

---

## FINAL NOTICE

---

**To: Guaranty Trust Bank (UK) Limited**

**Reference  
Number: 466611**

**Address: 62 Margaret Street, London W1W 8TF**

**Date: 10 January 2023**

### **1. ACTION**

- 1.1. For the reasons given in this Final Notice, the Financial Conduct Authority (“the Authority”) hereby imposes on Guaranty Trust Bank (UK) Limited (“GT Bank”) a financial penalty of £7,671,800 pursuant to section 206 of the Financial Services and Markets Act 2000 (“the Act”).
- 1.2 GT Bank agreed to resolve this matter at an early stage 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 £10,959,700 on GT Bank.

### **2. SUMMARY OF REASONS**

- 2.1. Fighting financial crime is an issue of international importance and there has been a regime in place for the prevention of money laundering in the UK since 1994.

Regulated firms play a key role in the UK's fight against financial crime and must have in place effective, proportionate and risk-based systems and controls to mitigate the risk of their businesses being used for money laundering or terrorist financing. The importance of firms' systems and controls in preventing financial crime has featured as one of the Authority's priority areas in its Business Plans throughout the relevant period.

- 2.2. Authorised firms are required by the Money Laundering Regulations and by the Authority's rules to put in place policies and procedures to prevent and detect money laundering. These include systems and controls to identify, assess and monitor money laundering risk as well as conducting customer due diligence ("CDD"), enhanced due diligence ("EDD") and ongoing monitoring of both business relationships and transactions to manage the risks identified.
- 2.3. GT Bank should have played its part in the fight against financial crime by ensuring it had in place effective anti-money laundering ("AML") systems and controls. These are required in order to mitigate the risk of individuals and organisations using financial institutions to circumvent restrictions designed to prevent them benefitting from assets obtained by illegal means. Instead, GT Bank failed to ensure compliance with its regulatory obligations in respect of its systems and controls relating to AML during the relevant period.
- 2.4. This is not the first time GT Bank has been disciplined by the Authority for serious weaknesses in its AML systems and controls. By a Final Notice, dated 8 August 2013, GT Bank was fined £525,000 by the Authority for similar failings in relation to its AML systems and controls.<sup>1</sup> The Authority considers this repeated misconduct to be a direct result of the inability of the senior management within GT Bank, over a prolonged period of time, to formulate and implement an effective plan capable of addressing the weaknesses identified within its AML and financial crime systems and controls.
- 2.5. As this behaviour mirrored previous misconduct, the Authority has significantly increased the penalty to be paid by GT Bank.
- 2.6. GT Bank breached Principle 3 (management and control) of the Authority's Principles for Businesses ("the Principles") between 21 October 2014 and 12 July

---

<sup>1</sup> <https://www.fca.org.uk/publication/final-notice/guaranty-trust-bank-uk-ltd.pdf>

2019 ("the relevant period") by failing to take reasonable care to organise and control its AML processes responsibly and effectively, with adequate risk management systems.

2.7. In particular, during the relevant period, GT Bank failed to:

- (1) take appropriate remedial action to rectify the weaknesses in its AML systems and controls – these weaknesses were identified by its Compliance and Internal Audit functions, by the external consultant employed by GT Bank and were also identified and directly flagged to GT Bank by the Authority in 2014 and 2017;
- (2) ensure that remedial work that was required as a result was appropriately performed and monitored, and that it was completed in a timely manner;
- (3) carry out adequate customer risk assessments, often failing to assess and document the money laundering risks posed by customers;
- (4) carry out adequate CDD, as required, when establishing a business relationship with a customer;
- (5) carry out adequate EDD, as required, on higher risk customers;
- (6) establish, verify and evidence the source of funds and source of wealth for higher risk customers;
- (7) conduct adequate ongoing monitoring of customer relationships, as required, to ensure that customer risk assessment and due diligence information was kept up to date and that the activity on customer accounts was consistent with expected activity;
- (8) conduct adequate transaction monitoring of customer accounts, as required;
- (9) ensure that an effective system to improve the quality of transaction monitoring parameters and alerts was implemented;
- (10) ensure relevant staff were provided with appropriate AML training; and

- (11) implement a culture where customer facing teams gave adequate and effective consideration to the money laundering risks posed by prospective and existing customers.
- 2.8. The majority of these failings had a direct bearing on GT Bank’s ability to comply with its regulatory obligations during the relevant period, which included requirements for GT Bank to:
- (1) apply CDD measures when establishing a business relationship or carrying out a transaction for a customer;
  - (2) apply CDD at other appropriate times to existing customers on a risk-sensitive basis;
  - (3) apply scrutiny to transactions undertaken throughout the course of its relationships with customers;
  - (4) keep documents, data or information obtained for the purposes of applying CDD measures up to date;
  - (5) apply EDD measures and enhanced ongoing monitoring in any situation which by its nature may present a higher risk of money laundering or terrorist financing; and
  - (6) establish and maintain appropriate and risk-sensitive policies and procedures relating to the above.
- 2.9. In addition to the breach of Principle 3, GT Bank also breached the following Senior Management Arrangements, Systems and Controls (“SYSC”) rules set out in the Authority’s Handbook: SYSC 6.1.1R and SYSC 6.3.1R (which are listed in the Annex to this Notice).
- 2.10. It is acknowledged by the Authority that, during the relevant period, GT Bank spent considerable time and resource on attempts to remediate customer files to make them compliant with regulatory requirements. However, progress remained slow and for too long standards remained below those required.

2.11. The Authority considers that the failings of GT Bank are particularly serious for the following reasons:

- (1) this is not the first time GT Bank has been disciplined by the Authority for serious weaknesses in its systems and controls as they relate to AML. GT Bank was fined £525,000 by the Authority for similar failings in relation to its AML systems and controls on 8 August 2013;
- (2) GT Bank's AML control framework was reviewed during the relevant period by:
  - a) GT Bank's Compliance and Internal Audit functions;
  - b) the external consultant;
  - c) the Authority; and
  - d) GT Bank's parent entity during the relevant period, Guaranty Trust Bank Plc ("GT Bank Plc"),

All of these reviews identified inadequate systems and controls and, although required remedial action was clearly highlighted, GT Bank took insufficient steps to remediate and, in some cases, decided to cease remediation work before it was completed;

- (3) it provided financial services to a significant number of customers from, or closely linked to, jurisdictions outside of the UK which have been identified by industry recognised sources, such as the Basel AML Index and the Corruption Perceptions Index, as having a higher vulnerability to money laundering and terrorist financing risk and corruption. GT Bank acted as an entry point to the UK financial system for these customers and as a result should have had in place robust systems and controls to mitigate the risk that the UK would be used to launder the proceeds of financial crime or to finance terrorism;
- (4) the failure to remediate clearly identified deficiencies in its AML control framework over a significant period demonstrates that GT Bank did not have in place an appropriate and effective strategy to enable it to meet its

AML responsibilities and obligations and resulted in an increased risk that it could be used to facilitate financial crime; and

- (5) industry compliance with the Money Laundering Regulations and with the Authority's regulatory rules and requirements relating to AML have been key features of the fight against financial crime for over 25 years, and the Authority has issued numerous well-publicised Final Notices against authorised firms in recent years for AML systems and controls weaknesses of which GT Bank was or should have been aware.

2.12. The Authority hereby imposes on GT Bank a financial penalty of £7,671,800.

2.13. For the avoidance of doubt, this Notice makes no criticism of any person other than GT Bank.

### **3. DEFINITIONS**

3.1. The definitions below are used in this Notice:

"2013 Final Notice" means the Final Notice issued by the Authority on 8 August 2013 to GT Bank;

"the 2014 visit" means the visit by the Authority to GT Bank on 21 and 22 October 2014;

"the 2017 visit" means the visit by the Authority to GT Bank between 13 to 15 June 2017;

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

"AML" means anti-money laundering;

"AMLOC" means GT Bank's AML Oversight Committee;

"the Authority" means the Financial Conduct Authority;

"the external consultant" means the external consultant that GT Bank engaged throughout the relevant period to undertake various reviews on its AML systems and controls, policies and procedures, including reviews of its customer files;

"BRCC" means GT Bank's Board Risk and Compliance Committee;

"CDD" means customer due diligence measures as defined in regulation 5 of the MLR 2007 and regulation 28 of the MLR 2017;

"Compliance" means GT Bank's internal Compliance function based in its London office;

"customer facing teams" means the teams within GT Bank's core business lines comprised solely of customer facing staff (i.e. business line Heads of Department and the Relationship Managers within the respective departments) who interacted with GT Bank's potential and existing customers;

"Consolidated List" means the list maintained by HM Treasury and the Office of Financial Sanctions Implementation that sets out the names of sanctioned persons and entities under UN and EU sanctions regimes which have effect in the UK;

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

"EDD" means enhanced customer due diligence measures, applied in circumstances as set out in regulation 14 of the MLR 2007 and regulation 33 of the MLR 2017;

"Financial Crime Team" refers to the various financial crime teams that were in place at GT Bank throughout the relevant period that were responsible for carrying out key AML activities within GT Bank including customer onboarding, transaction monitoring, PEP and sanctions screening and ongoing monitoring. The Financial Crime Team was also responsible for undertaking the Look Back exercise;

