drug source or transit countries);

(3) how much weight should be placed on the information the questions on the form elicited;

(4) when and in which circumstances to escalate to senior management and/or compliance for review;

(5) how much risk GIB was willing to accept; and

(6) how the information obtained would be used when GIB was determining whether to establish a business relationship with the proposed respondent.

4.72. In 2014, GIB started to use Wolfsberg Questionnaires in place of the risk assessment forms. The Wolfsberg Group produced the Wolfsberg Questionnaire to provide an overview of a financial institution's anti-money laundering policies and practices. It consists of a series of questions with "*Yes*" / "*No*" responses across categories including "*general AML policies, practices and procedures*", "*risk assessment*", "*know your customer, due diligence and enhanced due diligence*", "*reportable transactions and prevention and detection of transactions with illegally obtained funds*", "*transaction monitoring*", and "*AML training*". In June 2011, the Authority had published guidance 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 "Authority's June 2011 Report") which specifically criticised an "*over-reliance on [Wolfsberg Questionnaires] which gives only simple "yes" or "no" answers to basic AML questions*" without using it in conjunction with other forms of assessment. The Authority's Report dated June 2011 marked this activity as poor practice for not seeking "*more substantive, narrative information about respondents' AML controls*". This Report further stated that this made it "*difficult*

for […] banks to make any qualitative assessment of their respondents' AML frameworks".

4.73. In practice, GIB took a blanket approach and classified risk by "*customer type*". Subsequently, irrespective of respondent-specific risks, GIB categorised its correspondent banking business and therefore all respondents as high risk. GIB did not differentiate between respondents within this category despite some potentially posing more of a risk than others due, for example, to the involvement of PEPs in their business, or their own correspondent banking relationships or by virtue of their geographical location. The failure to differentiate suggests GIB's approach was not sufficiently risk-sensitive.

4.74. By applying a "*one size fits all*" approach to due diligence with no assessment of the risks of doing business with respondents located in higher risk countries and thereby taking a blanket approach to categorising risk, GIB failed to incorporate good practice within its business, such as undertaking:

(1) Regular assessments of correspondent banking risks taking into account various money laundering risk factors such as respondents' countries and their AML regimes; ownership / management structure including the possible impact / influence that ultimate beneficial owners with political connections may have; products / operations; transaction volumes; market segments; the quality of the respondent's AML systems and controls and any adverse information known about the respondent;

(2) More robust monitoring of respondents identified as presenting a higher risk;

(3) Risk scores that drive the frequency of relationship reviews; and

(4) Taking into consideration publicly available information from national government bodies and non-governmental organisations and other credible sources.

4.75. Although GIB categorised all its respondents as high risk, it did not consistently record the risk rating on the respondent's customer file or in its internal banking systems. During the Relevant Period, GIB established correspondent banking relationships with 14 respondents. The risk rating of 11 of the 14 respondents (who were onboarded between 2012 and 2014) was not recorded on their customer file or on GIB's systems until May 2015.

4.76. GIB's failure to record respondents' risk rating meant there was a risk that staff would not perform due diligence and ongoing monitoring on these respondents in accordance with GIB's assessment of their risk, leading to the risk of money laundering going undetected.

Fragmented nature of GIB's policies and procedures

4.77. Throughout the Relevant Period, to gather all the information they needed to perform their job, GIB's staff were required to successfully navigate a voluminous and interwoven set of policies and procedures, the complexity of which meant they were not effectively communicated internally. These policies and procedures were insufficiently cross referenced and sign-posted to alert staff that information in any single policy or procedures might be incomplete. For example:

(1) Whilst the Fraud and Money Laundering Policy was effective until at least the end of the Relevant Period, GIB's Board approved a separate Anti-Financial Crime Policy in October 2016. The Anti-Financial Crime Policy did not reference the Fraud and Money Laundering Policy thus creating a risk that staff would be confused when trying to determine which policy to follow. The Fraud and Money Laundering Policy refers to the need for staff to conduct EDD for high-risk customers including respondents but does not specify what this means in practice. Within the same policy there is a discrete section specific to "*Ghanaian Banks*", detailing that relationship managers in Ghana, will meet respondents at least annually and confirm that they have a money laundering policy in place, that it is being implemented, they will carry out a risk assessment of the correspondent banking relationship and that the respondent itself audits compliance. This contrasts with the Anti-Financial Crime Policy that includes a KYC programme section which lists GIB's "*safeguards and monitoring processes*" specific to its correspondent banking business. While detailing seven high-level safeguards, it includes no differentiation between Ghanaian banks and other non-EEA banks, does not reference the relationship managers in Ghana or the checks performed over the Ghanaian banks on an annual basis. GIB failed to ensure that staff working from either document would be aware of the necessity to also refer to the other.

(2) Each version of the Fraud and Money Laundering Policy in use during the Relevant Period included a requirement for each department to maintain an "*operations manual*". There was, however, no list of the departments, their

respective manuals, nor the role of each department in the onboarding and ongoing monitoring of respondents.

(3) GIB's Retail Banking team onboarded all new customers, including respondents, and had its own operations manual: the Retail Banking Manual. One of the purposes of the Retail Banking Manual was to assist staff with the opening of new customer accounts. Aside from alerting staff to the need to complete a checklist appended to the Money Laundering Reporting Manual, the Retail Banking Manual did not set out the EDD that needed to be undertaken when onboarding a respondent. As detailed in paragraphs 4.31 to 4.34 above, the EDD requirements were instead set out to varying degrees in versions of the Money Laundering Reporting Manual in use during the Relevant Period. The Retail Banking Manual however, did not reference that EDD requirements could be found in the Money Laundering Report Manual, and the Money Laundering Reporting Manual did not cross-refer to the Retail Banking Manual either. Both manuals remained effective concurrently until at least the end of the Relevant Period.

(4) In November 2016, GIB introduced a KYC Procedures – Know Your Customer Manual (KYC Policy Manual). The KYC Policy Manual did not reference the Retail Banking Manual or the Money Laundering Reporting Manual and therefore it would not have been clear to staff if it was to be used instead of or in addition to those manuals already in use.

4.78. The fragmented nature of GIB's policies and procedures and the fact that they were not appropriately communicated internally increased the risk that staff, when carrying out their roles, would not have the information available that they needed to onboard and carry out on-going monitoring of respondents in alignment with the rules, regulations and guidance to which GIB was required to adhere. The fact that these policies and procedures were not appropriate or sufficiently risk-sensitive meant that there was a risk they would not detect money laundering activity.

Training

4.79. GIB failed to establish and maintain an appropriate and risk-sensitive training process relating to the internal communication of its policies and procedures to staff.

E-learning

4.80. GIB offered various AML e-learning training courses via external providers, either to all staff or limited to certain employees throughout the Relevant Period, except during 2014 when no e-learning took place. When made available to all staff, the training was generally limited to off-the-shelf e-learning modules that were not specific to GIB, its business, systems or processes. Modifications GIB made to the e-learning were limited to inserting aspects of its policies and procedures. For the reasons stated in paragraphs 4.17 to 4.78, GIB's policies and procedures were not appropriate and sufficiently risk sensitive meaning that GIB amending generic e-learning in this way would not have addressed the AML risks specific to its business:

(1) In 2012, the AML e-learning offered by GIB to all staff was limited to generic courses concerning bribery and corruption and combating money laundering and terrorist financing.

(2) GIB offered the same generic e-learning to all staff in 2013, but limited availability to a single day in May. Later the same year and into early 2014, training titled, "*Ghana Bank Anti-money Laundering Training*" was offered to all staff. The content of this course is not known.

(3) In 2014, GIB did not offer AML e-learning to staff.

(4) GIB resumed its e-learning provision in 2015, offering a broad fraud prevention course to all staff. However, while it also provided a number of AML training courses such as anti-bribery, economic sanctions, financial crime prevention and money laundering prevention, none were particular to the specific needs of GIB's correspondent banking business and access was limited to a subgroup of only nine individuals. Two further AML courses were offered in the year to senior management and staff in specific business areas.

