
FINAL NOTICE

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

FRN: **466611**

Address: **60-62 Margaret Street**
London
W1W 8TF

Date: **8 August 2013**

1. ACTION

- 1.1. For the reasons given in this notice, the Authority hereby imposes on Guaranty Trust Bank (UK) Limited (GTBUK or the Firm) a financial penalty of £525,000 for breaches of Principle 3 (management and control) of the Authority's Principles for Businesses between 19 May 2008 and 19 July 2010 (the Relevant Period).
- 1.2. GTBUK agreed to settle at an early stage of the Authority's investigation. It therefore 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 £750,000 on GTBUK.

2. SUMMARY OF REASONS

- 2.1. During the Relevant Period GTBUK breached Principle 3 because it failed to take reasonable care to establish and maintain effective anti-money-laundering (AML)

systems and controls in relation to customers that were identified by the Firm as presenting a higher risk of money-laundering or terrorist financing for the purposes of the 2007 Regulations, including those customers deemed to be a politically exposed person (PEP).

- 2.2. The laundering of money through UK financial institutions undermines the UK financial services sector. It is the responsibility of UK financial institutions to ensure that they minimise the risk of being used for criminal purposes and, in particular, that they do not handle the proceeds of crime. Unless firms have in place robust systems and controls in relation to AML particularly with respect to higher risk customers, they risk leaving themselves open to abuse by money launderers. The Authority has the operational objective of protecting and enhancing the integrity of the UK financial system enshrined in statute (the Integrity Objective). The integrity of the UK financial system is endangered by failures which risk the system being used for a purpose connected with financial crime.
- 2.3. The Authority must, so far as is compatible with acting in a way which advances the Integrity and Consumer Protection Objectives, discharge its general functions in a way which promotes effective competition in the interests of consumers. Firms that do not meet minimum standards for AML may be perceived to have an unfair competitive (cost) advantage over firms that are compliant. Effective enforcement action provides a significant disincentive to non-compliance and therefore encourages firms to compete in legitimate ways that benefit consumers without imposing the costs associated with non-compliance.
- 2.4. The Relevant Period commenced when GTBUK started their operations in the UK, therefore GTBUK had only been regulated for a short period of time at the start of the Relevant Period. During this time they expanded their customer base significantly, establishing relationships with individuals from jurisdictions which posed increased risks of money laundering and corruption. Despite being a relatively new firm, it is vital that regulated activity is carried out in a compliant manner from the outset.
- 2.5. The failings at GTBUK were serious and systemic resulting in an unacceptable risk of handling the proceeds of crime. In particular, during the Relevant Period the Firm 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 customer due diligence and carry out enhanced due diligence when establishing relationships with higher risk customers; and
 - (3) conduct the appropriate level of on-going monitoring for its existing higher risk customers.
- 2.6. As part of its investigation, the Authority reviewed a sample of 51 of GTBUK's higher risk retail customer files, 18 of which related to PEPs, and the Authority found that GTBUK had failed to do one or more of the following in each of the files:
 - (1) carry out and/or document an adequate risk assessment of the potential money-laundering risks posed by higher risk customers in accordance with their policies and procedures;
 - (2) screen prospective customers against HMT sanction lists prior to commencing the relationship;
 - (3) screen prospective customers against PEP databases prior to commencing a business relationship;
 - (4) obtain and/or document senior management approval to establish a business relationship with PEPs;
 - (5) establish sufficiently the purpose and intended nature of prospective customers' accounts;
 - (6) establish and verify with adequate evidence the source of wealth and funds of higher risk customers; and
 - (7) conduct on-going reviews of higher risk customer files periodically to ensure the information and risk assessment was up-to-date and that the activity on accounts was consistent with expected activity.
- 2.7. In addition to the breach of Principle 3, GTBUK also breached the following Senior Management Arrangements, Systems and Controls rules (SYSC) in the FCA Handbook: SYSC 6.1.1R and SYSC 6.3.1R (which are listed in the Appendix to this Notice).
- 2.8. GTBUK's failings merit the imposition of a financial penalty. The FCA considers the failings to be serious because:

- (1) There was an unacceptable risk that GTBUK could have been used by customers to launder the proceeds of crime.
- (2) GTBUK provided financial services to a significant number of higher risk customers, acting as a gateway to the UK financial system for these customers, most of which emanated from jurisdictions which do not have AML requirements equivalent to those in the UK and identified by industry recognised sources as posing a higher risk of money-laundering.
- (3) The failings were not identified by the Firm.
- (4) The failings referred to in this Notice also occurred in a period during which the Authority brought and published other Enforcement cases against a number of institutions for shortcomings in their financial crime systems and controls. As such, the Firm ought to have been aware of the importance of systems and controls to prevent and detect all types of financial crime, including money-laundering.

2.9. In deciding upon the appropriate disciplinary sanction, the Authority has taken the following into account:

- (1) GTBUK and its senior management have co-operated fully and engaged with the Authority's investigation;
- (2) GTBUK has invested heavily in improving its AML systems and controls including, significantly increasing the resource of its compliance department by hiring additional personnel, employing a compliance consultant and investing in systems to assist managing AML risk; and
- (3) the Firm has made a strategic decision to move away from establishing relationships with PEPs, including exiting current relationships, wherever possible.