"GT Bank" means Guaranty Trust Bank (UK) Limited;

"GT Bank Plc" means Guaranty Trust Bank Plc, the parent company of GT Bank during the relevant period, which was incorporated in Nigeria;

“Handbook” means the Authority’s Handbook of rules and guidance;

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

“Look Back exercise” was a remediation exercise undertaken by GT Bank in 2015 and 2016 with the objective of ensuring that CDD/AML issues with its customers and customer files were identified and rectified. The Look Back exercise was conducted over two phases: (1) a ‘review’ phase which focused on identifying due diligence gaps within customer files and (2) a ‘remediation’ phase which involved requesting necessary due diligence documentation from customers to close identified gaps and updating customer risk assessments;

“MI” means management information;

“Money Laundering Regulations” means the Money Laundering Regulations 2007 (SI 2007/2157) (“the MLR 2007”), which came into force on 15 December 2007, and were superseded for conduct commencing after 26 June 2017 by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI 2017/692) (“the MLR 2017”), as in force from time to time in the relevant period;

“PEP” means a politically exposed person as defined in regulation 14(5) of the MLR 2007 and regulation 35(12) of the MLR 2017;

“Principle” means one of the Authority’s Principles for Businesses;

“relevant period” means 21 October 2014 to 12 July 2019;

“September 2013 review” refers to the review which was undertaken by the external consultant and commenced in September 2013, of GT Bank’s AML policies, procedures, systems and controls;

“September 2014 review” refers to the independent assessment which was undertaken by the external consultant and commenced in September 2014, of GT Bank’s AML policies, procedures, systems and controls and implementation of previous recommendations from the external consultant’s report dated December 2013;



“Six Point Review” means a remediation exercise undertaken by GT Bank in 2014 and 2015 which sought to identify and remediate deficiencies within “Very High” and “High” risk customer files and ensure that information relating to: (i) sanctions; (ii) PEP and adverse media screening; (iii) source of income and source of wealth; (iv) purpose of account; (v) nature of relationship; and (vi) beneficial ownership were properly evidenced;

“Skilled Person” means the skilled person appointed by GT Bank pursuant to the requirement, dated 20 December 2017, imposed by the Authority under section 166 of the Act;

“SYSC” means the part of the Authority’s Handbook entitled “Senior Management Arrangements, Systems and Controls”;

“System A” means the automated transaction monitoring system that GT Bank used to monitor customer transactions up until March 2015;

“System B” means the automated transaction monitoring system that GT Bank implemented in May 2017 as a replacement for its previous automated transaction monitoring system, System A; and

“Tribunal” means the Upper Tribunal (Tax and Chancery Chamber).

## **4. FACTS AND MATTERS**

### **Background**

- 4.1. GT Bank is a wholly owned UK subsidiary of Guaranty Trust Bank Nigeria Limited which is a wholly owned subsidiary of Guaranty Trust Bank Holding Company Plc. During the relevant period, GT Bank was a UK subsidiary of GT Bank Plc, a Nigerian multinational financial services institution that provided a range of banking services across Africa and the United Kingdom. Guaranty Trust Bank Holding Company Plc is (and GT Bank Plc was) a public limited company, listed on both the London and Nigerian stock exchanges.
- 4.2. GT Bank offers a wide range of regulated and unregulated financial products and services in the UK including mortgage lending, trade finance, correspondent banking services to other entities in the GT Bank group, personal banking services

and deposit taking activities. However, its principal focus is on the provision of mortgage products and trade finance to African counterparties, and its stated aim is to be the premier African bank for Africans who are not resident in the UK but have business connections there.

### **Previous action by the Authority and assessments of GT Bank's AML control framework**

#### 2013 Final Notice

4.3. On 8 August 2013, the Authority issued a Final Notice and imposed a financial penalty of £525,000 on GT Bank for breaching Principle 3 between 19 May 2008 and 19 July 2010. In addition to the breach of Principle 3, GT Bank also breached SYSC rule 6.1.1R and SYSC rule 6.3.1R. The failings at GT Bank were serious and systemic and resulted in an unacceptable risk of it handling the proceeds of crime. In particular, the Authority found that, between 19 May 2008 and 19 July 2010, GT Bank did not:

- (1) maintain adequate and risk sensitive systems and controls to identify, assess and manage potential money laundering risks;
- (2) carry out and document adequate CDD and carry out EDD when establishing relationships with higher risk customers; and
- (3) conduct an appropriate level of ongoing monitoring for its existing higher risk customers.

4.4. As part of its investigation leading to the 2013 Final Notice, the Authority reviewed a sample of 51 of GT Bank's higher risk retail customer files and identified weaknesses in each of the files, which included a failure by GT Bank to:

- (1) carry out and/or document an adequate risk assessment of the potential money laundering risks posed by high risk customers, in accordance with GT Bank's policies and procedures;
- (2) screen prospective customers against HM Treasury sanction lists prior to commencing the relationship;

- (3) establish and verify with adequate evidence the source of wealth and source of funds of higher risk customers; and
- (4) conduct ongoing reviews of higher risk customer files periodically to ensure the information and risk assessment was up to date, and that the activity on the accounts was consistent with expected activity.

4.5. Following the 2013 Final Notice, GT Bank engaged the external consultant in September 2013 to carry out a review of its AML policies and procedures, and systems and controls. The external consultant's report, which followed, was completed in December 2013 and it made 65 recommendations which GT Bank attempted to address throughout 2014.

#### Authority visit – 2014

4.6. In October 2014, the Authority carried out the 2014 visit, a formal supervisory visit to GT Bank as part of its AML supervisory strategy. Following this, the Authority highlighted to GT Bank a number of findings in relation its AML systems and controls, including:

- (1) lack of clarity around initial customer risk assessments;
- (2) missing CDD documentation within several customer files and a lack of follow up when documentation failed to be provided by the customer;
- (3) several files where insufficient information in relation to customer source of wealth had been gathered and recorded and a lack of understanding amongst GT Bank employees on the difference between source of wealth and source of funds; and
- (4) deficiencies within GT Bank's transaction monitoring system.

4.7. In December 2014, GT Bank set out the actions that it would take to address the Authority's findings from the 2014 visit, which included:

- (1) the implementation of a new risk assessment framework which would ensure that the rationale for both initial and ongoing risk ratings would be clearer and adequate narrative would be held on file;

- (2) the Look Back exercise relating to its customer files to address issues such as gaps in risk ratings, missing CDD and EDD documentation, missing source of wealth information, absence of evidence of Compliance sign-off; and to ensure that the requisite documentation was in place going forward; and
- (3) the implementation of a new transaction monitoring system.

#### Authority visit – 2017

- 4.8. In June 2017, the Authority carried out the 2017 visit, a second formal supervisory visit to GT Bank to review and test the adequacy of its AML, sanctions and terrorist financing systems and controls. The Authority found that despite assurances made by GT Bank in December 2014 that it would address findings identified by the Authority during the 2014 visit, in the Authority's view, significant weaknesses remained within GT Bank's AML systems and controls, including in areas that had been previously flagged such as deficiencies in the quality of source of wealth information gathered and inadequate narrative for risk ratings held on file. As part of the 2017 visit, the Authority also identified weaknesses in other areas of GT Bank's AML framework such as EDD, the investigation and closure of transaction monitoring alerts and adverse media hits.

#### The Skilled Person's report

- 4.9. As a result of the findings from the 2017 visit, a Skilled Person was appointed to:
- (1) assess the adequacy of GT Bank's financial crime governance arrangements and the effectiveness of senior management, systems and controls for AML and financial sanctions, including its transaction monitoring system and the effectiveness of its Compliance and Internal Audit functions;
  - (2) assess GT Bank's remediation plan based on the 2017 visit, its own findings and the relevant regulations and applicable guidance, and make recommendations to address any identified weaknesses in the remediation plan; and

- (3) subsequently test and evaluate the effectiveness of any remediation work undertaken by GT Bank.

4.10. The Skilled Person produced a report, dated 4 May 2018, which highlighted a number of significant deficiencies with respect to GT Bank's AML systems and controls, including:

- (1) as a result of existing gaps within the design and operating effectiveness of GT Bank's AML framework, its financial crime function was not fully embedded and effective;
- (2) MI in relation to GT Bank's adherence to its AML risk appetite and tracking of financial crime related actions and issues appeared to be inadequate;
- (3) a number of documentation gaps in customer files that had been subject to recent remediation by GT Bank, in areas such as applying appropriate EDD, and identifying and verifying source of funds and source of wealth;
- (4) failures to adhere to GT Bank's periodic customer file review process resulting in customer files not being reviewed in line with GT Bank's policy requirements; and
- (5) issues around the effectiveness of the escalation and review of unusual and/or suspicious activity, including the subsequent reporting of any such activity.