(5) The same e-learning courses were offered in 2016 to all staff. However, despite being assigned for completion by GIB, 20% of staff did not undertake relevant modules.

Other training

4.81. In addition to the e-learning offered as set out above, throughout the Relevant Period, certain members of GIB's compliance team and/or senior management

received larger amounts of AML training. GIB thereby failed to provide training that was both directed to the AML requirements of GIB's correspondent banking business *and* available to all the staff GIB relied on to prevent and mitigate its correspondent banking AML risks from occurring.

4.82. GIB's process for offering broader staff training beyond e-learning was reliant on a small group of employees. While their employment responsibilities included identifying, planning and managing certain training, GIB's ad-hoc and reactive approach was dependent on the employees, specialists in their (non-training) area, attending external training before themselves then sharing it with other employees as they deemed necessary. They also developed and offered training in response to triggers such as FCA publications. While this system was in place from the commencement of the Relevant Period, only in 2015 and 2016 did this include GIB specific AML training to whole departments or all staff.

4.83. Examples of the training the individuals offered to whole departments and all staff included:

(1) May 2015: AML and CTF awareness training to three departments;

(2) June 2015: AML & CDD workshops to two departments and AML training to all staff; and

(3) August 2016: Sanctions refresher training to all staff.

4.84. GIB's training process failed to communicate to staff how to navigate its fragmented, confusing and overlapping policies and procedures. Further, the training that GIB had in place for much of the Relevant Period, was either (1) not particular to the AML risks specific to its business, (2) a one-off training event (in late 2013), or, (3) from 2015, available to only a small number of employees. At no point during the Relevant Period did GIB provide training that was both directed to the AML requirements of GIB's correspondent banking business *and* available to all the staff GIB relied on to prevent and mitigate its correspondent banking AML risks from occurring. GIB's failures in this regard, when accompanied by a lack of practical guidance relevant to its correspondent banking business (see paragraphs 4.17 to 4.78), increased the likelihood that staff would not understand what they needed to do to onboard a respondent correctly, or how to perform monitoring on an on-going basis. This further increased the risk of GIB not satisfying its AML obligations.

Deficiencies in due diligence

4.85. During the Relevant Period, GIB commenced correspondent banking relationships with 14 new respondents, all of which were based in non-EEA countries. As a result of GIB's failure to establish an appropriate procedure which explained to staff how they should conduct due diligence on proposed respondents, there were deficiencies in the due diligence GIB obtained in respect of all 14 respondents.

Purpose and intended nature of business

4.86. To identify transactions or activity that may be suspicious, a correspondent is required to understand fully the nature of its respondents' business. This includes ensuring it is aware of its respondents' expected account activity, including anticipated transaction volumes and values.

4.87. GIB failed to ensure that it collected sufficient information regarding the purpose and nature of the respondents' businesses. For example, GIB did not always obtain information regarding the type of business a respondent was engaged in or the type of market and customers the respondent served. Further, GIB did not always obtain information regarding the respondent's anticipated transaction volumes. In the absence of this information, GIB was unable to adequately assess the risks associated with each business relationship and its ability to identify unusual transactions would have been frustrated. This failing impeded GIB's ability to manage its money laundering and terrorist financing risks effectively, and to establish a basis for monitoring customer activity and transactions.

Determining from publicly available information the reputation of the respondent and the quality of its supervision

4.88. As stated in paragraph 4.14(2) above, correspondents are under an obligation to determine from publicly available information the reputation of a respondent. One of the ways in which a correspondent can do this is by performing an adverse media check against the respondent, its directors and beneficial owners.

4.89. In respect of the 14 respondents with whom it established a correspondent banking relationship during the Relevant Period, GIB failed to perform adverse media checks in relation to 11 of them.

4.90. In one example, the Authority noted that GIB established a new business relationship with a respondent in 2014. Allegations of bribery had been made against the respondent's directors/beneficial owners in 2013. As GIB did not

perform any adverse media checks on the respondent, its directors or beneficial owners, it was unaware of the allegations, and proceeded with the onboarding process unaware of a readily identifiable risk.

4.91. In respect of the remaining 3 respondents, GIB performed adverse media checks either several months before or after the business relationship was established. By performing adverse media checks several months before onboarding, GIB risked relying upon out-of-date information. By failing to perform adverse media checks, or by performing such checks after a respondent had already been onboarded, GIB failed to take steps to determine the reputation of the respondents concerned at the beginning of the relationship, or throughout.

4.92. Correspondents must also determine the quality of a respondent's supervision. Correspondents can do this by, for example, consulting FATF's Mutual Evaluation Reports and, relevant to GIB's activities in West Africa, GIABA's public statements. FATF's reports focus on the supervision provided by the regulator in a respondent's jurisdiction and GIABA's public statements often comment upon the AML/CTF weaknesses in a respondent's jurisdiction. Inherently, some jurisdictions, such as many members of FATF, have more robust regulatory environments and should be lower risk. Conversely, other jurisdictions are recognised internationally as having inadequate anti-money laundering standards, insufficient regulatory supervision and/or presenting greater risk of financial crime.

4.93. In a section titled, "*Assessing overseas AML regimes*", in the Authority's June 2011 Report, the guidance explains that banks should consider the primary regulatory body responsible for overseeing or supervising the respondent and the quality of its supervision. This important part of the due diligence process may alert firms to previous criminal or regulatory action against respondents. The guidance then describes examples of good practice that includes firms:

(1) Undertaking detailed discussions with the local regulator about the AML framework.

(2) Meeting the local regulator and taking additional steps in order to make a better assessment of a country's AML regime, such as considering the AML regime; fines; censures of particular banks; level of AML compliance of banks; the main money laundering risks that are faced and how banks are controlling those risks; audit; and training on AML compliance.

(3) Making a proper assessment of information obtained and following up where issues have been identified.

4.94. In February 2015, a third-party contractor to GIB issued a draft report to the bank's management that assessed GIB's process for the 9 respondent banks it onboarded during 2014.

4.95. For 8 of the 9 respondents, GIB gathered no information about the quality of supervision of its respondents. In the case of 1 respondent, GIB considered its banking licence, an approval letter from the respondent's central bank and a fine that had been issued for a breach of cash reserve. In none of its onboarding processes did GIB consider the FATF or GIABA assessments for the respective respondents' country.

4.96. GIB did not therefore take appropriate steps to determine the quality of the supervision of any of the 9 respondent banks it onboarded during 2014. GIB's failure to determine the quality of supervision meant it exposed itself to unknowingly onboarding respondents based in countries where there was no AML regime/regulatory supervision or where the AML regime/regulatory supervision was so poor as to have had little effect. In such circumstances, the risk that money laundering could occur would increase and would potentially have been insufficiently considered and mitigated.

Assessment of the respondent's AML controls

4.97. Due to the nature of the correspondent banking relationship, the correspondent is reliant on the quality of the respondent's AML controls. A correspondent is therefore required to carry out an assessment of the quality of those controls, to include establishing whether the controls meet internationally recognised standards. If the respondent is not adequately regulated for AML purposes or required to verify the identity of its customers, the JMLSG Guidance states that the correspondent is required to undertake EDD to obtain, and most importantly assess the effectiveness of, the respondent's AML controls.

4.98. GIB failed to evidence that it received or assessed the AML controls of 12 of the 14 respondents that it onboarded during the Relevant Period, prior to onboarding them.

4.99. Where GIB evidenced its assessment of its respondents' AML controls, it exhibited an inadequate, "*tick-box*" approach, lacking any narrative, commentary, feedback points such as sections that needed more detail, identification of weakness or

other indication it had sufficiently considered these important documents. By not receiving and considering narrative information about respondents' AML controls, GIB could not make any qualitative assessment of its respondents' AML frameworks.

4.100. By failing to undertake an assessment of the quality of the respondents' AML controls, GIB could not determine and understand the risks each respondent posed.