3. DEFINITIONS

3.1. The definitions below are used in this Final Notice.

"the 2007 Regulations" means the Money Laundering Regulations 2007, which came into force on 15 December 2007

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

"AML" means anti-money-laundering

"the Authority" means the body corporate previously known as the Financial Services Authority and renamed on 1 April 2013 as the Financial Conduct Authority of 25 The North Colonnade, Canary Wharf, London, E14 5HS;

"CDD" means customer due diligence measures, defined in Regulation 5 of the 2007 Regulations

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

"Designated Persons" means those individuals and entities who are the subject of financial sanctions orders imposed by HM Treasury which prohibit firms from carrying out transactions with them. Such Designated Persons appear on the consolidated list of targets published by HM Treasury.

"EDD" means enhanced due diligence, The circumstances where EDD should be applied are included in Regulation 14 of the 2007 Regulations

"the Firm" and "GTBUK" means Guaranty Trust Bank (UK) Limited

"GTB" means Guaranty Trust Bank PLC, which is incorporated in Nigeria

"higher risk customers" means individual and corporate customers, including those customers deemed to be a politically exposed person (PEP), that present a higher risk of money-laundering or terrorist financing for the purposes of the 2007 Regulations

"HMT" means HM Treasury

"JMLSG" means the Joint Money Laundering Steering Group

"JMLSG Guidance" means the guidance issued by the JMLSG on compliance with the legal requirements in the 2007 Regulations, regulatory requirements in the FCA Handbook and evolving practice within the financial services industry from time to time.

"KYC" means know your customer

"MLRO" means money laundering reporting officer

"PEP" means Politically Exposed Person. A PEP is defined in the 2007 Regulations as *'an individual who is or has, at any time in the preceding year, been entrusted with a*

prominent public function' and an immediate family member, or a known close associate, of such a person. The definition only applies to those holding such a position in a state outside the UK, or in a European Community institution or an international body

"the Relevant Period" means 19 May 2008 and 19 July 2010

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

"SYSC" means the FCA's Senior Management Arrangement, systems and controls rules

4. FACTS AND MATTERS

Background

- 4.1. GTBUK is the wholly owned UK subsidiary of GTB, a leading Nigerian financial services institution that provides a range of banking services across West Africa and the United Kingdom, employing over 5,000 people in seven countries. GTB is a public limited company, listed on the Nigerian and London stock exchanges. GTBUK represents approximately 4% of GTB's overall business, with an annual turnover of £4.6m in 2010 and £1.8m in 2009. GTBUK made annual losses of £1.27m and £3.57m in those years respectively.
- 4.2. GTBUK has been authorised since the 10 March 2008 and started accepting customers on the 19 May 2009, the start of the Relevant Period. GTBUK has 50 employees operating out of one office in London offering retail and wholesale banking products and services to private, corporate and institutional clients. During the Relevant Period, GTBUK had approximately 2,800 retail customers, of which almost 70% were regarded by GTBUK as posing a higher risk of money-laundering, primarily because of the customer's country of residence.

AML legal and regulatory obligations

- 4.3. Firms are required by the 2007 Regulations and the Authority's Handbook to implement and maintain systems and controls to prevent and detect money-laundering. Further to the 2007 Regulations, a firm must be able to demonstrate to its supervisory authority that the extent of the due diligence and on-going monitoring measures it applies is appropriate in view of the risks of money-laundering and terrorist financing it faces.

- 4.4. The JMLSG is a body comprising the leading UK trade associations in the financial services industry. Since 1990, the JMLSG has produced advice, which is approved by an HMT Minister, for the financial services sector on AML controls. The JMLSG Guidance during the Relevant Period provided guidance on compliance with the legal requirements in the 2007 Regulations, regulatory requirements in the FCA Handbook and evolving practice within the financial services industry.
- 4.5. The FCA's SYSC rules provide that when considering whether a breach of its rules on systems and controls against money-laundering has occurred, the Authority will have regard to whether the Firm followed the relevant provisions in the JMLSG Guidance (which are listed in the Appendix to this Notice).

The Authority's Thematic Review

- 4.6. In June 2011, the Authority reported on the findings of a thematic review of how banks operating in the UK were managing money-laundering risk in higher risk situations, including the risks arising from PEPs and other high risk customers.
- 4.7. As part of the thematic review, the Authority visited GTBUK on 18 and 19 May 2010 to assess its AML systems and controls. The results of this visit gave the Authority cause for concern.
- 4.8. After further investigation, including further file reviews, the Authority identified failings in respect of GTBUK's AML systems and controls in relation to its higher risk customer relationships, including PEPs. These failings are described below.

Risk assessment of prospective customers

- 4.9. To implement its obligations under the 2007 Regulations, GTBUK was required to put in place adequate and risk-sensitive AML policies and procedures. This means that GTBUK had to identify and assess its money-laundering risk, and put in place sufficient systems and controls to manage and mitigate this risk.
- 4.10. GTBUK's policies and procedures set out the specific money-laundering risks relating to their services, products and customers and having identified these risks the measures implemented to mitigate them. One of the ways the Firm sought to mitigate money-laundering risk was to have a comprehensive KYC process. This process included documenting for each customer a risk assessment of both the business to be undertaken with the client and the client.

- 4.11. The Authority's file review found that 46 of the 51 files reviewed did not have adequate documentation evidencing that an assessment of the money-laundering risks associated with prospective customers had taken place. Although the Authority recognises that the customer files reviewed had been correctly identified as posing a higher risk of money-laundering, it was not always clear what risks had been identified and that all the relevant risk factors, as set out in the Firm's policies and procedures, had been considered.
- 4.12. As such, the Authority could not find evidence that a comprehensive risk assessment of these 46 customers had been carried out and whether GTBUK had considered all the risks posed by these customers before approving the relationship. This failure would impede the on-going monitoring of these relationships.