4.11. Following the 2017 visit, in early 2018, GT Bank suspended onboarding of new customers. Subsequently, on 13 November 2018 due to the Authority's ongoing concerns about the effectiveness of the systems and controls in place, GT Bank agreed to the voluntary imposition of wider requirements on its business to the effect that:

- (1) it would not accept or process new account applications from new customers;
- (2) it would not offer or provide new products to existing customers; and

- (3) where existing customers applied for new products, it would communicate to the customer that it was not accepting new applications for the named product at this time.
- 4.12. After improvements were made by GT Bank to its AML systems and controls, the Authority granted a temporary exception to these requirements on 26 June 2020 and GT Bank was permitted to engage with new customers and offer existing customers new products, for a limited period of time, albeit subject to continued close scrutiny by the Authority and the Skilled Person. Following validation from the Skilled Person that GT Bank had completed its remediation plan in relation to the Skilled Person's review, the Authority lifted the voluntary imposition of requirements on 8 July 2021.

### **The remediation of customer files following the 2013 Final Notice**

#### September 2014 review and the Six Point Review

- 4.13. In September 2014, GT Bank engaged the external consultant to conduct the September 2014 review, a further assessment of its AML policies, procedures, systems and controls. The external consultant was also asked to review the progress GT Bank had made with implementing the 65 recommendations set out in its first report.
- 4.14. The September 2014 review found that gaps still remained in GT Bank's AML framework in areas such as policies and procedures, customer risk assessment, CDD, ongoing monitoring, and transaction monitoring systems.
- 4.15. Whilst the September 2014 review was ongoing, GT Bank simultaneously conducted its own internal review of its AML procedures and customer files. The findings arising from this internal review prompted GT Bank to commence the Six Point Review, a remediation of its customer files. The objective of the Six Point Review was to identify and remediate deficiencies within its "Very High" and "High" risk customer files and ensure that information relating to: (i) sanctions; (ii) PEP and adverse media screening; (iii) source of income and source of wealth; (iv) purpose of account; (v) nature of relationship; and (vi) beneficial ownership were "*addressed and adequately evidenced on file.*"
- 4.16. The Six Point Review identified deficiencies in all six of the areas outlined above, resulting in 915 of GT Bank's "Very High" or "High" risk customer files requiring

remedial work. By February 2015, GT Bank was of the view it had remediated 630 customer files, at which point it stopped work on the Six Point Review. This left, issues remaining across the other 285 customer files which GT Bank proposed to remediate through a separate review based on the new Risk Assessment Framework.

- 4.17. GT Bank's Compliance function subsequently found the remedial work that had been carried out as part of the Six Point Review had been inadequate, particularly in relation to addressing issues around the establishment of source of funds received by GT Bank and explanations of source of wealth in new applications.

#### The Look Back exercise

- 4.18. GT Bank commenced its Look Back exercise at the end of July 2015. The Look Back exercise was designed to ensure that KYC/AML issues with GT Bank's customers and customer files were "*duly identified and rectified*" and that files were made fit for purpose.
- 4.19. The exercise was conducted in two phases – a "*review*" phase and a subsequent "*remediation*" phase. As part of the review phase, GT Bank focused solely on the review and identification of due diligence gaps within customer files. The remediation phase, which involved taking steps to request and obtain the missing required due diligence documentation, took place afterwards. This approach meant that GT Bank delayed addressing gaps in its individual and corporate customer files in circumstances where GT Bank had informed the Authority in December 2014 that it was aiming to complete this exercise by the end of 2015.

#### Remediation of issues identified as part of the Look Back exercise

- 4.20. As part of the Look Back exercise, GT Bank reviewed 1,156 active customer files. The results of the Look Back exercise, which considered these customer files against the improved standards imposed by GT Bank's new Risk Assessment Framework which had been approved in April 2015, highlighted that each of the 1,156 files reviewed was inadequate and required further due diligence information and therefore required remedial action.

- 4.21. GT Bank commenced the remediation phase of the Look Back exercise in December 2015, which involved requesting required but missing CDD/EDD documentation from customers throughout 2016.
- 4.22. GT Bank failed to put in place an adequate process to handle customer responses as part of the remediation phase of the Look Back exercise and as a result the review of responses was slow and follow-up queries and outstanding actions were not adequately tracked and/or resolved.
- 4.23. Based on the 920 responses received by 14 October 2016, GT Bank remediated 294 files but still had 475 files that required further information before they could be considered adequate. However, in an attempt to "*close out the remediation program within October*", it was suggested to close the remediation phase of the Look Back exercise in October 2016 and to inform the BRCC that follow-up steps to obtain additional information in relation to any files that still needed to be remediated would be rolled over to be addressed through the annual periodic customer file review process for the following year.
- 4.24. However, whilst it was reported to the BRCC by Compliance that the remediation phase of the Look Back exercise had closed, the remediation of outstanding files continued in practice and continued to be characterised by slow progress with insufficient resources allocated to completing the task. Furthermore, instead of addressing file deficiencies as part of the periodic review process as reported to the BRCC, the Financial Crime Team continued to focus on completing the remediation of files as a separate task and as a result GT Bank placed the periodic review of customer files on hold between January to March 2017, following which they were completed in April 2017.
- 4.25. By 6 March 2017, GT Bank had remediated 161 of an outstanding 475 files that still required remediation. In an effort to clear the outstanding backlog of 314 files in time for the April 2017 BRCC meeting, GT Bank senior management created a new simplified review process to enable files to be reviewed more quickly. An update was provided by Compliance to AMLOC on 30 March 2017 stating that the remediation in respect of the Look Back exercise was complete and that it had been achieved through use of newly received information from customers for 161 files, and by using information within GT Bank and accessed through public sources for the remaining 314 (i.e. existing information on the file, account usage history and adverse information checks).



- 4.26. By using information already held on file, GT Bank failed to consider whether a customer's personal circumstances had changed and the impact that this could have on the level of money laundering risk they posed. The 314 files had been identified as requiring remediation as part of the Look Back exercise because the information held on file was not considered to be adequate. In addition, GT Bank did not retain information about anticipated account activity in its internal systems and staff were unable to undertake any analysis of a customer's expected activity versus actual activity. Therefore, a review of account usage history would not, in the Authority's view, have been sufficient to assess the adequacy of the CDD recorded on the file.

The Skilled Person's review of remediated customer files

- 4.27. As part of its review in 2018, the Skilled Person reviewed a sample of 45 customer files, all of which GT Bank had attempted to remediate as part of the various remediation exercises described above. The Skilled Person identified weaknesses in all 45 files including deficiencies in the application of appropriate level of EDD, where required, and in the identification and verification of the source of funds and source of wealth of its customers, both of which were failings also identified within the 2013 Final Notice.
- 4.28. The Skilled Person noted in its report, dated 4 May 2018, that:

*"the quality of CDD and EDD information maintained on customer files requires improvement. Further enhancements are required to ensure that the level of CDD and EDD maintained on customer files satisfies the AML requirements and relevant guidance as well as the Bank's own financial crime policies and procedures".*

- 4.29. The Skilled Person's findings indicate that the customer file remediation work undertaken by GT Bank between 2014 and 2017 was inadequate, and that GT Bank continued to fail to carry out and document adequate CDD and EDD (where required) as previously identified by the Authority in the 2013 Final Notice.

**GT Bank's AML controls and framework**

- 4.30. Following the 2013 Final Notice, which set out serious failings in relation to GT Bank's customer risk assessment, CDD, EDD, source of wealth and ongoing

monitoring controls, the Authority expected that GT Bank would take steps to ensure its AML systems and controls generally, and particularly in these areas, were adequate and effective going forward. This issue should have been a key focus for GT Bank's senior management.

- 4.31. However, significant weaknesses and issues in GT Bank's AML systems and controls persisted throughout the relevant period, as set out below, resulting in ongoing deficiencies in customer risk assessment, customer onboarding, CDD and EDD, periodic reviews, screening and transaction monitoring.

#### Customer risk assessment

##### *Requirements*

- 4.32. Firms are required to assess the money laundering risk posed by individual customers and use this assessment to determine, on a risk-sensitive basis, the extent of CDD measures that should be applied at the outset of the business relationship and at other appropriate times. A firm should also be able to demonstrate that the extent of the measures applied is appropriate in view of the risks of money laundering and terrorist financing.
- 4.33. Firms must also document their risk assessments, keep these assessments up to date, and have appropriate mechanisms to provide appropriate risk assessment information to competent authorities.

##### *Issues with GT Bank's customer risk assessment process*

- 4.34. In the 2013 Final Notice, the Authority found that GT Bank failed to carry out and/or document an adequate risk assessment of the potential money laundering risks posed by higher risk customers in accordance with its policies and procedures.
- 4.35. Various internal and external reviews conducted throughout the relevant period, as set out above and below, showed that there continued to be weaknesses in GT Bank's AML controls and that the customer risk assessments continued to be inadequate. This created the risk that the due diligence undertaken on customers, particularly ones presenting a higher risk of money laundering risk, was insufficient.