Senior management approval

4.101. To mitigate the possibility of taking on respondent relationships that present an unacceptable level of risk, correspondents must obtain senior management approval before establishing new business relationships.

4.102. GIB consistently failed to obtain senior management approval before establishing a new business relationship, with 3 of the 14 respondents receiving no management sign off at all. GIB was also unable to identify the individual senior manager who had purportedly provided approval for the onboarding of a further 6 respondents as the signature on the paperwork was either illegible or unidentifiable. In those cases, therefore, it was not possible to determine whether a member of GIB's senior management team had in fact provided the required approval.

4.103. In 1 further instance, while approval was obtained, this was on the day following GIB's completion of the respondent's onboarding. In another instance, approval was conditional on a reference being obtained that was not subsequently recorded on the onboarding file. The respondent was nevertheless onboarded.

Document the responsibilities of the correspondent and respondent

4.104. The ML Regulations at Regulation 14(3)(e) requires a correspondent to "*document the respective responsibilities of the respondent and correspondent*".

4.105. Until GIB considered its practices following the Authority's publication of the Turkish Bank (UK) Ltd Decision Notice in July 2012 and produced a report which noted its failure to document the respective responsibilities of the correspondent and respondent in a correspondent banking relationship, GIB did not have a requirement in place for staff to undertake this action as part of its onboarding process.

4.106. Subsequently, from September 2012, GIB's Money Laundering Reporting Manual included the requirement to document such responsibilities, however, this merely reproduced the ML Regulations, as specified above in paragraph 4.34 and did not provide staff with practical, firm-specific guidance.

4.107. Even though GIB identified its failure to include the requirement and took steps to amend its policy, albeit, at a high level, it continued not to document the respective responsibilities of the respondent and GIB, as correspondent, until at least 2016. This affected at least 12 of the 14 respondents onboarded during the Relevant Period.

Sanctions screening at onboarding

4.108. GIB's Money Laundering Reporting Manuals included a restriction which stated that GIB did not do business with any person or entity on the Consolidated List. Further, following the implementation of sanctions screening software in May 2012, GIB was to screen all new customers and the directors and beneficial owners of corporate customers using this facility. Prior to the sanctions screening software being implemented, onboarding staff were expected to undertake manual searches.

4.109. Of the 14 respondents with whom GIB established a business relationship during the Relevant Period, GIB failed to perform sanctions screening in relation to 4 of them at the time they were onboarded. Of the remaining 10 respondents, GIB either performed the sanctions screening weeks before (2 respondents) or after the respondents were onboarded (5 respondents).

4.110. The failure to perform sanctions screening prior to onboarding, or at all, meant there was a risk that GIB could breach government sanctions, as well as its own procedures by providing services to these respondents. Further, where undertaking screening prior to onboarding but not in a timely manner, GIB risked relying on out-of-date information.

4.111. GIB's failure to establish and communicate an appropriate procedure which explained to staff how to conduct due diligence on proposed respondents led to the EDD failings identified in paragraphs 4.85 to 4.110 above. These failings meant that GIB established business relationships with respondents in circumstances where it did not fully understand the money laundering risks each respondent posed.

Deficiencies in ongoing monitoring

4.112. To help mitigate the money laundering risks arising from correspondent banking activities, GIB was under an obligation to conduct ongoing monitoring over its respondents; those with whom it established business relationships both prior to and during the Relevant Period.

Customer documents, data and information

4.113. Firms are under an obligation to keep documents, data or information obtained for the purpose of applying customer due diligence measures up to date. This helps to ensure that accounts continue to be used in line with agreements made and that risk categorisations remain valid. Examples of enhanced monitoring might include, but are not limited to, more senior involvement in resolving transaction alerts and lower transaction monitoring alert thresholds. More generally, firms should proactively follow up gaps in, and update, CDD during the course of a relationship.

4.114. On 16 February 2012, FATF issued a Public Statement whereby it added Ghana to its public list of "*jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies*".

4.115. Following the FATF's Public Statement, in March 2012, GIB internally agreed the following actions:

(1) Advising relevant GIB departments that Ghana had been "blacklisted".

(2) Sending letters to Ghanaian respondents "*asking for their updated money laundering policies and manuals […] plus information on the senior management of their firms*".

(3) Sending letters "*to corporates and parastatals for an update of their current directors, shareholding structures and authorised signatories*".

(4) Monitoring transactions with Ghana more closely.

4.116. In accordance with the above, and following publication of the Turkish Bank (UK) Ltd Decision Notice, GIB issued AML questionnaires for respondents to complete and return for GIB to update its due diligence accordingly.

4.117. GIB compiled a spreadsheet which set out the dates when the AML questionnaires had been sent to and received from respondents. This showed that GIB had been slow to obtain the questionnaires from respondents. For example, in April 2012 GIB sent out questionnaires to 12 respondents. In 1 case, GIB did not obtain the questionnaire from the respondent until October 2012, a delay of almost 6 months, and in another case, the questionnaire was not obtained until almost 10 months later, in February 2013. Questionnaires were also sent out to 20 respondents in September 2012. In 2 cases, GIB did not obtain the questionnaires from respondents until December 2012, a delay of over 3 months, and in another case, the questionnaire was not obtained until 5 months later, in February 2013.

4.118. In March 2013, GIB arranged to visit 10 of the respondents to chase and assist them to complete the questionnaires. GIB reported that it obtained a questionnaire from the final respondent by 17 April 2013. In some instances, important items in the questionnaire concerning the respondents' anticipated transaction volumes and values, AML controls and client reputation were not answered. Without this information, GIB's ability to identify and adequately assess the risks posed by each respondent was limited as it would have been unable to establish a basis for monitoring customer activity and transactions.

Failure to terminate relationships

4.119. In circumstances where respondents fail to provide satisfactory answers to reasonable questions regarding their transactions or activities, banks should consider terminating correspondent banking relationships and also consider their obligation to report suspicious activity.

4.120. Whilst GIB knew the respondents took extended periods of time to return the AML questionnaires, it did not place any restrictions on the respondents' accounts in the meantime. This was despite that in January 2013, GIB decided that if respondents "*persisted to ignore our requests for AML Policies and other due diligence requirements then we should give notice that we would not be able to do further business with them".* Although GIB agreed it would give notice to respondents who continued to ignore its requests for AML policies and other due diligence, it failed to do so and took no such action. GIB not taking action to cease transactions or terminate relationships with respondents who failed to provide requested information meant that the CDD and EDD GIB held relating to its respondents became increasingly out of date. This further hampered GIB's ability to identify and report unusual or suspicious transactions or activities.

GIB's failures in relation to ongoing monitoring

4.121. As stated in paragraph 4.51 above, at the start of the Relevant Period, whilst GIB's Money Laundering Reporting Manual encouraged staff to revisit and update information whenever a customer was formally interviewed, opened a new account or when new information was received, this was specific to particular customer types, such as personal and corporate customers and was not required of its correspondent banking business. Further, it did not state that periodic reviews were to take place in accordance with the risk rating assigned to each customer. This failing was out of alignment with the industry standard at the time, where relationships considered to be high-risk were reviewed at least annually.

4.122. In September 2012, following publication of the Turkish Bank (UK) Ltd Decision Notice, GIB updated its Money Laundering Reporting Manual to include a requirement that on an annual basis staff needed to review and update the information GIB had collected from its respondents as high-risk customers during the customer acceptance and due diligence processes.

4.123. Despite this, GIB did not undertake full periodic reviews of the information it held in relation to all respondents on an annual basis. When GIB provided evidence of the sort consistent with a periodic review being started, it was irregular and insufficient. GIB routinely failed to obtain the evidence it would have needed to have appropriately scrutinised transactions using a risk-based approach to ensure that they were in keeping with GIB's recorded knowledge of the customer, including their activities and risk profile.