Senior management approval for PEPs

- 4.13. Firms are required by the 2007 Regulations to obtain senior management approval when establishing a business relationship with a PEP. As such, GTBUK's policies and procedures stipulated that approval from the MLRO, Managing Director and Executive Director-Operations (jointly) was required before an account could be opened for a PEP. However, the Authority found that 13 out of GTBUK's 18 PEP customer files reviewed did not contain the correct level of senior management sign off at account opening. In one instance there was no evidence of any sign off by senior management.

Customer due diligence

- 4.14. CDD consists of fundamental checks that apply to all new customers, whether they are higher risk or not. In accordance with the 2007 Regulations, a firm must typically conduct CDD for all business relationships. CDD measures include:
- (1) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
 - (2) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant person is satisfied that he knows who the beneficial owner is; and

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

4.15. CDD is not just a requirement to gather documents, firms must give active consideration to information they gather and seek clarification and explanation of anything missing or inconsistencies in the information gathered.

Purpose and intended nature of the business relationship

4.16. The 2007 Regulations and JMLSG Guidance stipulate that a firm must understand the purpose and intended nature of the business relationship or transaction to assess whether the proposed business relationship is in line with the firm's expectation and to provide a meaningful basis for on-going monitoring.

4.17. In 23 of the 51 higher risk customer files reviewed by the Authority, GTBUK failed to establish or document adequately, the purpose and intended nature of the business relationship.

4.18. GTBUK's standard account application forms included the question '*What is the main reason for applying for the account? (Please specify e.g. day to day expenses).*' This question formed the basis for GTBUK's understanding of the intended purpose of accounts.

4.19. The Authority's review found that 13 customers all of which were resident in Nigeria, had responded to this question with the suggested answer of '*day to day expenses.*' Despite this answer appearing to contradict the customers' profiles GTBUK failed to seek clarification from the customer. Whilst the Firm has since clarified with these customers the purpose of opening their accounts, there is no evidence that this was understood at the time of account opening.

4.20. In addition, of the files reviewed, 10 had not answered this question or had completed an application form that failed to ask why they were applying for the account.

4.21. The Authority found that GTBUK failed to demonstrate that they had given due consideration to the intended purposes of prospective customers' accounts. Failing to make enquires of customers about missing, insufficient or implausible responses to questions is indicative of treating CDD as an administrative box ticking exercise and not a meaningful assessment of the risks posed by customers. Further in some cases, GTBUK's standard forms did not even ask the initial question.

- 4.22. The Authority recognises that in some cases customers may have been asked by GTBUK representatives the purpose of opening their account. But not recording this would severely hamper GTBUK's ability to conduct on-going monitoring.

EDD

- 4.23. In accordance with the 2007 Regulations, a firm must, on a risk sensitive basis, apply EDD measures and enhanced on-going monitoring in any situation which by its nature presents a higher risk of money laundering and also when the firm proposes to have a business relationship or carry on an occasional transaction with a PEP (as well as in other specific situations).
- 4.24. The main objective of EDD is to ensure a firm has a better understanding of the risks associated with particular customers thereby enabling a firm to decide whether to establish or continue with the business relationships and, where necessary, to mitigate any risk of money-laundering. A firm must be able to demonstrate that the extent of the EDD measures it applies is commensurate with the money-laundering and any terrorist financing risks posed by the particular customer.
- 4.25. The information gathered for EDD purposes also forms a basis for a firm's understanding of its customers' affairs so that it may properly undertake enhanced on-going monitoring of transactions.
- 4.26. EDD includes taking adequate measures to establish a customer's source of wealth and source of funds which are involved in the business relationship or occasional transaction.

Source of wealth & source of funds

- 4.27. Consistent with its regulatory obligations, GTBUK's policy required that, as part of its EDD there be *'measures to establish and verify the origin of wealth and source(s) of funds (including the economic activity that created the wealth) as well as the source of funds to be used in the relationship. Care should be taken to ensure original supporting documentation... ..are reviewed and certified copies retained.'*
- 4.28. GTBUK requested information about customers' source of wealth and funds in account application forms. Despite the application form requiring customers to provide documentary evidence, such as payslips or sales agreements, GTBUK accepted customers' responses to these questions at face value without sufficient

follow up requests for documentary evidence. This failure was exacerbated by many customers giving vague responses, such as a customer's source of wealth being from '*sale of business*' with no indication as to what business, or '*Earnings or profit*' without any clarification as to where these emanated.

- 4.29. The Authority found that GTBUK had failed to establish adequately a customer's source of wealth on 42 of the 51 customer files reviewed. In particular, 36 of these files failed to hold any documentary evidence to back up the responses by customers and five where customers had not responded to the questions about source of wealth and no other information had been gathered by GTBUK. In one of the files reviewed, the Authority found that there were inconsistencies between the source of wealth information provided and the evidence provided by the customers.
- 4.30. In 40 out of 51 files reviewed GTBUK failed to establish or document adequately customers' source of funds. In the vast majority of files (34 files) this was due to a failure to gather documentary evidence to back up the often vague responses by customers. Six of the customer files had no information as to the source of funds expected to be used in the relationship.
- 4.31. The source of wealth and funds to be used in the relationship of many of the customers was said to come from their salary. Most of these files recorded the identity of the customer's employer, but few provided documentary evidence, such as pay slips or bank statements verifying their employer and level of income.
- 4.32. By not adequately establishing the legitimacy of customers' source of wealth and funds used in business relationship, GTBUK could not make a fully informed decision about accepting customers with higher money-laundering risks or take steps to mitigate adequately any money-laundering risks and ultimately that these accounts were not used to launder the proceeds of crime.
- 4.33. One account related to a PEP customer whose source of wealth had been recorded but not quantified or evidenced by separate documentary evidence. During this relationship the customer deposited a cheque for more than £500,000 from an offshore account. Apart from an advice slip indicating that this cheque represented the closing balance on the customer's account, there was no evidence of GTBUK requesting information about the ultimate source of these funds and how they were generated.