*Documentation of customer risk assessment*

- 4.36. During the 2014 visit, the Authority noted that GT Bank reviewed customer risk ratings and updated these accordingly, providing a narrative for its reasons, as part of its annual review process. However, the Authority was unable to find evidence of initial risk assessments within most customer files and the lack of narrative meant that it was not clear how GT Bank had initially rated its customers.
- 4.37. In response to the above findings, GT Bank explained in a letter to the Authority, dated 9 December 2014, that its revised risk assessment framework would address the issue of the initial risk assessment of customers for account opening purposes and that adequate narrative to explain the rationale for ratings would be held on file. However, GT Bank failed to sufficiently address this issue as following a review of ten customer files in 2017, the external consultant identified that the customer risk assessment documents found in the files superseded earlier versions and that the previous versions were not retained on file.

*Justification of risk rating and application of CDD measures*

- 4.38. Following a review of a sample of GT Bank's customer files in July 2015, the external consultant found that it was not clear whether the risk ratings assigned to customers had driven the extent of due diligence completed and recommended that:
- (1) GT Bank should avoid assigning default "High" risk ratings based on the customer's geographic location with no further consideration given to other risk factors; and
  - (2) GT Bank should evidence within its customer files that a customer's risk assessment had driven the level of due diligence completed.
- 4.39. Issues with the adequacy of the customer risk assessments, including documentation of assessment and rationale for the assigned risk rating, continued throughout the relevant period. For example:
- (1) following a review of 46 of GT Bank's customer files in September 2014, the external consultant found that there was limited documented

justification to record why the risk rating awarded was considered appropriate given GT Bank's knowledge of the customer. The external consultant also noted that the actual risk rating awarded to customers differed to the rating that should have been awarded in line with GT Bank's AML policies and procedures;

- (2) following a review of a sample of new accounts opened and reviewed for the period May to September 2016, GT Bank's Compliance function reported to the BRCC in October 2016 that it had found:

*"insufficient risk mitigation and AML risks analysis on Risk Assessments, repetition on customers' information and most of the risk assessment report[s], signed by [members of senior management], are formulaic in nature"; and*

- (3) in 2017, GT Bank's Compliance function reported that improvements were needed on the risk assessments conducted on customers, stating that:

*"initial assessments and call reports must be more informative and cover in more detail the reasons for the account being opened and the purpose. They should focus on identifying specific AML/CTF risks and the degree of risk of handling the proceeds of financial crime and money laundering so that these are identified upfront with proposed mitigants and before [the Financial Crime Team] begin work. This is not evident from the initial review and calls into question the purpose of it".*

Despite these concerns around the inadequacy of risk assessments undertaken, the exact same issue was reported by the Compliance function to the BRCC again in April 2018.

- 4.40. GT Bank did not take steps to incorporate the recommendations of the external consultant from July 2015 (see paragraph 4.38 above). Following a review of GT Bank's customer onboarding procedures in 2017, the external consultant again found that in all files reviewed, GT Bank's customers were categorised as "Very High" or "High" risk, primarily based on GT Bank's view of the money laundering risk posed by the customer's geographic location and that the key difference in due diligence procedures applied to medium, high and very high risk customers

related to the frequency at which ongoing monitoring was conducted for each respective risk level.

#### Customer onboarding – CDD and EDD

##### *Requirements*

- 4.41. When establishing a business relationship, a firm must carry out CDD on a customer. This requires the firm to:
- (1) identify the customer and verify the customer's identity on the basis of documents or other data obtained from a reliable and independent source;
  - (2) identify any beneficial owners of a corporate customer, and take adequate measures on a risk sensitive basis to verify their identity; and
  - (3) understand the purpose and intended nature of the customer's relationship with the firm.
- 4.42. In situations which can present a higher risk of money laundering or terrorist financing, firms are required to apply risk sensitive EDD measures.

##### *Issues with GT Bank's CDD and EDD processes*

- 4.43. Following the 2013 Final Notice, which found that GT Bank had failed to carry out and document adequate CDD and to conduct EDD when establishing relationships with higher risk customers, GT Bank was already on notice of the weaknesses in its systems and controls in this area. However, issues around GT Bank's CDD procedures, including the quality of CDD documentation held on customer files, were again identified in 2014 and repeatedly throughout the rest of the relevant period. The findings made by the Authority, GT Bank's Compliance function, GT Bank Plc and the external consultant, as set out in the paragraphs below, were similar to those that had been set out in the 2013 Final Notice. However, GT Bank failed to remediate these failings despite being notified of similar CDD/EDD weaknesses within customer files at various points during the relevant period:

- (i) 2014

- (1) as part of the September 2014 review, the external consultant reviewed 46 of GT Bank's customer files. The external consultant noted that a number of areas required improvement relating to CDD, including that GT Bank's internal CDD procedures were not always followed in practice and that a number of gaps in actual CDD information held on file had been identified. It also found that where CDD information had been included on the file, given a failure to document appropriate justifications and conclusion, the CDD information was often insufficient to evidence that GT Bank had appropriately reviewed and considered the CDD information received for potential issues;
- (2) between September 2014 to October 2014, GT Bank Plc carried out an assessment of all of GT Bank's customer files. As part of this review, GT Bank Plc identified that GT Bank did not have a process in place that enabled it to track whether outstanding CDD documentation had been received and that there was no follow through process to ensure that documents were actually received. The fact that documentation was still outstanding was often not identified until the file was reviewed as part of subsequent annual review cycles; and
- (3) during the 2014 visit, the Authority found that CDD documentation was missing across several files and that whilst the missing documentation had been requested during annual reviews, there was no evidence on file that documents had been obtained;
  - (ii) *2015*
- (4) between July 2014 and 21 August 2015, the Compliance function reviewed and signed-off on all new account applications. Between March and September 2015, the following issues were highlighted within quarterly reports to the BRCC:
  - (a) insufficient steps were taken to establish and verify the sources of wealth and income;
  - (b) identification and verification documentation was not obtained or not certified adequately; and

- (c) insufficient steps were taken to establish the nature and purpose of accounts for corporate accounts;
- (5) following changes to its AML policies and procedures, including its customer account opening application form in July 2015, GT Bank's senior management questioned whether the newly implemented due diligence processes were appropriate or if they were excessive. GT Bank engaged the external consultant to review a sample of files, including ones which had been recently onboarded under the revised processes and pending account applications to assess this. Following its review, the external consultant identified a number of CDD issues, including that "*none of the cases demonstrated that sufficient adequate due diligence was recorded appropriately*" and concluded that the depth of CDD undertaken by GT Bank should be enhanced in order for it to meet its AML obligations;
- (iii) 2016
- (6) as part of GT Bank's 2016 compliance monitoring programme, the Compliance function reviewed a sample of new accounts that were opened between May and September 2016. Following the review, the Compliance function noted that "*the current quality of on-boarding and remediation work undertaken by the bank is poor*". The findings presented to the BRCC in October 2016 included a lack of documented evidence of the purpose and intended nature of the business relationship, incomplete or inadequate details provided on account application forms and inconsistencies with the submission of identification documents; and
- (7) the Compliance function's findings also indicated that the information provided by the customer was often not checked, verified or challenged by GT Bank prior to account approval. For example:
- (a) in one instance, the customer risk assessment stated that the customer had studied at the "*University of Life, Nigeria*", which is not a recognised formal institute of higher education; and
  - (b) in several instances, the figures provided for annual turnover were inconsistent with the anticipated number of transactions and amounts per month.

4.44. Concerns around GT Bank's approach to CDD were raised throughout the relevant period. In July 2015, the external consultant found that although the CDD undertaken by GT Bank throughout the relevant period was process-driven with various file reviews showing that documents were obtained from the customer, there was no documentation of the assessment of the impact the information provided had on the relationship between GT Bank and its customer. In October 2016, GT Bank's Compliance function flagged that the standard and validity of CDD documents was not fully reviewed by staff in GT Bank's customer facing teams, and that this created a risk that GT Bank was not fully aware of the money laundering risks associated with the customer. In December 2017, GT Bank's Compliance function reported to the BRCC that greater care was needed to ensure all documents were reviewed, and that information was recorded on file and fully assessed.

Customer onboarding – source of funds and source of wealth

4.45. In the 2013 Final Notice, the Authority found that GT Bank had failed to establish and verify with adequate evidence the source of funds and wealth of higher risk customers. During the 2014 visit, the Authority found that insufficient information had been gathered and recorded in several customer files in relation to source of wealth and that there was confusion between the different concepts of source of funds and source of wealth. In response to this, GT Bank stated in its letter to the Authority, dated 9 December 2014, that one of the actions it would take would be to reiterate the difference between these concepts to its staff and ensure that this was incorporated within its training programme. GT Bank also updated its account opening application form to include a better description and explanation of what source of funds and source of wealth evidence was required.