(1) In one instance, a respondent with whom GIB had established a business relationship in 2006 ceased to trade in 2011 but did not inform GIB and GIB failed to notice. No further activity took place on the respondent's accounts from that point but contrary to industry guidelines, GIB failed to mark the account as dormant or investigate further. In fact, GIB did not attempt to perform a periodic review in respect of this respondent until March 2015. When the respondent did not reply, GIB performed searches in June 2016 and identified that the respondent had ceased to trade some 5 years earlier.

(2) A further 2 respondents, both of whom were onboarded prior to January 2012, were also not contacted by GIB for the purposes of updating due diligence until March 2015.

4.124. As GIB itself recognised, the principal reason for terminating dormant or non-responsive relationships was to guard against the risk of fraud, including money laundering, which, if established, could go undetected for extended periods.

GIB's remediation project

4.125. Following receipt of the December 2014 audit report prepared by the Internal Auditor, which identified the lack of a process to perform periodic file reviews (see paragraph 4.57 above), GIB implemented a remediation project. As part of this project, in May 2015 GIB reviewed all of its respondent files before then contacting respondents to request updated KYC information. The respondent file review was inadequate as, despite the respondents being high risk and necessitating EDD, aside from considering whether it held its respondents' AML policies on file, GIB failed to take into consideration any of the Regulation 14 EDD requirements, limiting its analysis to CDD which was not commensurate with or sufficient to mitigate the risk posed by correspondent banking. For example, GIB failed to consider if it held information about expected transaction volumes, the reputation of the respondent, the quality of its supervision or if respective responsibilities had been documented.

4.126. Of the 46 files assessed, the Authority concludes that GIB had failed to obtain the AML policies of 15 of its respondents and that GIB had either not performed periodic reviews for those respondents adequately or not performed them at all.

4.127. On or around 1 October 2015, and over 4 months after GIB had performed the file reviews, it sent letters to respondents to request updated KYC information. Where respondents did not reply, GIB only repeated their request 4 months later. In 1 instance where the respondent still did not reply, GIB did not then repeat its request until June 2016, more than a year after conducting the most recent file review exercise.

4.128. The progress of the remediation project remained slow overall. By April 2016, GIB had received incomplete responses from 33 respondents and was awaiting documents from a further 13. By July 2016, GIB had still not received complete responses from 15 respondents. GIB considered all but one respondent file fully remediated by November 2016, some 18 months after the remediation project had started.

4.129. The Authority considers that GIB could not have sufficiently remediated the respondents' files in 2015/16. As stated in paragraphs 4.125 to 4.128 above, the

file review process did not take into account the Regulation 14 requirements so any missing or out of date EDD would not have been identified. Consequently, GIB's letters to respondents would not have requested all the information and documentation needed to remediate the files fully.

4.130. Following the Authority's visit to GIB in December 2016, a skilled person was appointed under section 166 of the Financial Services and Markets Act 2000. GIB continues to work with the Authority and the skilled person to improve its financial crime controls and remediate its respondent files.

Failure to determine respondents' reputation and carry out sanctions screening

4.131. GIB also did not routinely perform adverse media checks or sanctions screening on respondents as part of periodic reviews. GIB also did not generally perform such reviews in response to trigger events. Instances where GIB failed to undertake reviews of its respondents included where it had filed internal suspicious activity reports and when it had been advised by business associates that they had opened investigations into customers they had in common with GIB.

4.132. Examples where GIB failed to perform sanctions checking as part of periodic reviews include:

(1) GIB onboarded respondent A prior to commencement of the Relevant Period at which point it did not perform sanctions checks. During the Relevant Period, GIB failed to conduct sanctions checks as part of its periodic review until 2015.

(2) GIB onboarded respondent B in June 2012, failing to perform sanctions checks. GIB then failed to conduct sanctions checks as part of periodic reviews until May 2015.

4.133. The Authority considers that the failure to implement a formal KYC annual review procedure directly impacted upon GIB's ability to keep respondents' documents, data and information up to date. Although GIB made some attempts to meet its ongoing monitoring obligations, the failures referred to in paragraphs 4.112 to 4.132(2) above meant that GIB was not kept adequately informed about the money laundering risks each respondent posed. This increased the risk that GIB could be used for the purposes of money laundering, terrorist financing or sanctions evasion.

Scrutiny of transactions undertaken

4.134. Firms are under an obligation to scrutinise customer transactions to ensure that they are consistent with the firm's knowledge of the customer (including where necessary, the source of funds), its business and risk profile.

4.135. GIB produced daily reports which listed all transactions from the previous day which exceeded the sum of £20,000. These reports were generated for all customers, irrespective of their risk classification and thus included respondents. The reports were created by pulling data from GIB's banking system and were manually reviewed by senior management. GIB also produced a daily report of the single highest value transaction of each of its respondents for a manual review.

4.136. When using a threshold-based system for transaction monitoring, firms should consider the risk profiles of their customers and set the thresholds accordingly. The £20,000 threshold used by GIB was a "*one size fits all*" set by senior management and did not take into account the risk profiles of its customers.

4.137. In June 2013, GIB implemented software which could be used to produce reports which identified transactions by value for its high-risk customers on a daily and monthly basis. The reports were downloaded into spreadsheet format and could be sorted and filtered before being manually reviewed. Although these reports could be analysed so that transactions with a value of less than £20,000 could be reviewed, which would enable GIB to identify high volumes of lower value transactions that were suspicious when aggregated, there was no formal procedure in place which instructed staff when or how to do this. For example, GIB did not communicate to its staff the need for them to prioritise higher risk respondents and transactions for review.

4.138. Until September 2015, a single GIB employee also performed quarterly checks over all high-risk customer transactions, irrespective of value, by manually reviewing the customer's monthly statements. Whilst they noted that a quarterly check had been performed across GIB's respondent customers, they made no record of the specific transactions that had been reviewed or their assessment of them. GIB provided no guidance for the individual to follow. The individual was themselves reliant on GIB's transaction processors preventing unusual transactions from taking place. GIB provided no instruction in its various manuals for how staff should undertake such checks when processing respondents' transactions.

4.139. To scrutinise the transactions listed in the above reports sufficiently, GIB needed to fully understand the nature of a respondent's business and the volume and value of anticipated transactions for each respondent. This information would have assisted GIB to then identify if any of the transactions listed in the reports looked unusual or out of character. GIB routinely failed to obtain such information from respondents. Of the 48 respondents onboarded prior to 2016, GIB failed to obtain details of the anticipated transactions of 34 of them throughout the Relevant Period. For a further 12 respondents, GIB failed to obtain these details more than once throughout the entirety of the Relevant Period. For example:

(1) A respondent, onboarded prior to the start of the Relevant Period, was not contacted by GIB for the purposes of updating due diligence until March 2015. Although updated documentation was requested at that stage, the respondent was not asked to provide, nor did it provide information regarding the nature of its business or the volume and value of anticipated transactions. GIB closed the respondent's accounts in November 2015; and

(2) GIB failed to obtain information from a respondent about the volume and value of anticipated transactions at the time the respondent was onboarded in 2012. When GIB submitted requests for updated due diligence later during the Relevant Period, it again failed to ensure that the respondent provided the anticipated transaction information.

4.140. GIB's failure to obtain this information meant there was a risk that it would be unable to distinguish suspicious from routine transactions, and therefore unable to identify and report suspicious activity.

5. FAILINGS

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

Deficiencies in policies and procedures

5.2. On the basis of the facts and matters set out in paragraphs 4.17 to 4.78, GIB breached ML Regulation 20(1)(a) and (e) of the ML Regulations, by failing to establish and maintain appropriate and sufficiently risk-sensitive policies and procedures relating to customer due diligence, ongoing monitoring, and risk assessment and management for correspondent banking relationships. It further breached ML Regulation 20(1)(f) by failing to have in place appropriate processes for internal communication of such policies and procedures.

5.3. GIB failed to establish and maintain appropriate and risk-sensitive policies and procedures relating to customer due diligence, ongoing monitoring and risk management that were sufficient to counter the risk of money laundering. Those policies and procedures which it did have in place were inappropriate because they lacked key information without which it was impossible for GIB staff to conduct appropriate and effective due diligence. For example, its Fraud and Money Laundering Policy did not refer to the different risk classifications in place for customers or the circumstances in which EDD needed to be undertaken until April 2013 and then did not include a requirement to undertake periodic reviews, or set out the frequency of those reviews, until April 2015.