4.34. At the time of the transaction there was no adverse information about the customer, however later in the relationship information came to light that the customer was wanted by UK authorities in connection with laundering millions of dollars of embezzled public funds. The Authority recognises that GTBUK took appropriate steps once they identified this information and that this transaction may have been legitimate, however GTBUK had not gathered sufficient information about the customer or the funds at the time of the transaction which might have identified the transaction as being suspicious.

PEP and Sanction screening

4.35. To comply with the 2007 Regulations, firms are required, on a risk sensitive basis, to have appropriate risk based procedures to determine whether a customer is a PEP. Failing to identify prospective or existing customers as a PEP would give rise to an unacceptable risk that such customers would not be subject to the appropriate money laundering controls.

4.36. To comply with the 2007 Regulations, firms are obliged not to provide funds or financial services to Designated Persons, unless a licence is obtained from the HMT. HMT maintains a consolidated list of Designated Persons that are subject to financial sanctions applied by the United Nations, European Union and United Kingdom. In order to reduce the risk of breaching these obligations, by conducting business with or on behalf of Designated Persons, the JMLSG Guidance provides that all customers should be screened against the sanctions list during the establishment of a business relationship or as soon as possible after the relationship has commenced.

4.37. In order to ensure compliance with these requirements regarding identification of PEPs and Designated Persons, GTBUK's policies stipulated that checks be carried out to identify whether a prospective customer is a PEP or appears on any sanction lists prior to opening an account. The results were required to be recorded on the customer's file.

4.38. To carry out these checks GTBUK utilised a third party screening service to screen customers against sanction and PEP databases. Once screened, customers were automatically periodically re-screened by the third party system so that the Firm would be notified if any existing customers had been added to sanctions or PEP lists.

- 4.39. The Authority's investigation found that results of screening carried out was not recorded on files, unless there was a positive match, and that screening of customers had not been done in all cases prior to the opening accounts, or within a reasonable timeframe, for 29 of the 51 customer files reviewed. Of these files:
- (1) three had been opened for more than two years before being screened;
 - (2) two had been opened for more than a year before being screened; and
 - (3) five had been opened for more than six months before they were screened.

Enhanced on-going monitoring

- 4.40. In accordance with the 2007 Regulations, a firm must conduct on-going monitoring of all business relationships. Where the customer is considered to be higher risk, that monitoring must be enhanced. Enhanced on-going monitoring is important for understanding any changes to the money-laundering risks posed by customers. It includes performing regular reviews of what is known about customers and taking steps to ensure that information obtained about customers remains current. It also requires heightened scrutiny of transactions undertaken in the course of the business relationship to ensure activity is consistent with what is known about a customer.
- 4.41. Without adequate knowledge of a customer's profile and without an adequate and effective on-going monitoring programme in place, a firm cannot properly re-assess the risk profiles of its customers as they develop over time. In addition, a firm may not be able to identify transaction activity that potentially involves money-laundering.
- 4.42. In accordance with their policies and procedures, GTBUK was required to review PEP and higher risk customer relationships annually to ensure customer information was up-to-date and that the customer risk status was maintained appropriately. However, GTBUK did not start the process of reviewing higher risk customer relationships until July 2010.
- 4.43. Of the 51 customer files reviewed by the Authority, 46 raised concerns with GTBUK's on-going monitoring of the relationship. In particular, the Authority found 14 higher risk customers that had not been reviewed for more than 3 years.

4.44. These failings meant that changes to a customer's risk profile, including those that had the potential to increase significantly the money-laundering risks posed by the customer, would not necessarily have been highlighted and given full consideration. They would also undermine the ability of GTBUK to conduct effective transaction monitoring.

5. FAILINGS

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

5.2. The Authority considers that GTBUK breached Principle 3 by failing to take reasonable care to establish and maintain effective AML systems and controls in relation to PEPs and other higher risk customers. As a result, GTBUK did not in all cases during the Relevant Period:

- (1) carry out and/or document an adequate risk assessment of the potential money-laundering risks posed by higher risk customers in accordance with their policies and procedures;
- (2) screen prospective customers against HMT sanction lists prior to commencing the relationship;
- (3) screen prospective customers against PEP databases prior to commencing a business relationship;
- (4) obtain and/or document senior management approval to establish a business relationship with PEPs;
- (5) establish sufficiently the purpose and intended nature of prospective customers' accounts;
- (6) establish and verify with adequate evidence the source of wealth and funds of higher risk customers; and
- (7) conduct on-going reviews of higher risk customer files periodically to ensure the information and risk assessment was up-to-date and that the activity on accounts was consistent with expected activity.

5.3. These weaknesses in GTBUK's AML systems and controls resulted in an unacceptable risk that the Firm could have been used by customers to launder the proceeds of crime.

- 5.4. As well as breaches of Principle 3, these failings amounted to breaches of SYSC 6.1.1R and SYSC 6.3.1R.