4.46. However, issues around source of funds and source of wealth persisted. Accordingly, adverse findings in relation to adequately assessing and obtaining sufficient evidence for customer source of funds and source of wealth when onboarding new customers were made by the Compliance function and the external consultant throughout the relevant period, particularly after the conclusion of the Look Back exercise. For example:

- (1) between July and August 2015, the Compliance function reviewed and signed-off all new account applications prior to the account being opened. Key issues were reported to the BRCC in quarterly Compliance and Anti-



Money Laundering Reports and the reports for this period highlighted issues around insufficient steps being taken to establish and verify source of funds and/or source of wealth;

- (2) following a review of recently onboarded customer files and pending applications in July 2015, the external consultant found "*confusion between source of funds and source of wealth*" where the same items were used as evidence of both. This review also highlighted that it was unclear from the files what information had been obtained and assessed to evidence source of funds, considerations made by GT Bank or whether GT Bank considered the evidence sufficient;
- (3) in 2016, as part of the Compliance Monitoring Programme, the Compliance function reviewed a sample of new accounts opened and reviewed for the period May to September 2016. As part of this review, the Compliance function identified that inadequate information was provided with regards to both source of funds and source of wealth; and
- (4) as part of a file review undertaken on recently onboarded customer accounts in November 2017, the external consultant found deficiencies around how GT Bank identified customer source of wealth, including where information recorded by GT Bank did not match that provided by the customer.

4.47. GT Bank's failure to obtain sufficient information in respect of source of funds and source of wealth was also a breach of its internal policies. Prior to entering into a business relationship, GT Bank's policies required that the "*provenance of assets that are to be introduced into the relationship (i.e. source of income, source of wealth and source of funds – how the income, wealth, and funds were originally earned or acquired by the customer, by whom, from whom, from where etc)*" must be understood.

4.48. In its report dated May 2018, the Skilled Person found that GT Bank's definitions of source of funds and source of wealth were not always clearly distinguishable. Furthermore, the Skilled Person found from its file reviews that, where applicable, source of funds and source of wealth were not adequately identified and verified. In failing adequately to establish and verify source of funds and source of wealth for its customers, GT Bank was unable to make fully informed decisions around

the legitimacy of customer funds and therefore, was unable to ensure that accounts were not being used to facilitate the proceeds of crime.

#### Customer facing teams

- 4.49. Primary responsibility for assessing the money laundering risk posed by customers and obtaining CDD and EDD information, including adequate evidence of a customer's source of funds and source of wealth, at onboarding sat with staff in GT Bank's customer facing teams throughout the relevant period.
- 4.50. However, the customer facing teams failed to demonstrate sufficient meaningful engagement with, or ownership of, the onboarding process during the relevant period. GT Bank's Compliance function commented in October 2016 that the process of assessing risk and due diligence was treated as a *"tick-box exercise instead of giving the documents the attention they deserve"*. Following completion of what was intended to be the risk assessment, and after receipt of what was intended to be the required due diligence information, the customer facing teams were supposed to pass prospective customer applications to the Financial Crime Team for review. In practice, the customer facing teams often provided incomplete account applications with inadequate CDD/EDD documentation to the Financial Crime Team. The strong focus of the customer facing teams on getting new business was to the detriment of carrying out appropriate CDD/EDD.
- 4.51. There was a lack of sufficient understanding within the customer facing teams of what was required of them. This was further exacerbated by a culture whereby the customer facing teams did not consider key AML tasks, such as undertaking a risk assessment and obtaining the necessary due diligence information, to be their responsibility.
- 4.52. Whilst the attitude and competence of the customer facing teams towards AML compliance was a known issue to senior management, steps taken to improve the compliance culture within these teams were insufficient resulting in persistent disregard for processes and procedures throughout the relevant period. This was one of the root causes of many of the ongoing due diligence failings within GT Bank during the relevant period and is particularly serious given that the customer facing teams were GT Bank's first line of defence against money laundering risk and held ultimate responsibility for assessing the financial crime risk posed by prospective customers.

### Ongoing monitoring – periodic review

#### *Requirements*

- 4.53. A firm must conduct ongoing monitoring of all business relationships, tailored in accordance with the firm's risk assessment of that customer. Ongoing monitoring includes keeping CDD up to date through periodic review of the customer files and/or conducting reviews of the due diligence held in response to certain trigger events. Where the business relationship is considered to be higher risk, the ongoing monitoring must be enhanced.

#### *Periodic review of customer files*

- 4.54. In its letter to the Authority dated 9 December 2014, GT Bank stated that the Look Back exercise would be conducted and that future periodic reviews would continue to take place to ensure that CDD information was kept up to date. GT Bank did not conduct separate periodic reviews of customer files in 2015, as this was subsumed within the Look Back exercise. Periodic reviews of customer files, including follow-up for additional information and documentation requested from customers, resumed in November 2016 following completion of the remediation phase of the Look Back exercise in October 2016.
- 4.55. Following the completion of periodic reviews for customer files in November 2016 and December 2016, periodic reviews were suspended once again whilst GT Bank senior management changed the periodic review process to a simpler format and process to enable staff to complete reviews more quickly.
- 4.56. Periodic reviews were due to restart in February 2017 using the new process, however, GT Bank did not undertake any periodic review assessments between January and March 2017, resulting in a backlog of customer files to be reviewed. Whilst this backlog was cleared in April 2017, reviews fell behind again between May and December 2017. A backlog of customer files awaiting review and outstanding queries remained until April 2018, as in January 2018 GT Bank's attention shifted to another remediation exercise of all customer files that had been initiated following the 2017 visit. This was triggered by senior management identifying that a number of findings made by the Authority during the 2017 visit were "*the same in 2014 and earlier*".

4.57. As part of the periodic reviews undertaken between January 2017 and August 2017, GT Bank requested information from 165 customers where it was identified that further CDD/EDD information was required. However, GT Bank only received 18 responses. Despite the low response rate, GT Bank failed adequately to follow-up on outstanding requests for CDD/EDD documents. As a result, a number of information requests remained outstanding and unaddressed for several months. For example:

- (1) in January 2017, GT Bank awaited further information from 15 customers. AMLOC reports show that only 4 out of 15 customers responded and that the 11 remaining responses were still outstanding by August 2017;
- (2) in February 2017, GT Bank awaited further information from 18 customers, however, GT Bank did not receive a single response. AMLOC reports show that GT Bank had still not received the required information from these customers by August 2017; and
- (3) where responses were received, in some instances, GT Bank failed to review the information as the documentation was placed in boxes rather than put on the customer's file.

4.58. The weaknesses in GT Bank's periodic review processes were further exacerbated by a lack of adequate resources in the relevant teams. This was made worse by pressure from the customer facing teams who required staff to prioritise the opening of new accounts over the periodic review of existing accounts.

4.59. The issues around the periodic review of customer files that persisted throughout the relevant period were also identified by the Skilled Person in its report dated 4 May 2018. Key points included that:

- (1) 62% of the customer files reviewed did not contain up to date CDD and/or EDD; and
- (2) 74% of the customer files in the testing sample (the majority of which were for "High" risk or "Very High" risk customers) had not been reviewed in line with the defined frequency noted in GT Bank's policy.

- 4.60. The Skilled Person identified CDD and/or EDD weaknesses in 100% of the files sampled as part of its review and concluded that whilst GT Bank's periodic review policies reflected regulatory requirements and guidance, GT Bank had failed to effectively embed the periodic review cycle in practice. The Skilled Person noted that the majority of customer files reviewed as part of its sample had not undergone a periodic review in accordance with the GT Bank's internal policy and required remedial action in this regard.

Ongoing monitoring – monitoring of customer transactions

*Requirements*

- 4.61. As part of its obligation to monitor all business relationships with existing clients, a firm must also scrutinise customer transactions to ensure that they are consistent with the firm's knowledge of the customer, its business and its risk profile. Where the business relationship is considered to present a higher risk of money laundering or terrorist financing, a firm must apply enhanced ongoing monitoring.

*GT Bank's systems and processes for monitoring transactions*

- 4.62. In October 2014, GT Bank used a combination of System A, an automated transaction monitoring system, and manual processes to monitor customer transactions and activity. Following the decision in March 2015 to decommission System A, pending the implementation of a new automated transaction monitoring system, GT Bank relied solely on manual transaction monitoring processes.
- 4.63. GT Bank's manual transaction monitoring processes involved reviewing customer transactions on a daily basis and looking for "*large transactions*" (i.e. those transactions equal to or above the threshold for a particular type of account) or any suspicious pattern of transactions. Discrepancies were to be noted and additional information requested, where required. If the explanation received was unsatisfactory, the transaction was escalated. Responsibility for GT Bank's manual transaction monitoring process sat with the staff in GT Bank's Financial Crime Team throughout the relevant period.

- 4.64. GT Bank ceased its manual transaction monitoring processes in May 2017 following the implementation of System B, its new automated transaction monitoring system.

*Issues with GT Bank's transaction monitoring*

- 4.65. In October 2014, the Authority highlighted several deficiencies with System A. GT Bank had also identified that System A was "*very problematic*" and was in the process of replacing it. However, GT Bank's testing and implementation of System B was delayed by inadequate resourcing of the project, a lack of senior management engagement and oversight and unclear timescales and deadlines. This contributed to the failure to implement System B in a timely manner.
- 4.66. The effectiveness of GT Bank's monitoring system in identifying unusual activity depended on the quality of the parameters which determined what alerts were generated, and the ability of staff to assess the alerts and take appropriate action. Concerns in relation to both these areas were escalated to GT Bank senior management throughout the relevant period.