5.4. In particular, GIB failed to establish appropriate and risk-sensitive procedures for conducting due diligence on proposed respondents from non-EEA countries. Again, those policies and procedures which existed did not sufficiently set out what needed to be done to counter the risk of money laundering effectively. Examples of this include the following:

(1) GIB's Retail Banking Manual failed to set out the specific EDD requirements that needed to be met when onboarding a respondent. These requirements were also not included in the version of the Money Laundering Reporting Manual in use at the start of the Relevant Period.

(2) Whilst EDD requirements were listed at a high level in the Money Laundering Reporting Manual from September 2012 onwards, GIB failed to provide staff with any guidance regarding how the EDD should be undertaken in practice. Checklists appended to the Money Laundering Reporting Manual and which the Retail Banking Manual instructed staff to complete were inappropriate as they were not specific to the onboarding of respondents.

(3) Whilst GIB introduced respondent specific checklists from 2015 onwards, these failed to list all the information that staff needed to obtain and the checks and searches they needed to perform.

(4) GIB also failed to provide guidance regarding how staff should perform reputational checks on respondents' owners, managers and business and how potential sanctions screening matches should be investigated.

5.5. GIB failed to establish and maintain appropriate and risk-sensitive policies and procedures relating to risk management. The risk assessment form GIB introduced in September 2012 was not accompanied by guidance on how staff

should complete it or a methodology for determining the resulting risk classification. It was therefore not clear what level of detail was required when completing the form, how much weight should be placed on the various information provided, when and in which circumstances to escalate to senior management or how much risk GIB was willing to accept. This failure was compounded by GIB failing to articulate clearly what its risk appetite was in relation to correspondent banking, for example by not producing a correspondent banking risk appetite statement. In 2014, GIB started to use Wolfsberg Questionnaires in place of the risk assessment form. The Authority considers that it was inappropriate for GIB to have relied upon the simple "yes" or "no" answers to the basic AML questions contained in the Wolfsberg Questionnaire without also seeking more substantive, narrative information from a respondent about its AML controls.

5.6. GIB failed to establish appropriate and risk-sensitive procedures for conducting ongoing monitoring on respondents. Again, those policies and procedures which existed did not sufficiently set out what needed to be done to counter the risk of money laundering effectively. Examples of this include the following:

(1) The requirement for staff to update customer information was not included in the correspondent banking section of GIB's Money Laundering Reporting Manual at the start of the Relevant Period. GIB amended this section in September 2012 to state that periodic reviews needed to take place on an annual basis for respondents. GIB failed however, to include any practical information regarding how the periodic reviews should be performed, managed, or tracked. GIB's KYC Policy Manual effective November 2016 failed to include a requirement for staff to update customer due diligence.

(2) At the start of the Relevant Period, GIB's Money Laundering Reporting Manual referred to the general need, irrespective of customer type, for staff to report suspicious transactions. In September 2012 GIB amended the correspondent banking section of the Money Laundering Reporting Manual to require staff to scrutinise respondents' transactions and later, GIB's KYC Policy Manual effective November 2016 referred to the need to undertake transaction monitoring. GIB failed to explain either in the Money Laundering Reporting Manual or KYC Policy Manual how the transaction monitoring should be performed consequently it would not have been clear to staff who was responsible for transaction monitoring, what thresholds were in place

and the factors that needed to be taken into consideration such as linked transactions.

5.7. GIB failed to establish and maintain appropriate policies and procedures relating to the internal communication of its processes to staff around customer due diligence, ongoing monitoring and risk management in that it failed to explain effectively what was required to be done. In addition to the examples referred to in paragraphs 5.4 to 5.6 above:

(1) Towards the end of the Relevant Period, in October 2016, GIB introduced an Anti-Financial Crime Policy which did not reference the Fraud and Money Laundering Policy despite the clear potential for overlap. Whilst the policy included safeguards for GIB's correspondent banking business, these were high level and no guidance was included in the policy to assist staff to interpret them.

(2) GIB's KYC Policy Manual in force from November 2016 included indicative guidelines which set out customer identification requirements. The policy manual did not explain how staff should meet these requirements and failed to reference the Retail Banking Manual and Money Laundering Reporting Manual.

(3) GIB's training process failed to explain to staff how to navigate its fragmented, confusing and overlapping policies and procedures.

5.8. Taken together, these failings demonstrate that GIB did not communicate what was required to conduct effective due diligence, ongoing monitoring or risk assessment to its staff. This was another reason why the policies and procedures GIB had in place were not appropriate or sufficiently risk-sensitive to counter the risk of money laundering activity.

Deficiencies in due diligence

5.9. On the basis of the facts and matters set out in paragraphs 4.87 and 4.113, GIB breached ML Regulation 14(1) and 14(3) of the ML Regulations. GIB did not perform adequate EDD for the 14 respondents it onboarded during the Relevant Period. GIB also failed to perform enhanced ongoing monitoring over all its respondents.

5.10. With regard to the 14 respondents onboarded during the Relevant Period, GIB failed to:

(1) obtain sufficient information about the purpose and intended nature of a respondent's business from all 14 respondents. GIB also failed to obtain anticipated transaction volumes from 6 of the 14 respondents, with the information remaining ambiguous and unchecked in respect of 1 additional respondent;

(2) determine from publicly available information the reputation of a respondent. GIB failed to perform adverse media checks in relation to 11 of the 14 respondents and performed such checks either several months before or after the onboarding of the remaining 3 respondents;

(3) determine from publicly available information the quality of a respondent's supervision. GIB failed to determine the quality of supervision in respect of 8 out of the 9 respondents onboarded in 2014;

(4) adequately assess the respondent's AML controls. GIB failed to evidence that it had received or assessed the AML controls for 12 of the 14 respondents;

(5) consistently obtain senior management approval before establishing a correspondent banking relationship. GIB failed to obtain senior management approval in the case of 3 of the 14 respondents. Sign off was purportedly provided for a further 6 respondents but in circumstances where the signature on the paperwork was either illegible or unidentifiable. In 1 instance, sign off was obtained the day after the respondent was onboarded and in another instance, approval was conditional upon a reference being obtained which was not subsequently recorded on the respondent's file; and

(6) document the respective responsibilities of the respondent and GIB, as correspondent. GIB failed to document the responsibilities in the case of at least 12 of the 14 respondents.

5.11. GIB failed to perform sanctions checks in relation to 4 of the 14 respondents at the time the business relationships were established. GIB also performed sanctions screening weeks before onboarding in the case of 2 respondents and after the respondents had been onboarded in the case of 5 respondents.

5.12. GIB's failure to conduct adequate levels of due diligence meant that correspondent banking relationships were established in circumstances where GIB did not understand and had not fully assessed the money laundering risks each respondent posed.

Deficiencies in ongoing monitoring

5.13. After GIB sent out AML questionnaires for the purposes of updating due diligence in 2012, it was slow to contact respondents who had failed to reply to its AML questionnaires which resulted in unacceptable delays of up to 10 months occurring in updating the material it held. In the intervening period, GIB did not place restrictions on the respondents' accounts. Further, GIB failed to query unanswered questions relating to important items concerning anticipated transactions, AML controls and client reputation. Without this information GIB's ability to identify and appropriately to assess the risks posed by each respondent was limited as it would have been unable to establish a base for monitoring customer activity and transactions.

5.14. GIB failed to undertake full periodic reviews of the information it held in relation to respondents on an annual basis and in accordance with its own requirements as set out in the September 2012 and later versions of the Money Laundering Reporting Manual. GIB routinely failed to obtain the evidence needed to appropriately scrutinise transactions and routinely failed to perform adverse media checks or sanctions screening as part of any periodic review.