6. SANCTION

- 6.1. The Authority has considered the disciplinary and other options available to it and has concluded that a financial penalty is the appropriate sanction in the circumstances of this particular case.
- 6.2. The Authority's policy on the imposition of financial penalties is set out in Chapter 6 of DEPP which forms part of the Authority's Handbook. Since the majority of the misconduct occurred before the introduction of the new penalty regime on 6 March 2010, the Authority has applied the penalty regime that was in place before that date. DEPP 6.5.2G sets out factors that may be of particular relevance in determining the appropriate level of financial penalty for a firm or approved person. The criteria are not exhaustive and all relevant circumstances of the case are taken into consideration in determining whether a financial penalty is appropriate and the amount.

Deterrence

- 6.3. The Authority considers that the financial penalty will promote high standards of regulatory conduct by deterring firms which have breached regulatory requirements from committing further contraventions, helping to deter other firms from committing contraventions and demonstrating generally to firms the benefit of compliant behaviour. It strengthens the message to the industry that it is vital to take proper steps to ensure that AML systems and controls are adequate.

Seriousness of the breaches

- 6.4. The Authority has had regard to the seriousness of the breaches, including the nature of the requirements breached and the number and duration of the breaches. For the reasons set out in paragraph 2.8 of this notice, the Authority considers that GTBUK's breaches are of a serious nature.

The extent to which the breach was deliberate or reckless

- 6.5. The Authority does not consider that GTBUK deliberately or recklessly contravened regulatory requirements.

The size, financial resources and other circumstances of the firm

- 6.6. The Authority has taken into account GTBUK's size and financial resources. There is no evidence to suggest that GTBUK is unable to pay the penalty.

Disciplinary record and compliance history

- 6.7. The Authority has taken into account the fact that GTBUK has not been the subject of previous disciplinary action.

Conduct following the breach

- 6.8. Since the commencement of the Authority's investigation, GTBUK has worked in an open and cooperative manner with the Authority.

Previous action taken by the Authority in relation to similar findings

- 6.9. In determining whether and what financial penalty to impose on GTBUK, the Authority has taken into account action taken by the Authority in relation to other authorised persons for comparable behaviour.

Authority guidance and other published material

- 6.10. Pursuant to DEPP 6.2.3G and SYSC 6.3.5G, the Authority has had regard to whether GTBUK followed the relevant provisions of the JMLSG Guidance when considering whether to take action in respect a breach of its rules on systems and controls against money-laundering.

7. PROCEDURAL MATTERS

Decision maker

- 7.1. The decision which gave rise to the obligation to give this Notice was made by the Settlement Decision Makers.
- 7.2. This Final Notice is given under, and in accordance with, section 390 of the Act.

Manner of and time for Payment

- 7.3. The financial penalty must be paid in full by GTBUK to the Authority by no later than 22 August 2103, 14 days from the date of the Final Notice.

If the financial penalty is not paid

- 7.4. If all or any of the financial penalty is outstanding on 23 August 2013, the Authority may recover the outstanding amount as a debt owed by GTBUK and due to the Authority.

Publicity

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

Authority contacts

- 7.7. For more information concerning this matter generally, contact Guy Wilkes (direct line: 020 7066 7574) of the Enforcement and Financial Crime Division of the Authority.

Tom Spender

Head of Department

Financial Conduct Authority, Enforcement and Financial Crime Division

APPENDIX

THE FCA'S PRINCIPLES FOR BUSINESSES

Principle 3

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

RULES AND GUIDANCE

For the period from 19 May 2008 to 31 March 2009

SYSC 6.1.1 R

A common platform 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.

SYSC 6.3.1 R

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

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

SYSC 6.3.2 G

"Money laundering risk" is the risk that a firm may be used to further money laundering. Failure by a firm to manage this risk effectively will increase the risk to society of crime and terrorism.

SYSC 6.3.4 G

A common platform firm may also have separate obligations to comply with relevant legal requirements, including the Terrorism Act 2000, the Proceeds of Crime Act 2002 and the Money Laundering Regulations.

SYSC 6.3.5 G

The Authority, when considering whether a breach of its rules on systems and controls against money laundering has occurred, will have regard to whether a firm has followed relevant provisions in the guidance for the United Kingdom financial sector issued by the Joint Money Laundering Steering Group.

SYSC 6.3.6 G

In identifying its money laundering risk and in establishing the nature of these systems and controls, a common platform firm should consider a range of factors, including:

- (1) its customer, product and activity profiles;
- (2) its distribution channels;
- (3) the complexity and volume of its transactions;
- (4) its processes and systems; and
- (5) its operating environment.

For the period from 1 April 2009 to 19 July 2010.

Identical provisions applied during this period, save that the words 'common platform firm' were removed and replaced by 'firm'.

For the whole of the Relevant Period

DEPP 6.2.3 G

The FCA's rules on systems and controls against money laundering are set out in SYSC 3.2 and SYSC 6.3. The FCA, when considering whether to take action for a financial penalty or censure in respect of a breach of those rules, will have regard to whether a firm has followed relevant provisions in the Guidance for the UK financial sector issued by the Joint Money Laundering Steering Group.

DEPP 6.5.2 G

The following factors may be relevant to determining the appropriate level of financial penalty to be imposed on a person under the Act:

(1) Deterrence

When determining the appropriate level of penalty, the FCA will have regard to the principal purpose for which it imposes sanctions, namely to promote high standards of regulatory and/or market conduct by deterring persons who have committed breaches from committing further breaches and helping to deter other persons from committing similar breaches, as well as demonstrating generally the benefits of compliant business.