GT Bank's transaction monitoring methodology and parameters

- 4.67. Weaknesses in GT Bank's manual transaction monitoring methodology were repeatedly raised by the Compliance function. In particular, concerns were flagged around the ineffectiveness of the methodology in identifying linked transactions.
- 4.68. In 2018, the Skilled Person identified that GT Bank's thresholds for monitoring repeat and linked transactions were not included in the defined parameters on System B. As such, GT Bank's controls around identifying transactions that could evade thresholds for unusual or suspicious activity remained inadequate despite repeated concerns being raised throughout the relevant period and the implementation of an automated system.
- 4.69. Firms are expected to obtain appropriate information to understand a customer's circumstances and business, including the expected nature and level of transactions. Whilst GT Bank requested information such as "*anticipated account turnover*" and "*anticipated number of transactions per month*" from customers, it did not record this information on its systems and, accordingly, staff were unable to undertake any analysis of a customer's expected account activity versus their

actual account activity. This limited GT Bank's ability to identify unusual or suspicious transactions.

- 4.70. In June 2015, the external consultant raised concerns about the suitability and appropriateness of GT Bank's transaction monitoring parameters. GT Bank's senior management did not address these concerns following the implementation of System B in May 2017. However, GT Bank's Internal Audit function and the Authority both raised concerns around the scenarios in System B and the effectiveness of the 'one size fits all' approach adopted by GT Bank. The Skilled Person noted in its report, dated 4 May 2018, that GT Bank's overall approach to transaction monitoring required "*further enhancement before it can be considered adequate and effective*", and found that "*the Bank's transaction monitoring parameters do not fully reflect and are not specific to the different types of customers and sectors the Bank operates in*", including that there were no specific parameters defined for monitoring high risk customer accounts.

#### Review and closure of transaction monitoring alerts

- 4.71. Concerns around the adequacy of investigation of transaction monitoring alerts were consistently raised by both GT Bank's Compliance function and the external consultant in 2014 and 2015. Despite assurances that the replacement automated transaction monitoring system would address concerns in respect of alert closure narratives, weaknesses in the quality of review and closure of transaction monitoring alerts persisted and were raised by GT Bank Plc, the Authority, and the Skilled Person.
- 4.72. Pending the implementation of System B, GT Bank should have ensured that its manual transaction monitoring processes were fit for purpose and effective in the identification of unusual or suspicious activity. However, weaknesses in GT Bank's manual transaction monitoring processes followed by the lack of effectiveness of transaction monitoring parameters set in System B after its implementation, resulted in the absence of robust transaction monitoring controls during the relevant period. This increased the potential of GT Bank being used to facilitate financial crime over a prolonged period of time.

#### PEP, sanctions and adverse media screening

- 4.73. Firms should have processes to manage the risk of conducting business with or on behalf of individuals and entities on the Consolidated List, such as screening

their customers and certain transaction data and assessing the potential money laundering risk posed by the customer and/or transactions.

- 4.74. GT Bank used various third party screening systems to ascertain whether prospective or existing customers should be classified as PEPs or subject to sanctions or prohibitions, or any adverse media reports. The names of prospective customers were screened as part of the onboarding process and once onboarded, the customer names were added to an "*Ongoing Active*" list so that the customer names could be screened on an ongoing basis. GT Bank's entire customer database was automatically screened on a daily basis to identify PEP, sanctions or adverse media matches, and results were printed and retained on the customer file.
- 4.75. GT Bank's procedures required staff to document any reasoning or rationale applied in circumstances where a result was deemed to be a false positive match and the alert was closed. However, concerns around quality of screening, particularly in relation to the documentation of justification of decisions, were raised throughout the relevant period. For example:
- (1) as part of the September 2014 review, the external consultant found a lack of evidence to indicate that customers had undergone PEP, sanctions and adverse media screening. The external consultant also identified that a PEP had been incorrectly classed as a 'non-PEP' but that there was no justification as to the reason for this documented on the customer's file;
  - (2) the external consultant conducted a subsequent review of additional client files in July 2015 and again identified a lack of evidence on file to support any investigation or analysis completed, including documented justification and conclusions around the potential implications of any results, particularly in relation to adverse media identified;
  - (3) in September 2015, the Internal Audit function identified that 8,339 screening records had a screening status of "*initial only*" and had not been marked as "*Ongoing Active*" in line with GT Bank's screening procedures (see paragraph 4.74 above) meaning that these records were not screened on a daily basis and any adverse media associated with these individuals and/or corporate entities would not be identified. Internal Audit stated in its report that senior management should ensure that all statuses were set



to "on going". Despite this issue being raised, adequate steps were not taken to address it, as the Compliance function raised similar concerns between May 2016 and March 2017 around whether customer names were being added to the "Ongoing Activity" list to enable adequate ongoing monitoring;

- (4) between May 2016 and March 2017, following file reviews conducted as part of GT Bank's Compliance Monitoring Programme, the Compliance function identified a lack of evidence on customer files to show that screening results had been adequately reviewed and analysed and that there was an impression that results were just "printed and simply filed"; and
- (5) during the 2017 visit, the Authority found a number of deficiencies in the recording rationales of discounted adverse media reports across high risk customer accounts.

4.76. As part of a review of investigations undertaken by GT Bank, as a result of customer screening alerts generated by third party systems, the Skilled Person found that 83% of PEP alerts and 90% of sanctions alerts reviewed did not contain sufficient information on file to substantiate the conclusion reached that the match was a false positive and should be dismissed.

4.77. The Skilled Person also noted that GT Bank's approach to adverse media was not clearly articulated and that the approach to conducting adverse media searches was inconsistent amongst staff. Furthermore, it was not always clear how staff reviewed and/or assessed and analysed search results.

### **Senior management oversight**

4.78. GT Bank's senior management were responsible for ensuring that its AML systems and controls were appropriately designed and implemented and effective at reducing the risk of GT Bank being used in connection with money laundering or terrorist financing.

4.79. Following the 2013 Final Notice, the Authority expected that GT Bank's senior management would prioritise addressing weaknesses within its AML control framework, including the remediation of its customer files, by ensuring that sufficient focus was given to remediation efforts, that teams responsible for

carrying out remedial work, such as the Financial Crime Team, were adequately resourced and that AML issues were addressed in a timely manner.

4.80. However, GT Bank's senior management failed adequately to address AML deficiencies and weaknesses and address the root causes of these issues. This resulted in the repeated and continued failings identified by the Authority, GT Bank's Compliance function, GT Bank Plc and the external consultant at various points during the relevant period. These failures in senior management oversight were characterised by a lack of clearly defined roles and responsibilities, and inadequate challenge of poor MI. For example:

- (1) it was unclear who, at senior management level, held direct responsibility for the management and oversight of the Look Back exercise. Given the importance of the remediation of customer files in this context, the Authority would expect roles and responsibilities at senior management level to have been clearly defined; and
- (2) the Skilled Person identified in its report, dated 4 May 2018, that MI was inadequate and that it was not subject to adequate review and challenge by senior management.

4.81. When GT Bank's senior management was questioned or challenged by the BRCC on issues around the slow progress of and management of remediation and delays to the implementation of System B they failed to take adequate steps to address these concerns, often reassuring the BRCC that issues had either been resolved or were being addressed when this was not the case.

### **Resourcing**

4.82. GT Bank's senior management were responsible for ensuring that adequate resources were dedicated to remediating the issues related to the deficiencies in AML systems and controls and countering the risk that GT Bank would be used for the purposes of financial crime.

4.83. The Financial Crime Team was responsible for carrying out key AML processes such as customer onboarding, transaction monitoring, PEP, sanctions and adverse media screening and periodic review throughout the relevant period. From July 2015, the Financial Crime Team was also tasked with completing both phases of

the Look Back exercise, as set out above, and the testing and implementation of System B.

- 4.84. Concerns about the resourcing levels of the Financial Crime Team and its ability to effectively perform all the tasks and responsibilities assigned to it were escalated to GT Bank's senior management in December 2015 and continued to be escalated by the Compliance function at the BRCC and AMLOC meetings between February and May 2016. GT Bank's senior management was acutely aware during this period of the significant amount of responsibility placed on the Financial Crime Team and that resourcing levels may have been inadequate.
- 4.85. Issues such as the slow progress of the remediation phase of the Look Back exercise, delays in the implementation of System B and backlogs of periodic reviews in 2017, should have been a clear indication to senior management that resourcing levels were insufficient for GT Bank to complete important and necessary AML tasks in a timely manner. For example:
- (1) instead of allocating additional resources to address concerns about the slow progress of the remediation phase of the Look Back exercise, senior management reorganised existing resources and created a dedicated remediation team comprising of members of the Financial Crime Team, although, at times, the degree of resource available in practice for this was minimal. Despite the creation of a dedicated team, progress remained slow and the capacity of the Financial Crime Team was reduced. As a result, other key tasks, such as testing of the replacement automated transaction monitoring system, were put on hold due to the lack of resources available to progress both tasks simultaneously;
  - (2) due to pressure from senior management to complete the remediation of outstanding files from the remediation phase of the Look Back exercise by April 2017, the Financial Crime Team was unable to carry out periodic reviews of customer files between January and March 2017 due to a lack of available resource. These periodic reviews were completed in April 2017; and
  - (3) backlogs in the periodic review process continued to persist throughout 2017 due to a lack of sufficient resource to adequately carry out the review of customer files within required timescales.