5.15. GIB set an arbitrary £20,000 threshold for its daily transaction monitoring reports. This failed to take into account the risk profiles of customers and did not include high volumes of lower value transactions. Although subsequent transaction monitoring reports could be manipulated so that transactions with a lower value could be reviewed, and the quarterly checks of all respondent transactions that GIB performed could in theory capture these, GIB failed to put in place a formal procedure which required staff to monitor lower value transactions.

5.16. Whilst GIB kept a record that quarterly checks for all respondent transactions had taken place, GIB failed to keep a record of the specific transactions reviewed or its assessment of them. The individual responsible for performing the quarterly checks was reliant on GIB's transaction monitoring processors preventing unusual transactions from taking place however, GIB had not provided those staff with instructions regarding the checks they needed to perform when processing respondents' transactions.

5.17. GIB consistently failed to obtain information regarding anticipated transaction activity. Of the 48 respondents onboarded prior to 2016, GIB failed to obtain anticipated transaction details from 34 of them. For a further 12 respondents, GIB failed to obtain these details more than once throughout the Relevant Period. The

Authority considers this failure to be particularly serious as this information would have assisted GIB to identify if any of the transactions listed in the monitoring reports looked unusual or out of character. GIB's failure to obtain information about anticipated account activity meant there was a risk that it would be unable to distinguish suspicious from routine transactions and thereby identify and report suspicious activity.

5.18. These weaknesses in GIB's AML systems and controls, particularly insofar as they related to correspondent banking, resulted in an unacceptable risk that GIB would be used by those seeking to launder money, evade financial sanctions or finance terrorism.

6. SANCTION

6.1. Pursuant to Regulations 2(1), 36(a) and 42(1) of the ML Regulations, the Authority is a designated authority which may impose a penalty on a relevant person for failure to comply with the requirements of the ML Regulations at issue in this Notice.

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

6.3. In deciding whether GIB has failed to comply with the relevant requirements of the ML Regulations, the Authority has considered whether GIB followed the relevant JMLSG Guidance as the JMLSG Guidance meets the requirements set out in Regulation 42(3) of the ML Regulations.

6.4. In accordance with Regulation 42(3) of the ML Regulations, the Authority has considered whether it can be satisfied that GIB 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 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 civil penalty of such amount as 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. Paragraph 19.15.5 of the Enforcement Guide states 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. The Authority's policy for imposing a financial penalty is set out in Chapter 6 of DEPP. DEPP 6.5A sets out the details of the five-step framework that applies in respect of financial penalties imposed on firms.

Step 1: disgorgement

6.9. 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.

6.10. The Authority has not identified any financial benefit that GIB derived directly from its breach.

6.11. Step 1 is therefore £0.

Step 2: the seriousness of the breach

6.12. 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.

6.13. The Authority considers that the revenue generated by GIB is indicative of the harm or potential harm caused by its breach. The Authority has therefore determined a figure based on a percentage of GIB's relevant revenue. GIB's relevant revenue is the revenue derived by GIB during the period of the breach. The period of GIB's breach was from 1 January 2012 to 31 December 2016. The Authority considers GIB's relevant revenue for this period to be £19,312,469.

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

Level 1 – 0%

Level 2 – 5%

Level 3 – 10%

Level 4 – 15%

Level 5 – 20%

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

(1) the breaches 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; and

(2) the breaches created a significant risk that financial crime would be facilitated, occasioned or otherwise occur.

6.16. DEPP 6.5A.2G(12) lists factors likely to be considered "level 1, 2 or 3 factors". Of these, the Authority considers the following factors to be relevant:

(1) little, or no, profits were made or losses avoided as a result of the breach, either directly or indirectly; and

(2) the breach was committed inadvertently.

6.17. Taking all of these factors into account, the Authority considers the seriousness of the breach to be level 4 and so the Step 2 figure is 15% of £19,312,469.

6.18. Step 2 is therefore £2,896,870.40.

Step 3: mitigating and aggravating factors

6.19. 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.

6.20. The Authority considers that the following factors aggravate the breach:

Authority's publications

6.21. The Authority has published guidance on the steps firms can take to reduce their financial crime risk and provided examples of good and bad practice since 2008. 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 within the financial services industry. Before, or during the Relevant Period, the Authority published the following guidance relating to AML controls, which set out good practice examples to assist firms in interpreting the ML Regulations:

(1) in March 2008, the Authority published a report titled "Review of firms' implementation of a risk-based approach to anti-money laundering". In respect of correspondent banking relationships, the report notes that there is a need for the correspondent to review the respondent's ownership and management, any PEP involvement and the respondent's AML controls;

(2) in June 2011, the Authority published 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 Authority's June 2011 Report). The Authority's June 2011 Report notes that if banks fail to implement appropriate controls when accepting correspondent banking relationships, this can give banks with inadequate AML systems and controls access to the international banking system;

(3) in December 2011, the Authority published "Financial Crime: A Guide for Firms". The guide highlights the need to conduct adequate customer due diligence checks, perform ongoing monitoring and carry out enhanced due diligence measures and enhanced ongoing monitoring when handling higher risk situations, including PEPs and correspondent banking relationships;

(4) in November 2014, the Authority published a report titled "How small banks manage money laundering and sanctions risk: Update". This report was issued as a follow up to the Authority's June 2011 Report and provided examples of good practice around money laundering risk assessments, customer due diligence, enhanced due diligence of correspondent banking relationships and enhanced ongoing monitoring; and

(5) in April 2015, the Authority published a report titled "Financial crime: a guide for firms Part 1: A firm's guide to preventing financial crime". This report consolidated FCA guidance on financial crime and provided guidance to firms on steps they could take to reduce their financial crime risk. It set out a series of non-exhaustive self-assessment questions and good and poor practice.

6.22. Accordingly, GIB had access to considerable guidance regarding the regulatory requirements and how to comply with them. GIB should therefore have been aware of the importance of implementing and maintaining robust AML systems and controls.

Authority's Final Notices

6.23. The Authority has published several Notices against firms for AML weaknesses both before and during the Relevant Period, including Habib Bank AG Zurich on 4 May 2012, Turkish Bank (UK) Ltd on 26 July 2012 and Guaranty Trust Bank (UK) Ltd on 8 August 2013. These actions stressed to the industry the Authority's view of firms with AML deficiencies especially in relation to higher risk customers. GIB was therefore aware of the importance of implementing and maintaining robust AML systems and controls.

GIB's remediation project

6.24. Although GIB voluntarily implemented a remediation project (as referenced in paragraphs 4.125 to 4.129 above), it did not take sufficient steps to implement a periodic review procedure in a timely way, or at all, or to remediate its respondent customer files, during the Relevant Period.

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

(1) The Authority recognises that GIB and its senior management agreed to a voluntary business restriction while seeking to remediate its AML breaches.

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

6.27. Step 3 is therefore £3,331,400.96.

Step 4: adjustment for deterrence

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

6.29. The Authority considers that DEPP 6.5A.4G(1)(a) is relevant in this instance and has therefore determined that this is an appropriate case where an adjustment for deterrence is necessary.

6.30. Without an adjustment for deterrence, the financial penalty would be £3,331,400.96 (before settlement discount). The Authority considers that a penalty of this size would not serve as a real credible deterrent to GIB or others. During the Relevant Period GIB considered correspondent banking to be critical to its business and to realising its growth strategy to develop new markets across Africa. On average, during the Relevant Period, income generated from correspondent banking totalled 14% of GIB's total revenue. Given the integral nature of correspondent banking within GIB and the nature of the misconduct, it is necessary for the Authority to increase the penalty to achieve credible deterrence.

6.31. Having taken into account the factors outlined at DEPP 6.5A.4G the Authority considers that a multiplier of 2.5 should be applied at Step 4.

6.32. Step 4 is therefore £8,328,502.41.

Step 5: settlement discount

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

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

6.35. Step 5 is therefore £5,829,951.69.

Penalty

6.36. The Authority has therefore decided to impose a financial penalty (rounded down to the nearest £100) of £5,829,900 (£8,328,500 before 30% (stage 1) discount) on GIB for breaching Regulations 14(1), 14(3) and 20(1) of the ML Regulations.