(2) The nature, seriousness and impact of the breach in question

The FCA will consider the seriousness of the breach in relation to the nature of the rule, requirement or provision breached. The following considerations are among those that may be relevant:

- (a) the duration and frequency of the breach;
- (b) whether the breach revealed serious or systemic weaknesses in the person's procedures or of the management systems or internal controls relating to all or part of a person's business;
- (c) in market abuse cases, the FCA will consider whether the breach had an adverse effect on markets and, if it did, how serious that effect was, which may include having regard to whether the orderliness of, or confidence in, the markets in question has been damaged or put at risk. This factor may also be relevant in other types of case;
- (d) the loss or risk of loss caused to consumers, investors or other market users;
- (e) the nature and extent of any financial crime facilitated, occasioned or otherwise attributable to the breach; and
- (f) in the context of contraventions of Part VI of the Act, the extent to which the behaviour which constitutes the contravention departs from current market practice.

(3) The extent to which the breach was deliberate or reckless

The FCA will regard as more serious a breach which is deliberately or recklessly committed. The matters to which the FCA may have regard in determining whether a breach was deliberate or reckless include, but are not limited to, the following:

- (a) whether the breach was intentional, in that the person intended or foresaw the potential or actual consequences of its actions;
- (b) where the person has not followed a firm's internal procedures and/or FCA guidance, the reasons for not doing so;
- (c) where the person has taken decisions beyond its or his field of competence, the reasons for the decisions and for them being taken by that person;
- (d) whether the person has given no apparent consideration to the consequences of the behaviour that constitutes the breach;
- (e) in the context of a contravention of any rule or requirement imposed by or under Part VI of the Act, whether the person sought any professional advice before the contravention occurred and whether the person followed that professional advice. Seeking professional advice does not remove a person's responsibility for compliance with applicable rules and requirements.
- (f) If the FCA decides that the breach was deliberate or reckless, it is more likely to impose a higher penalty on a person than would otherwise be the case.

(4) Whether the person on whom the penalty is to be imposed is an individual

When determining the amount of a penalty to be imposed on an individual, the FCA will take into account that individuals will not always have the resources of a body corporate, that enforcement action may have a greater impact on an individual, and further, that it may be possible to achieve effective deterrence by imposing a smaller penalty on an individual than on a body corporate. The FCA will also consider whether the status, position and/or responsibilities of the individual are such as to make a breach committed by the individual more serious and whether the penalty should therefore be set at a higher level.

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

- (a) The FCA may take into account whether there is verifiable evidence of serious financial hardship or financial difficulties if the person were to pay the level of penalty appropriate for the particular breach. The FCA regards these factors as matters to be taken into account in determining the level of a penalty, but not to the extent that there is a direct correlation between those factors and the level of penalty.

- (b) The purpose of a penalty is not to render a person insolvent or to threaten the person's solvency. Where this would be a material consideration, the FCA will consider, having regard to all other factors, whether a lower penalty would be appropriate. This is most likely to be relevant to a person with lower financial resources; but if a person reduces its solvency with the purpose of reducing its ability to pay a financial penalty, for example by transferring assets to third parties, the FCA will take account of those assets when determining the amount of a penalty.
- (c) The degree of seriousness of a breach may be linked to the size of the firm. For example, a systemic failure in a large firm could damage or threaten to damage a much larger number of consumers or investors than would be the case with a small firm: breaches in firms with a high volume of business over a protracted period may be more serious than breaches over similar periods in firms with a smaller volume of business.
- (d) The size and resources of a person may also be relevant in relation to mitigation, in particular what steps the person took after the breach had been identified; the FCA will take into account what it is reasonable to expect from a person in relation to its size and resources, and factors such as what proportion of a person's resources were used to resolve a problem.
- (e) The FCA may decide to impose a financial penalty on a mutual (such as a building society), even though this may have a direct impact on that mutual's customers. This reflects the fact that a significant proportion of a mutual's customers are shareholder members; to that extent, their position involves an assumption of risk that is not assumed by customers of a firm that is not a mutual. Whether a firm is a mutual will not, by itself, increase or decrease the level of a financial penalty.

(6) The amount of benefit gained or loss avoided

The FCA may have regard to the amount of benefit gained or loss avoided as a result of the breach, for example:

- (a) the FCA will propose a penalty which is consistent with the principle that a person should not benefit from the breach; and
- (b) the penalty should also act as an incentive to the person (and others) to comply with regulatory standards and required standards of market conduct.

(7) Difficulty of detecting the breach

A person's incentive to commit a breach may be greater where the breach is, by its nature, harder to detect. The FCA may, therefore, impose a higher penalty where it considers that a person committed a breach in such a way as to avoid or reduce the risk that the breach would be discovered, or that the difficulty of detection (whether actual or perceived) may have affected the behaviour in question.

(8) Conduct following the breach

The FCA may take the following factors into account:

- (a) the conduct of the person in bringing (or failing to bring) quickly, effectively and completely the breach to the FCA's attention (or the attention of other regulatory authorities, where relevant);
- (b) the degree of cooperation the person showed during the investigation of the breach by the FCA, or any other regulatory authority allowed to share information with the FCA, such as an RIE or the Takeover Panel. Where a person has fully cooperated with the FCA's investigation, this will be a factor tending to reduce the level of financial penalty;
- (c) any remedial steps taken since the breach was identified, including whether these were taken on the person's own initiative or that of the FCA or another regulatory authority; for example, identifying whether consumers or investors or other market users suffered loss and compensating them where they have; correcting any misleading statement or impression; taking disciplinary action against staff involved (if appropriate); and taking steps to ensure that similar problems cannot arise in the future; and
- (d) whether the person concerned has complied with any requirements or rulings of another regulatory authority relating to the breach (for example, where relevant, those of the Takeover Panel).