## **Staff knowledge, awareness and training**

- 4.86. Firms are required to take appropriate measures to ensure that all relevant employees are made aware of the law, rules and regulations relating to money laundering and terrorist financing and are regularly provided with training in how to recognise and deal with suspicious transactions and other activities.
- 4.87. Furthermore, JMLSG Guidance states that a firm's approach to training should be built around ensuring that the content and frequency of training reflects the risk assessment of the products and services of the firm and the specific role of the individual.
- 4.88. GT Bank's AML training programme consisted of AML awareness training at induction for new staff and annual AML refresher training for all staff, with specific in-house training delivered on an ad hoc basis. Following the September 2013 review, the external consultant concluded that whilst the AML training provided was of good quality and provided high-level information, there were areas for improvement in GT Bank's identification of training needs, training programme, attendance and records.
- 4.89. GT Bank failed to sufficiently address the recommendations from the September 2013 review as following the September 2014 review, the external consultant identified that GT Bank's training log required enhancement and that further role-specific training needed to be developed.
- 4.90. Subsequent reviews of GT Bank's AML training programme indicated weaknesses within the programme which continued, unaddressed, throughout the relevant period, for example:
- (1) in November 2017, the external consultant found that the induction AML training provided was high-level and not tailored to GT Bank's core products and customers; and
  - (2) this view was also shared by the Skilled Person in its report, dated 4 May 2018, noting that GT Bank did not maintain a consolidated and complete AML training log, an AML training plan or offer tailored AML training based on role and AML responsibilities and concluded that GT Bank's AML training

programme could not be considered fit for purpose and required enhancement.

- 4.91. An effective and comprehensive AML training programme is crucial to the success of a firm's AML strategy. The inadequacies of GT Bank's AML training programme, in relation to content, tracking and monitoring, resulted in an increased risk that its employees could not adequately assess the money laundering risks posed by its customers and were ill-equipped to identify suspicious and/or unusual activities or transactions. The weaknesses in training manifested themselves against a background of widespread failings within GT Bank throughout the relevant period in the key areas of customer risk assessment, CDD/EDD and transaction monitoring.

#### Concerns around staff knowledge and awareness

- 4.92. Firms are required to employ individuals with the skills, knowledge and expertise necessary for the discharge of the responsibilities allocated to them.
- 4.93. The external consultant had recommended that GT Bank create a skills matrix that set out the skills and experience required for each AML related role, the training required for that role and the training received by each staff member in that role. Despite GT Bank's senior management committing to develop this by 31 January 2014, the Skilled Person identified, in its report dated 4 May 2018, that GT Bank did not conduct training need assessments on an individual or departmental basis.
- 4.94. Without an adequate and full understanding of the AML knowledge and skills required to effectively carry out AML roles, GT Bank was unable to assess whether the level of AML knowledge of staff with significant AML responsibility was adequate and take steps to provide the requisite training to address any knowledge or competency gaps.
- 4.95. The Financial Crime Team had a significant amount of responsibility for carrying out AML activities within GT Bank, including signing off on CDD/EDD and transaction monitoring. As such, GT Bank's senior management should have ensured that those within the Financial Crime Team were competent and fully equipped with the necessary knowledge and training to perform their roles effectively. However, although concerns regarding the competence and

knowledge of those responsible for carrying out AML activities were escalated repeatedly throughout the relevant period to GT Bank senior management, these were not sufficiently addressed.

## **5. FAILINGS**

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

5.2. Based on the facts and matters described above, the Authority concludes that GT Bank has breached Principle 3.

5.3. GT Bank breached Principle 3 (management and control) by failing to take reasonable care to ensure it had effective systems and controls in place, with adequate risk management systems, within its AML process. In particular, GT Bank did not:

- (1) conduct adequate customer risk assessments, often failing to assess and document the money laundering risk posed by the customer or prospective customer. This includes:
  - a) during the 2014 visit, the Authority noted that there was limited evidence of initial risk ratings on customer files;
  - b) during 2014, the external consultant identified insufficient justification for the risk rating awarded to customers in GT Bank's files, and cases where the risk rating awarded to customers differed from the risk rating that should have been applied in line with GT Bank's procedures;
  - c) further weaknesses were identified in July 2015, when the external consultant found that risk ratings did not drive the extent of the due diligence conducted; and
  - d) in 2017 and 2018, GT Bank's Compliance function reported that initial risk assessments should be more detailed and informative.

The repeated failure to conduct adequate risk assessments meant that GT Bank was unable to properly assess and mitigate the risk that it may be used to facilitate financial crime;

- (2) conduct adequate CDD and EDD when establishing a business relationship with a customer. Reviews undertaken by the external consultant, GT Bank's Compliance function and the Skilled Person between 2015 and 2018 identified insufficient due diligence had been undertaken in relation to new customers. GT Bank failed to obtain sufficient information in relation to source of funds and source of wealth, failed to identify or verify customer identification documentation and failed to verify the authenticity of information provided by customers. This meant that GT Bank could not make fully informed and accurate risk assessments of the financial crime risk posed by its customers;
- (3) ensure that the information it held on customers was up to date and accurate by undertaking regular timely reviews of customer files in line with its internal policies and procedures. GT Bank failed to conduct any periodic reviews between July 2015 and October 2016, and although these resumed in November 2016, they were suspended once again in January 2017 and a backlog existed until April 2017. Periodic reviews were delayed again between May and December 2017, and a backlog existed until April 2018. This resulted in GT Bank being unable to assess, for large swathes of time, whether the risks posed by its customers had changed, and in particular whether they had increased;
- (4) conduct adequate and effective monitoring of customer transactions. System A, GT Bank's former automated transaction monitoring system, was not fit for purpose. Following the decommissioning of System A, GT Bank relied on manual transaction monitoring which was also ineffective in identifying unusual or suspicious activity within transactions. Furthermore, there were delays in the implementation of a replacement automated system, System B, due to inadequate resources being allocated to implement it, a lack of senior management oversight, and an absence of clear deadlines resulting in increased exposure to financial crime risk during the lengthy transition period. When System B was implemented in May 2017, both GT Bank's Internal Audit function and the Authority raised concerns about the effectiveness of the system and, in May 2018, the

Skilled Person found that further enhancement was required before the system could be considered adequate. The absence of a transaction monitoring system that was fit for purpose, over a significant period of time, resulted in an unacceptable risk that GT Bank may be used for the purposes of financial crime;

- (5) take appropriate, timely, remedial action to rectify the weaknesses in its AML and sanctions systems and controls identified by:
  - a) the 2013 Final Notice;
  - b) the Authority following its 2014 and 2017 visits;
  - c) GT Bank's own Compliance and Internal Audit functions, throughout the relevant period; and
  - d) the external consultant, throughout the relevant period.

This includes failure to complete the remediation of 1,156 active customer files in circumstances where, due to a variety of reviews that were carried out, GT Bank was aware that required due diligence information was missing. The Skilled Person noted that the quality of information held on customer files still required improvement in May 2018, almost four years after the commencement of the Six Point Review;

- (6) ensure that its staff received appropriate AML training. Despite concerns being raised by the external consultant and the Skilled Person throughout the relevant period, GT Bank's AML training was not targeted to the needs of staff members and was instead high-level and generic. This weakness occurred despite GT Bank being aware of the wide-ranging weaknesses in its AML systems and controls and the inadequacy of the ongoing remediation work. As a result, staff were ill-equipped to identify and assess financial crime risks posed by customers and lacked the necessary skills to help improve GT Bank's AML systems and controls; and
- (7) implement a culture which recognised the importance of preventing financial crime. GT Bank failed to provide sufficient resources, focus and challenge to various workstreams designed to remediate deficiencies in AML systems and controls and failed to put in place a culture where



customer facing teams understood and prioritised CDD and EDD to ensure that required information was complete and accurate.

- 5.4. The weaknesses in GT Bank's AML systems and controls resulted in an unacceptable risk that it would be used by those seeking to launder money, evade financial sanctions or finance terrorism.

## **6. SANCTION**

- 6.1. The Authority's policy for imposing a financial penalty is set out in Chapter 6 of DEPP. In respect of conduct occurring on or after 6 March 2010, the Authority applies a five-step framework to determine the appropriate level of financial penalties imposed on firms.

### **Step 1: disgorgement**

- 6.2. Pursuant to DEPP 6.5A.1G, at Step 1 the Authority seeks to deprive a firm of the financial benefit derived directly from the breach where it is practicable to quantify this.
- 6.3. The Authority has not identified any financial benefit that GT Bank derived directly from its breach.
- 6.4. Step 1 is therefore £0.

### **Step 2: the seriousness of the breach**

- 6.5. Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breach. Where the amount of revenue generated by a firm from a particular product line or business area is indicative of the harm or potential harm that its breach may cause, that figure will be based on a percentage of the firm's revenue from the relevant products or business area.
- 6.6. The Authority considers that the revenue generated by GT Bank is indicative of the harm or potential harm caused by its breach. The Authority has therefore determined a figure based on a percentage of GT Bank's relevant revenue. GT Bank's relevant revenue is the revenue derived by GT Bank's during the period of the breach. The period of GT Bank's breach was from October 2014 to July 2019.