7. PROCEDURAL MATTERS

7.1. This Decision Notice is given under Regulation 42(7) of the ML Regulations.

7.2. The following information is important.

Decision Maker

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

The Tribunal

7.4. 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, amongst 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.

7.5. 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.

7.6. Further details are available from the Tribunal website: http://www.justice.gov.uk/forms/hmcts/tax-and-chancery-upper-tribunal

7.7. A copy of Form FTC3 must also be sent to Anthony Williams 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

7.8. The financial penalty must be paid in full by GIB to the Authority by no later than 7 July 2022.

If the financial penalty is not paid

7.9. If any or all of the financial penalty is outstanding on 7 July 2022, the Authority may recover the outstanding amount as a debt owed by GIB and due to the Authority.

Access to evidence

7.10. 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) any secondary material which, in the opinion of the Authority, might undermine that decision.

Confidentiality and publicity

7.11. 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).

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

Authority contacts

7.13. For more information concerning this matter generally, contact Anthony Williams at the Authority (direct line: 020 7066 2196).

Mark Steward

Settlement Decision Maker, for and on behalf of the Authority

Edwin Schooling Latter

Settlement Decision Maker, for and on behalf of the Authority

ANNEX A – RELEVANT STATUTORY AND REGULATORY PROVISIONS AND GUIDANCE

The Money Laundering Regulations 2007 were in force from 15 December 2007 to 25 June 2017 inclusive and have been repealed and replaced by the Money Laundering Regulations 2017, which came into force on 26 June 2017, for action commencing after that date. In this Notice, the Authority refers to and has taken action under the Money Laundering Regulations 2007 as the Relevant Period ends on 31 December 2016.

Relevant extracts from the Money Laundering Regulations 2007

Meaning of customer due diligence measures

1. Regulation 5 states:

"Customer due diligence measures" means –

(1) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

(2) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant period is satisfied that he knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangements; and

(3) obtaining information on the purpose and intended nature of the business relationship.

Meaning of beneficial owner

2. Regulation 6 states:

(1) In the case of a body corporate, "beneficial owner" means any individual who –

(2) as respects any body other than a company whose securities are listed on a regulated market, ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25% of the shares or voting rights in the body; or

(3) as respects any body corporate, otherwise exercises control over the management of the body.

3. In the case of a partnership (other than a limited liability partnership), "beneficial owner" means any individual who –

(1) ultimately is entitled to or controls (whether the entitlement or control is direct or indirect) more than a 25% share of the capital or profits of the partnership or more than 25% of the voting rights in the partnership; or

(2) otherwise exercises control over the management of the partnership. […]

Application of customer due diligence measures

4. Regulation 7 states:

(1) Subject to regulations 9, 10, 12, 13, 14, 16(4) and 17, a relevant person must apply customer due diligence measures when he –

a) establishes a business relationship;

b) carries out an occasional transaction;

c) suspects money laundering or terrorist financing;

d) doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

(2) Subject to regulation 16(4), a relevant person must also apply customer due diligence measures at other appropriate times to existing customers on a risk-sensitive basis.

(3) A relevant person must –

a) determine the extent of customer due diligence measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction; and

b) be able to demonstrate to his supervisory authority that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing. […]

Ongoing monitoring

5. 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 and 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

6. 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 and terrorist financing.

(2) Where the customer has not been physically present for identification purposes, a relevant person must take specific and adequate measures to compensate for the higher risk, for example, by applying one or more of the following measures –

a) ensuring that the customer's identity is established by additional documents, data or information;

b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution which is subject to the money laundering directive;

c) ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution.

(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 the 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 –

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

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

(4) A relevant person who proposes to have a business relationship or carry out an occasional transaction with a politically exposed person must –

a) have approval from senior management for establishing the business relationship with that person;

b) take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or occasional transaction; and

c) where the business relationship is entered into, conduct enhanced ongoing monitoring of the relationship.

(5) In paragraph (4), a "politically exposed person" means a person who is –

a) an individual who is or has, at any time in the preceding year, been entrusted with a prominent public function by –

a state other than the United Kingdom;

a Community institution; or

an international body,

including a person who falls in any of the categories listed in paragraph 4(1)(a) of Schedule 2;

b) an immediate family member of a person referred to in sub-paragraph (a), including a person who falls in any of the categories listed in paragraph 4(1)(c) of Schedule 2; or

c) a known close associate of a person referred to in sub-paragraph (a), including a person who falls in either of the categories listed in paragraph 4(1)(d) of Schedule 2.

(6) For the purpose of deciding whether a person is a known close associate of a person referred to in paragraph 5(a), a relevant person need only have regard to information which is in his possession or is publicly known.

Policies and procedures

7. 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;

b) reporting;

c) recording-keeping;

d) internal control;

e) risk assessment and management;

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 – […]

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 of money laundering and terrorist financing of products and transactions which might favour anonymity;

c) to determine whether a customer is a politically exposed person; […]

(5) A credit of financial institution must communicate where relevant the policies and procedures which it establishes and maintains in accordance with this regulation to its branches and subsidiary undertakings which are located outside the United Kingdom.

Relevant extracts from the JMLSG Guidance

8. The JMLSG Guidance provisions set out below are taken from the 2011 version of the guidance. 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 2 Internal Controls

General legal and regulatory obligations

9. Paragraph 2.1 states:

There is a requirement for firms to establish and maintain appropriate and risk-based policies and procedures in order to prevent operations related to money

laundering or terrorist financing. FSA-regulated firms have similar, regulatory obligations under SYSC.

Part I, Chapter 3 Nominated Officer/Money Laundering Reporting Officer (MLRO)

Monitoring effectiveness of money laundering controls

10. Paragraph 3.27 states:

A firm is required to carry out regular assessments of the adequacy of its systems and controls to ensure that they manage the money laundering risk effectively. Oversight of the implementation of the firm's AML/CTF policies and procedures, including the operation of the risk-based approach, is the responsibility of the MLRO, under delegation from senior management. He must therefore ensure that appropriate monitoring processes and procedures across the firm are established and maintained.

Part I, Chapter 5 customer due diligence

Meaning of customer due diligence measures and ongoing monitoring

11. Paragraph 5.1.4 states:

Firms must determine the extent of their CDD measures and ongoing monitoring on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction. They must be able to demonstrate to their supervisory authority that the extent of their CDD measures and monitoring is appropriate in view of the risks of money laundering and terrorist financing.

12. Paragraph 5.1.6 states:

Where the customer is a legal person (such as a company) or a legal arrangement (such as a trust), part of the obligation on firms to identify any beneficial owner of the customer means firms taking measures to understand the ownership and control structure of the customer.

13. Paragraph 5.1.10 states:

The CDD and monitoring obligations on firms under legislation and regulation are designed to make it more difficult for the financial services industry to be used for money laundering or terrorist financing.

14. Paragraph 5.1.11 states:

Firms also need to know who their customers are to guard against fraud, including impersonation fraud, and the risk of committing offences under POCA and the Terrorism Act, relating to money laundering and terrorist financing.

15. Paragraph 5.1.12 states:

Firms therefore need to carry out customer due diligence, and monitoring, for two broad reasons:

> to help the firm, at the time due diligence is carried out, to be reasonably satisfied that customers are who they say they are, to know whether they are acting on behalf of another, and that there is no legal barrier (e.g. government sanctions) to providing them with the product or service requested; and
>
> to enable the firm to assist law enforcement, by providing available information on customers or activities being investigated.

16. Paragraph 5.1.13 states:

It may often be appropriate for the firm to know rather more about the customer than his identity: it will, for example, often need to be aware of the nature of the customer's business in order to assess the extent to which his transactions and activity undertaken with or through the firm is consistent with that business.