(9) Disciplinary record and compliance history

The FCA may take the previous disciplinary record and general compliance history of the person into account. This will include:

- (a) whether the FCA (or any previous regulator) has taken any previous disciplinary action against the person;

- (b) whether the person has previously undertaken not to do a particular act or engage in particular behaviour;
- (c) whether the FCA (or any previous regulator) has previously taken protective action in respect of a firm using its own initiative powers, by means of a variation of a firm's Part IV permission, or has previously requested the firm to take remedial action and the extent to which that action has been taken.
- (d) the general compliance history of the person, including whether the FCA (or any previous regulator) has previously brought to the person's attention, including by way of a private warning, issues similar or related to the conduct that constitutes the breach in respect of which the penalty is imposed.

A person's disciplinary record could lead to the FCA imposing a higher penalty, for example where the person has committed similar breaches in the past.

In assessing the relevance of a person's disciplinary record and compliance history, the age of a particular matter will be taken into account, although a longstanding matter may still be relevant.

(10) Other action taken by the FCA (or a previous regulator)

Action that the FCA (or a previous regulator) has taken in relation to similar breaches by other persons may be taken into account. This includes previous actions in which the FCA (whether acting by the RDC or the settlement decision makers) and a person on whom a penalty is to be imposed have reached agreement as to the amount of the penalty. As stated at DEPP 6.5.1 G(2), the FCA does not operate a tariff system. However, the FCA will seek to apply a consistent approach to determining the appropriate level of penalty.

(11) Action taken by other domestic or international regulatory authorities

Considerations could include, for example:

- (a) action taken or to be taken against a person by other regulatory authorities which may be relevant where that action relates to the breach in question;
- (b) the degree to which any remedial or compensatory steps required by other regulatory authorities have been taken (and whether taken promptly).

(12) FCA guidance and other published materials

- (a) A person does not commit a breach by not following FCA guidance or other published examples of compliant behaviour. However, where a breach has otherwise been established, the fact that guidance or other published materials had raised relevant concerns may inform the seriousness with which the breach is to be regarded by the FCA when determining the level of penalty.
- (b) The FCA will consider the nature and accessibility of the guidance or other published materials when deciding whether they are relevant to the level of penalty and, if they are, what weight to give them in relation to other relevant factors.

(13) The timing of any agreement as to the amount of the penalty

The FCA and the person on whom a penalty is to be imposed may seek to agree the amount of any financial penalty and other terms. In recognition of the benefits of such agreements, DEPP 6.7 provides that the amount of the penalty which might otherwise have been payable will be reduced to reflect the stage at which the FCA and the person concerned reach an agreement.

Relevant extracts from the Money Laundering Regulations 2007

Meaning of customer due diligence measures (Regulation 5)

“Customer due diligence measures” means—

- (a) identifying the customer and verifying the customer’s identity on the basis of documents, data or information obtained from a reliable and independent source;
- (b) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant person is satisfied that he knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and
- (c) obtaining information on the purpose and intended nature of the business relationship.

Application of customer due diligence measures (Regulation 7)

- (1) Subject to regulations 9, 10, 12, 13, 14, 16(4) and 17, a relevant person must apply customer due diligence measures when he—
 - (a) establishes a business relationship;
 - (b) carries out an occasional transaction;
 - (c) suspects money laundering or terrorist financing;
 - (d) doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.
- (2) Subject to regulation 16(4), a relevant person must also apply customer due diligence measures at other appropriate times to existing customers on a risk-sensitive basis.
- (3) A relevant person must—
 - (a) determine the extent of customer due diligence measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction; and
 - (b) be able to demonstrate to his supervisory authority that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.

Ongoing monitoring (Regulation 8)

- (1) A relevant person must conduct ongoing monitoring of a business relationship.
- (2) "Ongoing monitoring" of a business relationship means—
 - (a) scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile; and
 - (b) keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date.

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

Enhanced customer due diligence and ongoing monitoring (Regulation 14)

- (1) – A relevant person must apply on a risk sensitive basis enhanced customer due diligence measures and enhanced ongoing monitoring –
- (a) In accordance with paragraphs (2) to (4);
 - (b) In any other situation which by its nature can present a higher risk of money laundering or terrorist financing.
- (4) A relevant person who proposes to have a business relationship or carry out an occasional transaction with a politically exposed person must—
- (a) have approval from senior management for establishing the business relationship with that person;
 - (b) take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or occasional transaction; and
 - (c) where the business relationship is entered into, conduct enhanced ongoing monitoring of the relationship.

Directions where Financial Action Task Force applies counter-measures (Regulation 18)

The Treasury may direct any relevant person-

- (a) Not to enter into a business relationship;
- (b) Not to carry out an occasional transaction; or
- (c) Not to proceed any further with a business relationship or occasional transaction, with a person who is situated or incorporated in a non-EEA state to which the Financial Action Task Force has decided to apply counter-measures.

Policies and Procedures (Regulation 20)

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

- (a) customer due diligence measures and ongoing monitoring;
 - (b) reporting;
 - (c) record-keeping;
 - (d) internal control;
 - (e) risk assessment and management;
 - (f) the monitoring and management of compliance with, and the internal communication of, such policies and procedures, in order to prevent activities related to money laundering and terrorist financing.
- (2) The policies and procedures referred to in paragraph (1) include policies and procedures-
- (a) which provide for the identification and scrutiny of-
 - (i) complex or unusually large transactions;
 - (ii) unusual patterns of transactions which have no apparent economic or visible lawful purpose; and
 - (iii) any other activity which the relevant person regards as particularly likely by its nature to be related to money laundering or terrorist financing;
 - (b) which specify the taking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products and transactions which might favour anonymity; .
 - (c) to determine whether a customer is a politically exposed person;

OTHER RELEVANT PROVISIONS

Relevant extracts from the JMLSG Guidance

Part I, Chapter 5 – Customer due diligence

5.3 Application of CDD measures

Nature and purpose of proposed business relationship

Paragraph 5.3.21 - A firm must understand the purpose and intended nature of the business relationship or transaction to assess whether the proposed business relationship is in line with the firm's expectation and to provide the firm with a meaningful basis for ongoing monitoring. In some instances this will be self-evident, but in many cases the firm may have to obtain information in this regard.