The Authority considers GT Bank's relevant revenue for this period to be £29,822,390.

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

Level 1 – 0%

Level 2 – 5%

Level 3 – 10%

Level 4 – 15%

Level 5 – 20%

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

- (1) the breach revealed serious or systemic weaknesses in the firm's procedures or in the management systems or internal controls relating to all or part of the firm's business;
- (2) the breach created a significant risk that financial crime would be facilitated, occasioned or otherwise occur; and
- (3) the breach was committed deliberately or recklessly.

- 6.9. The Authority also considers that the following factors are relevant:

- (1) during the relevant period, various reviews of AML systems and controls were undertaken by the external consultant, GT Bank Plc and GT Bank's Compliance and Internal Audit functions. The Authority also conducted supervisory visits in 2014 and 2017. All of these identified inadequate AML systems and controls and clearly highlighted required remedial action.

However, GT Bank failed to take adequate steps to address significant deficiencies, and in some cases, ceased remedial work before it was completed;

- (2) GT Bank provided financial services to customers from or closely linked to higher risk jurisdictions identified by industry recognised sources such as the Basel AML Index and the Corruption Perceptions Index as having a higher vulnerability to money laundering and terrorist financing and corruption. GT Bank provided a gateway to the UK financial system for these customers and should have had systems and controls to mitigate the risk that the proceeds of financial crime could enter the UK. By failing to remediate serious deficiencies in systems and controls for a significant and prolonged period of time, there was an increased risk that GT Bank could be used to facilitate financial crime;
- (3) GT Bank's conduct was reckless, as it was aware of the serious and significant deficiencies in its AML systems and controls, which were clearly set out in the 2013 Final Notice, in subsequent reports produced by the external consultant, and GT Bank's Compliance and Internal Audit functions and in supervisory correspondence from the Authority. GT Bank was also aware that the inadequate AML systems and controls led to an increased risk that it could be used to facilitate financial crime. Furthermore, despite very clear recommendations in reports produced by the external consultant, GT Bank failed to take adequate steps to address the deficiencies; and
- (4) the deficiencies in the AML control framework at GT Bank created a significant risk that financial crime would be facilitated, occasioned or otherwise occur.

6.10. Taking all of these factors into account, the Authority considers the seriousness of the breach to be level 4 and so the Step 2 figure is 15% of £29,822,390.

6.11. Step 2 is therefore £4,473,359.

### **Step 3: mitigating and aggravating factors**

6.12. Pursuant to DEPP 6.5A.3G, at Step 3 the Authority may increase or decrease the amount of the financial penalty arrived at after Step 2, but not including any amount to be disgorged as set out in Step 1, to take into account factors which aggravate or mitigate the breach.

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

- (1) GT Bank was the subject of the 2013 Final Notice for similar serious and systemic failings in its AML systems and controls. This is an example of repeated misconduct by GT Bank;
- (2) GT Bank was aware of the failings set out in the 2013 Final Notice and was aware that the failings continued throughout the relevant period;
- (3) the widespread weaknesses in GT Bank's AML systems and controls continued over a significant period of time and were only addressed following action taken by the Authority to appoint a Skilled Person in December 2017;
- (4) the Authority carried out the 2014 visit and the 2017 visit to GT Bank and clearly set out to GT Bank in supervisory correspondence the findings and continued deficiencies in AML systems and controls and GT Bank did not sufficiently complete remedial action;
- (5) the 2013 Final Notice did not cause GT Bank to remediate sufficiently the material weaknesses in its systems and controls;
- (6) GT Bank had access to considerable guidance, from the Authority and other bodies, both before and during the relevant period, on how to comply with its regulatory requirements; and
- (7) the Authority has issued and published numerous Final Notices against authorised firms in recent years for AML weaknesses of which GT Bank was or should have been aware.

6.14. The Authority considers that the following factor mitigates the breach:

(1) in early 2018, GT Bank voluntarily imposed restrictions on its business that prevented it from onboarding new customers.

6.15. Having taken into account these aggravating and mitigating factors, the Authority considers that the Step 2 figure should be increased by 40%.

6.16. Step 3 is therefore £6,262,702.

#### **Step 4: adjustment for deterrence**

6.17. 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.

6.18. The Authority considers that the Step 3 figure of £6,262,702 represents an insufficient deterrent to GT Bank and others, given GT Bank's serious and repeated misconduct and so has increased the penalty at Step 4.

6.19. The Authority consider that it is appropriate to apply an adjustment for deterrence and increases the Step 3 figure by a multiple of 1.75.

6.20. Step 4 is therefore £10,959,728.

#### **Step 5: settlement discount**

6.21. 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.

6.22. GT Bank and the Authority reached agreement at Stage 1 and so a 30% discount applies to the Step 4 figure.

6.23. Step 5 is therefore £7,671,810.

- 6.24. The Authority therefore imposes a total financial penalty of £7,671,800 on GT Bank for breaching Principle 3 and SYSC.

## **7. PROCEDURAL MATTERS**

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

### **Decision maker**

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

### **Manner and time for payment**

- 7.4. The financial penalty must be paid in full by GT Bank to the Authority no later than 24 January 2023.

### **If the financial penalty is not paid**

- 7.5. If all or any of the financial penalty is outstanding on 25 January 2023, the Authority may recover the outstanding amount as a debt owed by GT Bank and due to the Authority.

### **Publicity**

- 7.6. Sections 391(4), 391(6) and 391(7) of the Act apply to the publication of information about the matter to which this notice relates. Under those provisions, the Authority must publish such information about the matter to which this notice relates as the Authority considers appropriate. The information may be published in such manner as the Authority considers appropriate. However, the Authority may not publish information if such publication would, in the opinion of the Authority, be unfair to you or prejudicial to the interests of consumers or detrimental to the stability of the UK financial system.

- 7.7. The Authority intends to publish such information about the matter to which this Final Notice relates as it considers appropriate.
- 7.8. 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). Under section 391(1A) of the Act a person to whom a decision notice is given or copied may not publish the notice or any details concerning it unless the Authority has published the notice or those details.

**Authority contacts**

- 7.9. For more information concerning this matter generally, contact Phoebe Spillane at the Authority (email: [phoebe.spillane@fca.org.uk](mailto:phoebe.spillane@fca.org.uk)).

**Kerralie Wallbridge**

Head of Department

Financial Conduct Authority, Enforcement and Market Oversight Division

---

## ANNEX

---

### RELEVANT STATUTORY AND REGULATORY PROVISIONS

#### 1. RELEVANT STATUTORY PROVISIONS

- 1.1. Pursuant to sections 1B and 1D of the Act, one of the Authority's operational objectives is protecting and enhancing the integrity of the UK financial system.
- 1.2. Pursuant to section 206 of the Act, if the Authority considers that an authorised person has contravened a requirement imposed on it by or under the Act, it may impose on that person a penalty in respect of the contravention of such amount as it considers appropriate.

#### 2. RELEVANT REGULATORY PROVISIONS

- 2.1. In exercising its powers to impose a financial penalty and to impose a restriction in relation to the carrying on of a regulated activity, the Authority has had regard to the relevant regulatory provisions published in the Authority's Handbook. The main provisions that the Authority considers relevant are set out below.

##### **Principles**

- 2.2. The Principles are a general statement of the fundamental obligations of firms under the regulatory system and are set out in the Authority's Handbook.
- 2.3. Principle 3 provides:

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

- 2.4. During the relevant period, the following rules applied:

##### **SYSC**



2.5. SYSC 3.1.1R provides:

*"A firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business."*

2.6. SYSC 3.2.6R provides:

*"A firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime."*

2.7. SYSC 5.1.1R provides:

*"A firm (other than a common platform firm) must employ personnel with the skills, knowledge and expertise necessary for the discharge of the responsibilities allocated to them."*

2.8. SYSC 6.1.1R provides:

*"A firm must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable, tied agents) with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime."*

2.9. SYSC 6.3.1R provides:

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

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

2.10. SYSC 6.3.3R provides:

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

2.11. SYSC 6.3.9R provides:

*"A firm (with the exception of a sole trader who has no employees) must:*

- (1) appoint an individual as MLRO, with responsibility for oversight of its compliance with the FCA's rules on systems and controls against money laundering; and*
- (2) ensure that its MLRO has a level of authority and independence within the firm and access to resources and information sufficient to enable him to carry out that responsibility."*

## **DEPP**

2.12. Chapter 6 of DEPP, which forms part of the Authority's Handbook, sets out the Authority's statement of policy with respect to the imposition and amount of financial penalties under the Act. In particular, DEPP 6.5A sets out the five steps for penalties imposed on firms.

## **Enforcement Guide**

2.13. The Enforcement Guide sets out the Authority's approach to taking disciplinary action. The Authority's approach to financial penalties and suspensions (including restrictions) is set out in Chapter 7 of the Enforcement Guide.