Application of CDD measures

17. Paragraph 5.3.1 states:

Applying CDD measures involves several steps. The firm is required to verify the identity of customers and, where appropriate, beneficial owners. Information on the purpose and intended nature of the business relationship must also be obtained.

Enhanced due diligence

18. Paragraph 5.5.1 states:

A firm must apply EDD measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. As part of this, a firm may conclude, under its risk-based approach, that the information it has collected as part of the customer due diligence process (see

section 5.3) is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer, the customer's beneficial owner, where applicable, and the purpose and intended nature of the business relationship.

19. Paragraph 5.5.2 states:

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

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

20. Paragraph 5.5.5 states:

A firm should hold a fuller set of information in respect of those business relationships it assessed as carrying a higher money laundering or terrorist financing risk, or where the customer is seeking a product or service that carries a higher risk of being used for money laundering or terrorist financing purposes.

21. Paragraph 5.5.18 states:

Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to firms as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the customer, of the beneficial owner, into a higher risk category.

22. Paragraph 5.5.25 states:

Firms are required, on a risk-sensitive basis, to:

> have appropriate risk-based procedures to determine whether a customer is a PEP;

obtain appropriate senior management approval for establishing a business relationship with such a customer;

take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction; and

conduct enhanced ongoing monitoring of the business relationship.

Monitoring customer activity

23. Paragraph 5.7.1 states:

Firms must conduct ongoing monitoring of the business relationship with their customers. Ongoing monitoring of a business relationship includes:

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 firm's knowledge of the customer, his business and risk profile;

ensuring that the documents, data or information held by the firm are kept up to date.

24. 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 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.

25. Paragraph 5.7.12 states:

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

Part II, Chapter 16 correspondent banking

Overview of the sector

26. Paragraph 16.1 states:

For the purposes of this guidance, correspondent banking is defined as 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.

27. Paragraph 16.9 states:

Enhanced customer due diligence (see Part I, section 5.5) must be undertaken on respondents (and/or third parties authorised exceptionally to provide instructions to the correspondent e.g. other entities within a respondent group) using a risk-based approach. The following risk indicators should be considered both when initiating a relationship, and on a continuing basis thereafter, to determine the levels of risk-based due diligence that should be undertaken:

> **The respondent's domicile.** The jurisdiction where the respondent is based and/or where its ultimate parent is headquartered may present greater risk (or may mitigate the risk, depending on the circumstances). Certain jurisdictions are recognised internationally as having inadequate anti-money laundering standards, insufficient regulatory supervision, or presenting greater risk for crime, corruption or terrorist financing. Other jurisdictions, however, such as many members of the Financial Action Task Force (FATF), have more robust regulatory environments, representing lower risks. correspondents should review pronouncements from regulatory agencies and international bodies such as the FATF, to evaluate the degree of risk presented by the jurisdiction in which the respondent and/or its parent are based.
>
> **The respondent's ownership and management structures.** The location of owners, their corporate legal form and/or a lack of transparency of the ultimate beneficial ownership are indicative of the risk the respondent presents. Account should be taken of whether the respondent is publicly or privately owned; if publicly held, whether its shares are traded on a recognised market or exchange in a jurisdiction with a satisfactory regulatory regime, or, if privately owned, the identity of any beneficial owners and controllers. Similarly, the location and experience of management may indicate additional concerns, as would unduly frequent management turnover. The involvement of PEPs in the management or ownership of certain respondents may also increase the risk.

The respondent's business and customer base. The type of business the respondent engages in, as well as the type of markets is serves, is indicative of the risk the respondent presents. Involvement in certain business segments that are recognised internationally as particularly vulnerable to money laundering, corruption or terrorist financing, may present additional concern. Consequently, a respondent that derives a substantial part of its business income from higher risk customers may present greater risk. Higher risk customers are those customers that may be involved in activities, or are connected to jurisdictions, that are identified by credible sources as activities or countries being especially susceptible of money laundering/terrorist financing or corruption.

Customer due diligence

28. Paragraph 16.15 states:

The correspondent in assessing the level of due diligence to be carried out in respect of a particular respondent (in addition to the issues raised in paragraph 16.9) must consider:

Regulatory status and history. The primary regulatory body responsible for overseeing or supervising the respondent and the quality of that supervision. If circumstances warrant, a correspondent should also consider publicly available materials to ascertain whether the respondent has been the subject of any criminal case or adverse regulatory action in the recent past.

AML/CTF controls. A correspondent should establish whether the respondent is itself regulated for money laundering/terrorist financing prevention and, if so, whether the respondent is required to verify the identity of its customers and apply other AML/CTF controls to FATF standards/equivalent to those laid down in the money laundering directive. Where this is not the case, additional due diligence should be undertaken to ascertain and assess the effectiveness of the respondent's internal policy on money laundering/terrorist financing prevention and its know your customer and activity monitoring controls and procedures. Where undertaking the due diligence on a branch, subsidiary or affiliate, consideration may be given to the parent having robust group-wide controls, and whether the parent is regulated for money laundering/terrorist financing to FATF standards/equivalent to those laid down in the money laundering directive.

If not, the extent to which the parent's controls meet FATF standards/equivalent to those laid down in the money laundering directive and whether these are communicated and enforced "effectively" throughout its network of international offices, should be ascertained.

Enhanced due diligence

29. Paragraph 16.7 states:

Correspondents are required by Regulation 14(3) of the ML Regulations to subject respondents from non-EEA States to enhanced customer due diligence, but should consider doing so whenever the respondent has been considered to present a greater money laundering/terrorist financing risk. The enhanced due diligence process should involve further consideration of the following elements designed to ensure that the correspondent has secured a greater level of understanding:

Respondent's ownership and management. For all beneficial owners and controllers, the source of wealth and background, including their reputation in the market place, as well as recent material ownership changes (e.g. in the last three years). Similarly, a more detailed understanding of the experience of each member of executive management as well as recent material changes in the executive management structure (e.g. within the last three years).

Respondent's business. Gather sufficient information about the respondent to understand fully the nature of its business. In addition, determine from publicly-available information the reputation of the respondent and the quality of its supervision.

PEP involvement. If a PEP (see Part I, paragraph 5.5.18-5.5.30) appears to have a material interest or management role in a respondent then the correspondent should ensure it has an understanding of that person's role in the respondent.

Respondent's anti-money laundering/terrorist financing controls. An assessment of the quality of the respondent's AML CTF and customer identification controls, including whether these controls meet internationally recognised standards. The extent to which a correspondent should enquire will depend upon the perceived risks. Additionally, the correspondent may wish to speak with representatives of the respondent to obtain comfort that

the respondent's senior management recognise the importance of anti-money laundering/terrorist financing controls.

Document the relationship. Document the respective responsibilities of the respondent and correspondent.

Other monitoring activity

30. Paragraph 16.21 states:

In addition to monitoring account/transaction activity, a correspondent should monitor a respondent for changes in nature and status. As such, information about the respondent collected during the customer acceptance and due diligence processes must be:

Reviewed and updated on a periodic basis. (Periodic review of customers will occur on a risk-assessed basis); or

Reviewed on an ad hoc basis as a result of changes to the customers information identified during normal business practices; or

Reviewed when external factors result in a material change to the risk profile of the customer.

31. Paragraph 16.22 states:

Where such changes are identified, the respondent should be subject to a revised risk assessment, and a revision of their risk categorisation, as appropriate. Where, as a result of the review, the risk categorisation is altered (either up or down) a firm should ensure that the due diligence standards for the respondent's new risk categorisation are complied with, by updating the due diligence already held. In addition, the level of monitoring undertaken should be adjusted to that appropriate for the new risk category.

32. Paragraph 16.24 states:

The firm will need to have a means of assessing that its risk mitigation procedures and controls are working effectively. In particular the firm will need to consider:

Reviewing ways in which different services may be used for ML/TF purposes, and how these ways may change, supported by typologies/law enforcement feedback etc.;

Adequacy of staff training and awareness;

Capturing appropriate management information;

Upward reporting and accountability; and

Effectiveness of liaison with regulatory and law enforcement agencies.