Paragraph 5.3.22 - Depending on the firm's risk assessment of the situation, information that might be relevant may include some or all of the following:

- nature and details of the business/occupation/employment;
- record of changes of address;
- the expected source and origin of the funds to be used in the relationship;
- the origin of the initial and ongoing source(s) of wealth and funds (particularly within a private banking or wealth management relationship);
- copies of recent and current financial statements;
- the various relationships between signatories and with underlying beneficial owners;
- the anticipated level and nature of the activity that is to be undertaken through the relationship.

Persons firms should not accept as customers

Paragraph 5.3.41 - The United Nations, European Union, and United Kingdom are each able to designate persons and entities as being subject to financial sanctions, in accordance with legislation explained below. Such sanctions normally include a comprehensive freeze of funds and economic resources, together with a prohibition on making funds or economic resources available to the designated target. A Consolidated

List of all targets to whom financial sanctions apply is maintained by HM Treasury, and includes all individuals and entities that are subject to financial sanctions in the UK. This list is at: www.hm-treasury.gov.uk/financialsanctions.

5.5 Enhanced due diligence

Paragraph 5.5.1 - A firm must apply EDD measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. As part of this, a firm may conclude, under its risk-based approach, that the standard evidence of identity is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer.

Paragraph 5.5.2 - As a part of a risk-based approach, therefore, firms should hold sufficient information about the circumstances and business of their customers and, where applicable, their customers' beneficial owners, for two principal reasons:

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

Paragraph 5.5.5 - A firm should hold a fuller set of information in respect of those customers, or class/category of customers, assessed as carrying a higher money laundering or terrorist financing risk, or who are seeking a product or service that carries a higher risk of being used for money laundering or terrorist financing purposes.

Paragraph 5.5.9 - The ML Regulations prescribe three specific types of relationship in respect of which EDD measures must be applied. These are:

- (a) where the customer has not been physically present for identification purposes;
- (b) in respect of a correspondent banking relationship;
- (c) in respect of a business relationship or occasional transaction with a PEP.

Politically exposed persons

Paragraph 5.5.18 - Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to firms as their

position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the customer, or the beneficial owner, into a higher risk category.

Paragraph 5.5.19 - A PEP is defined as “an individual who is or has, at any time in the preceding year, been entrusted with prominent public functions and an immediate family member, or a known close associate, of such a person”. This definition only applies to those holding such a position in a state outside the UK, or in a Community institution or an international body.

Paragraph 5.5.25 - Firms are required, on a risk-sensitive basis, to:

- have appropriate risk-based procedures to determine whether a customer is a PEP;
- obtain appropriate senior management approval for establishing a business relationship with such a customer;
- take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction; and
- conduct enhanced ongoing monitoring of the business relationship.

Senior management approval

Paragraph 5.5.29 – Obtaining approval from senior management for establishing a business relationship does not necessarily mean obtaining approval from the Board of directors (or equivalent body), but higher level of authority from the person seeking such approval. As risk dictates, firms should escalate decisions to more senior management levels.

On-going monitoring

Paragraph 5.5.30 - Guidance on the on-going monitoring of the business relationship is given in section 5.7. Firms should remember that new and existing customers may not initially meet the definition of a PEP, but may subsequently become one during the course of a business relationship. The firm should, as far as practicable, be alert to public information relating to possible changes in the status of its customers with regard to political exposure. When an existing customer is identified as a PEP, EDD must be applied to that customer.

5.7 Monitoring customer activity

Paragraph 5.7.1 - Firms must conduct ongoing monitoring of the business relationship with their customers. Ongoing monitoring of a business relationship includes:

- Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, his business and risk profile;
- Ensuring that the documents, data or information held by the firm are kept up to date.

Paragraph 5.7.2 - Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps firms know their customers, assist them to assess risk and provides greater assurance that the firm is not being used for the purposes of financial crime.

Paragraph 5.7.3 - The essentials of any system of monitoring are that:

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

Paragraph 5.7.12 - Higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring.

Part III, Chapter 4 – Compliance with the UK financial sanctions regime

Screening of customers and transactions

Paragraph 4.32 - Firms should have processes to manage the risk of conducting business with or on behalf of individuals and entities on the Consolidated List (which includes all the names of sanctioned persons and entities under UN and EU sanctions regimes which have effect in the UK). Firms should consider screening their customers on a periodic basis, and certain transaction data. The Consolidated List is available at www.hm-treasury.gov.uk/d/sanctionsconlist.pdf

Timing of screening

Paragraph 4.48 - All customers should be screened during the establishment of a business relationship or as soon as possible after the business relationship has commenced. Firms should be aware of the risks associated with screening customers after a business relationship has been established and/or services have been provided i.e., that they may transact with a sanctioned party in breach of sanctions prohibitions. Firms must be aware of the absolute restrictions embedded in the financial sanctions regime. Where there is any delay in screening, firms face a risk of breaching the legislation.